ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΑΝΑΠΤΥΞΗ ΠΛΑΙΣΙΟΥ ΛΕΙΤΟΥΡΓΙΩΝ ΓΙΑ ΤΗΝ ΑΝΙΧΝΕΥΣΗ, ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΚΑΤΗΓΟΡΙΟΠΟΙΗΣ Η ΑΠΕΙΛΩΝ ΣΤΟ ΕΣΩΤΕΡΙΚΟ ΑΣΤΙΚΟΥ ΔΙΚΤΥΟΥ ΜΕ ΤΗΝ ΧΡΗΣΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΠΕΡΛΕΠΕΣ ΛΕΩΝΙΔΑΣ

ΒΟΛΟΣ , 21 Ιουνίου 2012

Συμβουλευτική Επιτροπή: Κατσαβουνίδης Ιωάννης

Σταμούλης Γεώργιος

Σπυράκης Παύλος

Επταμελή Επιτροπή:

.

Κατσαβουνίδης Ιωάννης
Αναπ. Καθηγητής ΤΜΗΥΤΔ
Πανεπιστήμιο Θεσσαλίας

Σταμούλης Γεώργιος
Καθηγητής ΤΜΗΥΤΔ
Πανεπιστήμιο Θεσσαλίας

Σπυράκης Παύλος
Καθηγητής
Πανεπιστήμιο Πατρών

Χατζηευθυμιάδης Ευστάθιος
Επίκουρος Καθηγητής
Καποδιστριακό Πανεπιστήμιο Αθηνών

Μποζάνης Παναγιώτης Αναπ. Καθηγητής
Πανεπιστήμιο Θεσσαλίας

Ευμορφόπουλος Νέστορας
Λέκτορας
Πανεπιστήμιο Θεσσαλίας

Τσομπανοπούλου Παναγιώτα
Επίκουρη Καθηγήτρια
Πανεπιστήμιο Θεσσαλίας

ΒΟΛΟΣ , 21 Ιουνίου 2012

Ευχαριστίες

Πριν από την παρουσίαση αυτής της διδακτορικής διατριβής θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν στην πραγματοποίηση της και ιδιαίτερα:

Τον επιβλέποντα καθηγητή Δρ. Κατσαβουνίδη Ιωάννη καθώς και τα υπόλοιπα μέλη της τριμελούς επιτροπής Δρ. Σταμούλη Γεώργιο και Δρ. Σπυράκη Παύλο για τις πολύτιμες συμβουλές τους, την καθοδήγησή τους και την αμέριστη συμπαράσταση τους στην εκπόνηση της διατριβής.

Ευχαριστώ επίσης όλα τα μέλη της επταμελούς επιτροπής για την συνεργασία και την αξιολόγηση της διατριβής αυτής.

Ιδιαίτερες ευχαριστίες θέλω να εκφράσω επίσης προς τον Δρ. Κίκιρα Παναγιώτη, για τις συμβουλές και τις υποδείξεις που μου παρείχε, καθώς και για την καθοδήγηση και την αμέριστη συμπαράσταση του καθ' όλη την διάρκεια της εκπόνηση της παρούσας διατριβής.

Ακόμα, θα ήθελα να ευχαριστήσω όλους τους συναδέλφους μου φοιτητές για τις ανταλλαγές απόψεων ,το ενδιαφέρον τους και για τη σημαντική βοήθεια τους σε όλα τα στάδια της έρευνας.

Τέλος ένα μεγάλο ευχαριστώ στην οικογένειά μου για την αμέριστη συμπαράστασή που μου παρείχε όλα αυτά τα χρόνια.

Περίληψη

Αντικείμενο της παρούσας διδακτορικής διατριβής αποτελεί η ανάπτυξη ενός γενικού πλαισίου λειτουργικότητας επιτήρησης χώρων. Το γενικό αυτό πλαίσιο περιλαμβάνει την χρήση ακουστικών αισθητήρων για την αναγνώριση και κατηγοριοποίηση των απειλών ενώ ταυτόχρονα παρέχει ένα ολοκληρωμένο πλαίσιο ασφαλείας των ίδιων των κόμβων. Η βασική πλατφόρμα εφαρμογής του συγκεκριμένου πλαισίου λειτουργικότητας είναι τα ασύρματα δίκτυα αισθητήρων, οπότε και η ανάπτυξή του έχει γίνει με στόχο την ικανοποίηση των ιδιαίτερων απαιτήσεων τους, όπως οι χαμηλές υπολογιστικές δυνατότητες που έχουν καθώς και η χαμηλή διαθεσιμότητα ενέργειά τους.

Οι βασικές λειτουργίες ενός συστήματος ασφάλειας χώρων είναι ο έγκαιρος και ασφαλής εντοπισμός πιθανών απειλών αυτού. Το σύστημα θα πρέπει να είναι ικανό να ανιχνεύει, αναγνωρίζει και κατηγοριοποιεί έγκαιρα τις πιθανές απειλές που θα εμφανιστούν. Η αποτελεσματικότητα ενός τέτοιο συστήματος έγκειται στον έγκαιρο εντοπισμό μιας απειλής σε απόσταση ασφαλείας, πριν αυτή γίνει εξαιρετικά επικίνδυνη για την ασφάλεια του χώρου.

Η ανάπτυξη εφαρμογών επιτήρησης χώρων, όπως συνόρων και μεγάλων εγκαταστάσεων, αποτελούν πρόκληση, καθώς το πεδίο εφαρμογής τους πολλές φορές δεν είναι φιλόξενο και δεν παρέχονται οι απαραίτητες υποδομές. Για παράδειγμα, η ύπαρξη μόνιμης πηγής ενέργειας δεν είναι πάντοτε αυτονόητη σε αυτούς του χώρους. Το πλαίσιο λειτουργιών που περιγράφεται στην συγκεκριμένη διατριβή αντιμετωπίζει αποτελεσματικά αυτούς τους περιορισμούς μέσω της χρήσης ασύρματων δικτύων αισθητήρων.

Με τον όρο ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network) εννοούμε ένα σύνολο μικροηλεκτρονικών συσκευών με δυνατότητες κατόπτευσης και συλλογής πληροφοριών περί των συνθηκών του κείμενου περιβάλλοντος. Διαθέτουν ικανότητες επεξεργασίας αποθήκευσης και ανταλλαγής δεδομένων, διαμέσου της διασύνδεσής τους σε δίκτυο με αυτόνομο, κατανεμημένο και κλιμακούμενο τρόπο, πάνω από ένα ασύρματο κανάλι επικοινωνίας. Στην συγκεκριμένη περίπτωση οι αισθητήρες που φέρουν οι ασύρματοι κόμβοι του δικτύου αφορούν την καταγραφή των ακουστικών κυμάτων, αλλά και διάφορων περιβαλλοντικών συνθηκών όπως είναι: η θερμοκρασία, η σχετική υγρασία, η ατμοσφαιρική πίεση αλλά και η ταχύτητα και κατεύθυνση του ανέμου.

Στο πλαίσιο της συγκεκριμένης διατριβής, αρχικά γίνεται μια αναλυτική περιγραφή της φυσιολογίας των ακουστικών κυμάτων καθώς και των επιπτώσεων που έχουν οι περιβαλλοντικές συνθήκες στον τρόπο διάδοσής τους. Η μορφή του ακουστικού κύματος καθώς και ο τρόπος διάδοσής του παίζει καθοριστικό ρόλο στον ακριβή εντοπισμό και χαρακτηρισμό της πηγής του κύματος.

Συγκεκριμένα, όσων αφορά την ανίχνευση μιας απειλής με την χρήση των ακουστικών κυμάτων που αυτή παράγει, αρχικά γίνεται μια πλήρη αναφορά στην ύπαρξη παρόμοιων μεθόδων ανίχνευση απειλών ενώ ταυτόχρονα τονίζονται οι όποιες αδυναμίες αυτές έχουν. Έπειτα παρουσιάζεται μια αναλυτική περιγραφή των μεθόδων που αναπτύχτηκαν στα πλαίσια αυτής της διατριβής. Η ανάπτυξή τους λαμβάνει υπόψη τις ιδιαιτερότητες του πεδίου εφαρμογή, καθώς και τις ιδιαιτερότητες των ίδιων των ασύρματων κόμβων. Οι προτεινόμενες μέθοδοι εντοπισμού των απειλών δοκιμάζονται σε περιβάλλον προσημείωσης καθώς σε πραγματικούς κόμβους, τους Mica2. Οι τεχνικές

εξοικονόμησης ενέργειας που χρησιμοποιήθηκαν για την ανάπτυξή τους προσφέρουν μία αποδοτική διαχείριση των πόρων των ασύρματων κόμβων βελτιώνοντας τους έτσι την μέγιστη διάρκεια λειτουργίας τους σε ποσοστό 80%.

Στον τομέα της κατηγοριοποίησης των απειλών με χρήση των ακουστικών κυμάτων που αυτές παράγουν, αναπτύχθηκε ένα σύνολο μεθόδων το οποίο κάνει χρήση απλών ευρετικών κανόνων αλλά και πολύπλοκών μαθηματικών υπολογισμών προκειμένου να αναγνωρίσει με ακρίβεια τον τύπο της απειλής. Το σύνολο των μεθόδων κατηγοριοποίησης στοχεύει στην αναγνώριση 3 κύριων τύπων: του ανθρώπινου βηματισμού, των εκρήξεων, και των διάφορων τύπων οχημάτων (όπως είναι τα αυτοκίνητα, τα φορτηγά κλπ…). Η αποδοτικότητα των μεθόδων κατηγοριοποίησης ελέγχτηκε σε περιβάλλον προσομοίωσης αλλά και σε πραγματικές συνθήκες. Τέλος η ανάπτυξή τους προσαρμόστηκε στις απαιτήσεις των ασύρματων κόμβων Mica2 παρέχοντάς τους έτσι μια βελτιωμένη διαχείριση των ενεργειακών τους πόρων.

Τέλος, ιδιαίτερη προσοχή δόθηκε στην ασφάλεια των ίδιων των ασύρματων κόμβων. Σημαντικό ρόλο στην δημιουργία ενός αποτελεσματικού συστήματος επιτήρησης χώρων αποτελεί και η διαφύλαξη του ίδιου του συστήματος από εχθρικούς ή κακόβουλους χρήστες. Όπως αναφέραμε παραπάνω, το σύστημα θα βασίζεται στην χρήση κόμβων που θα βρίσκονται διάχυτοι στον χώρο και πάνω στις στολές των στρατιωτών και θα επικοινωνούν ασύρματα δημιουργώντας ένα ασύρματο δίκτυο αισθητήρων. Αυτή η ενσωμάτωση των κόμβων στον , προς επιτήρηση, χώρο έχει σαν αποτέλεσμα οι κόμβοι να είναι εύκολα προσβάσιμοι από εχθρικούς ή κακόβουλους χρήστες οι οποίοι μπορούν να αποκτήσουν πρόσβαση στο σύστημα και να επηρεάσουν ή να αλλάξουν τις μετρήσεις, την ακρίβεια των μετρήσεων καθώς και την εύρυθμη λειτουργία ολόκληρου του συστήματος. Η διαφύλαξη της ακεραιότητας των κόμβων αλλά και της ασφάλειάς των μετρήσεών τους εξασφαλίζεται με την ανάπτυξη και χρήση ενός πλαισίου λειτουργιών το οποίο κάνει χρήση ειδικών αλγορίθμων κρυπτογραφίας και τεχνικών ασφάλειας. Στην περίπτωση που κάποιο μη-εξουσιοδοτημένο πρόσωπο καταφέρει και αποκτήσει πρόσβαση υπάρχει μηχανισμός έγκαιρης ειδοποίησης για την αποφυγής λήψης αλλοιωμένων μετρήσεων και την έκδοση λάθος συμπερασμάτων από το σύστημα. Το πλαίσιο αυτό έχει αναπτυχτεί με γνώμονα την παροχή λειτουργιών ασφαλείας, εφαρμόζοντας παράλληλα μια αποδοτική ενεργειακά πολιτική για την διαχείριση των πόρων των ασύρματων κόμβων.

Abstract

The subject of this Doctoral Thesis is to develop a general surveillance framework. This framework is based on manipulation of acoustic signals in order to detect and recognize threats. Also, this framework offers security functionalities. As, a key role on this framework plays a Wireless Sensors Network , its development is in accordance with network's limitation and demands.

The main functionality of a surveillance system is the early detection of potential threats. The system should be able to detect, identify and classify potential threats in time to appear. The effectiveness of such a system lies in early detection of a threat at a safe distance, before they become extremely dangerous for the security of the site.

Surveillance application development, such as borders and large installations are challenging because their scope is often not welcoming and not provided the necessary infrastructure. For example, the existence of a permanent energy source is not always obvious in these spaces. The framework's functionality described in this thesis effectively addresses these limitations through the use of wireless sensor networks.

A Wireless Sensor Network could be described as a set of microelectronic devices with potential sighting and collection of environmental conditions. These nodes have processing capabilities while are able to storage and exchange data through the interconnection network of autonomous, distributed and scalable manner over a wireless communication channel. In this case, the sensors have wireless nodes for recording of acoustic waves, and various environmental conditions such as: temperature, relative humidity, atmospheric pressure and speed and wind direction. In the context of this thesis, wireless nodes have attached sensors capable to monitor acoustic signals and environmental conditions, such as temperature, humidity, atmospheric pressure and wind speed and direction.

Within this thesis, first an analytic description of the physiology of acoustic waves and the impact of environmental conditions on their propagation is presented. The shape of the acoustic wave and its propagation way plays a crucial role in the accuracy of source identification and characterization.

Specifically, what concerns the detection of threat, a full report on the existence of such threat detection methods is presented, while highlighted any weaknesses they have. Then, a detailed description of the methods being developed in this thesis. Their development takes into account the specificities of field conditions and characteristics of the wireless nodes themselves. The proposed methods are tested to simulation environments and real nodes, the Mica2. The energy saving techniques used for their development offer an efficient management of wireless nodes, improving them the maximum duration of 80%.

What concerns the categorization of threats using their acoustic waves developed a set of methods which make use of simple heuristic rules and complex mathematical calculations to accurately identify the type of threat. The classification method aims to identify 3 main types: human footstep, explosions, and various types of vehicles (such as cars, trucks, etc ...). The efficiency of categorization methods are tested to simulation environment and field conditions. Finally, the development adapted to the requirements of wireless nodes Mica2 thus giving them an improved management of their energy resources.

Finally, special attention was paid to the security of wireless nodes themselves. Important role in creating an effective surveillance system is preservation of the system itself from hostile or malicious users. As mentioned above, the system is based on the use of nodes that are diffuse in space and on soldiers uniforms while these are communicating wirelessly, creating a wireless sensor network. This nodes integration in space made nodes easily accessible by hostile or malicious users who can access the system and affect or change the measurements, the accuracy of measurements and the proper operation of the whole system. The nodes and data prevention is ensured by the development of a security framework which makes use of specific cryptographic algorithms and security techniques

Πίνακας περιεχομένων

Ευρετήριο Εικόνων

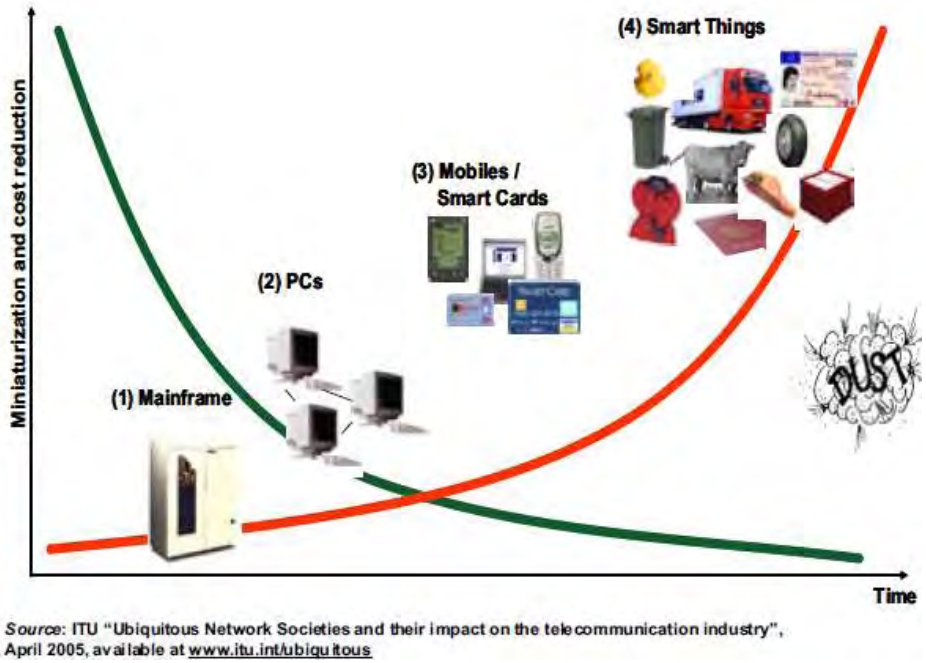
Ευρετήριο Πινάκων

1 ΕΙΣΑΓΩΓΗ

1.1 Μια νέα εποχή

Βρισκόμαστε στην αρχή μιας νέας πανταχού παρούσας υπολογιστικής (ubiquitous computing) και επικοινωνιακής εποχής, μιας εποχής που θα μεταμορφώσει ριζικά όλες τις πτυχές της καθημερινής μας ζωής. Σχεδόν δύο δεκαετίες πριν, ο Mark Weiser σε ένα άρθρο του στο Scientific American περιγράφει το όραμά του για το μέλλον του διάχυτου υπολογισμού, σαν την συνεχή αύξηση της υπολογιστικής ισχύος η οποία όμως θα συνοδεύεται από την συνεχή μείωση του μεγέθους του συστήματος που την προσφέρει. Επισημάνει ότι «οι πιο επιτυχημένες τεχνολογίες είναι αυτές που εξαφανίζονται… είναι αυτές, δηλαδή, που γίνονται αναπόσπαστο κομμάτι τις καθημερινής ζωής σε τέτοιο σημείο όπου τελικά είναι δύσκολο να τις διαφοροποιήσεις.» [1][2]

Οι προβλέψεις του, επιβεβαιώνονται και μάλιστα σε βαθμό, που ξεπερνά κατά πολύ τις αρχικές του εκτιμήσεις. Η ενσωμάτωση ασύρματων πομποδεκτών σε ένα μεγάλο εύρος συσκευών καθημερινής χρήσης, επιτρέπει την νέες μορφές επικοινωνίας ανάμεσα στους ανθρώπους και στα αντικείμενα, αλλά και μεταξύ των ίδιων των αντικειμένων. Αυτές οι νέες μορφές επικοινωνίας συμβάλουν στην δημιουργία ενός έξυπνου και αλληλεπιδραστικού περιβάλλοντος, το λεγόμενο Διαδίκτυο των Αντικειμένων (Internet of Things) [2][3]



Εικόνα 1: Το Διαδίκτυο των Αντικειμένων (Internet of Things)

Το Διαδίκτυο των Αντικειμένων αποτελεί μία από τις σημαντικότερες τεχνολογικές εξελίξεις των επόμενων ετών. Μπορεί να οριστεί ως: «Μια δυναμική παγκόσμια δικτυακή υποδομή με την ικανότητα να λειτουργεί σύμφωνα με πρότυπα και δυαλειτουργικά τηλεπικοινωνιακά πρωτόκολλα. Τα φυσικά και εικονικά αντικείμενα, που επικοινωνούν με την δομή αυτή, έχουν ταυτότητα, φυσικά χαρακτηριστικά και εικονικές προσωπικότητες, χρησιμοποιούν έξυπνες διεπαφές και είναι αδιάλειπτα ενσωματωμένα στο δίκτυο πληροφοριών» [4]

Χρησιμοποιώντας το Διαδίκτυο των Αντικειμένων, τα έξυπνα αντικείμενα συμμετέχουν ενεργά στις επιχειρησιακές, πληροφοριακές και κοινωνικές διεργασίες όπου μπορούν να αλληλεπιδρούν και να επικοινωνούν μεταξύ τους, αλλά και με το περιβάλλον, ανταλλάσοντας δεδομένα και πληροφορίες που έχουν λάβει από το γύρω περιβάλλον τους. Ακόμα μπορούν να αντιδρούν αυτόνομα σε πραγματικά ή εικονικά γεγονότα και να τα επηρεάζουν εκτελώντας κατάλληλες διεργασίες ακόμα και χωρίς την οποιαδήποτε ανθρώπινη παρέμβαση.

Τα έξυπνα αντικείμενα είναι μικρές συσκευές εφοδιασμένες με ένα ή περισσότερα αισθητήρια όργανα, ενεργοποιητές (actuators) και διαφόρων τύπων συσκευές επικοινωνίας, όπως είναι οι πομποδέκτες που χρησιμοποιούν πρωτόκολλα ZigBee. Αυτές οι συσκευές είναι ικανές να «αισθάνονται» μεγάλο πλήθος παραμέτρων και να επικοινωνούν με άλλες συσκευές. Πρόκειται για κινητές συσκευές οι οποίες τροφοδοτούνται από μπαταρία, και συνήθως αποτελούνται από τρία μέρη:

- την CPU , συνήθως πρόκειται για έναν μικρο-ελεγκτής 8, 16 ή 32-bit
- την μνήμη , το μέγεθος της συνήθως είναι μερικές δεκάδες kilobytes
- μια χαμηλής κατανάλωσης ασύρματο πομποδέκτη, της οποίας η δυνατότητα επικοινωνίας κυμαίνεται από μερικά kilobits το δευτερόλεπτο σε μερικές εκατοντάδες kilobits το δευτερόλεπτο. [5][6]

Αυτές οι συσκευές μπορούν να επικοινωνούν μεταξύ τους και να συνεργάζονται δημιουργώντας έτσι ένα Ασύρματο Δίκτυο Αισθητήρων. Με τον όρο Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks ή WSN όπως θα αναφέρεται στο εξής χάριν συντομίας) εννοούμε ένα σύνολο μικροηλεκτρονικών συσκευών με δυνατότητες κατόπτευσης και συλλογής πληροφοριών περί των συνθηκών του κείμενου περιβάλλοντος. Διαθέτουν ικανότητες επεξεργασίας αποθήκευσης και ανταλλαγής δεδομένων, διαμέσου της διασύνδεσής τους σε δίκτυο με αυτόνομο, κατανεμημένο και κλιμακούμενο τρόπο, πάνω από ένα ασύρματο κανάλι επικοινωνίας.

Η ταχύτατη ανάπτυξη της μικροηλεκτρονικής και των υλικών επέτρεψε την κατασκευή πολύ μικρών αισθητήρων, οι οποίοι έχουν την ικανότητα να μετρούν και να καταγράφουν μια κυριολεκτικά ατέλειωτη σειρά από περιβαλλοντολογικά ή βιολογικά μεγέθη, όπως τη θερμοκρασία, την ατμοσφαιρική πίεση, την υγρασία, τη φωτεινότητα, τη στάθμη υδάτων, την ωρίμανση καρπών, την ανίχνευση χημικών στοιχείων, την πίεση αίματος, τους σφυγμούς καρδιάς, την κίνηση αντικειμένων και ανθρώπων και πολλές ακόμα παραμέτρους που προστίθενται διαρκώς στον παραπάνω κατάλογο. Αξιοσημείωτο είναι ότι σε μία διάταξη ίση με ένα νόμισμα 2 ευρώ μπορούμε να συμπεριλάβουμε πολλά από τα παραπάνω αισθητήρια και να καταμετρούμε συγχρόνως διάφορα μεγέθη.

Παράλληλα, ανάλογη πρόοδος συντελέστηκε και στη σχεδίαση και υλοποίηση ειδικών πομποδεκτών που επιτρέπουν την αποτελεσματική διασύνδεση των διατάξεων μεταξύ τους και με την κεντρική μονάδα με τεχνολογίες ασύρματης δικτύωσης,

αξιολογημένες στα παγκόσμια δίκτυα κινητών επικοινωνιών. Το χαμηλό κόστος παραγωγής παρέχει τη δυνατότητα εγκατάστασης πολύ μεγάλων δικτύων με εκατοντάδες ή χιλιάδες στοιχεία με προηγμένο λογισμικό και ικανότητα να αυτοοργανώνονται, να βελτιστοποιούν και να διασφαλίζουν τη λειτουργία τους χωρίς ιδιαίτερη συντήρηση για μεγάλο χρονικό διάστημα.[7-12]

Το μεγάλο πλήθος των πλεονεκτημάτων , έναντι άλλων τεχνολογιών, καθώς και η ευελιξία και η ευκολία χρήσης των WSN συντελούν στην ανάπτυξη πλήθους εφαρμογών. Μερικές από τις πιο σημαντικές εφαρμογές είναι:

- Η παρατήρηση των ατμοσφαιρικών και μετεωρολογικών συνθηκών με μεγάλη ακρίβεια.
- Η επιτήρηση δασών, υδροβιότοπων, θερμοκηπίων και γενικά αγροτικών καλλιεργειών για έλεγχο υγρασίας, θερμοκρασίας, πίεσης, ωρίμανσης καρπών, κτλ.,
- Η επιτήρηση υγρών στοιχείων για ρύπους ή έλεγχο ακραίων φαινομένων όπως οι πλημμύρες.
- Η επιτήρηση βιομηχανικού περιβάλλοντος για την εξασφάλιση επιθυμητών συνθηκών της παραγωγικής διαδικασίας.
- Στοιχειώδεις ρυθμίσεις λειτουργιών σε κτίρια όπως θέρμανση, φωτισμός, συναγερμοί.

Ακόμα θα πρέπει να σημειωθεί ότι η τεχνολογία των WSN είναι ιδιαίτερα αποδοτική σε εφαρμογές φυσικής ασφάλειας χώρων όπως είναι:

- Τα στρατιωτικά Δίκτυα Αισθητήρων για την ανίχνευση και την λήψη όσο το δυνατόν περισσότερων πληροφοριών για τις εχθρικές κινήσεις, τις εκρήξεις, και άλλα φαινόμενα ενδιαφέροντος.
- Η εφαρμογή των Ασύρματων Δικτύων Αισθητήρων για την επιτήρηση για την παροχή ασφάλειας σε αεροδρόμια, βιομηχανικές περιοχές, εμπορικά πολυκαταστήματα, χώρους στάθμευσης, και άλλες εγκαταστάσεις.
- Η χρήση των Ασύρματων Δικτύων Αισθητήρων για την ασφαλή επιτήρηση των συνόρων μιας χώρας
- Η εφαρμογή των Ασύρματων Δικτύων Αισθητήρων στην παρακολούθηση οχημάτων

Τα ιδιαίτερα χαρακτηριστικά των Ασύρματων Δικτύων Αισθητήρων τα καθιστούν ιδανικά για την υλοποίηση ενός εύχρηστου συστήματος εντοπισμού εισβολέων, που μπορεί να χρησιμοποιηθεί σε εφαρμογές ασφάλειας [13]. Τα τελευταία χρόνια έχει υπάρξει ένα μεγάλο πλήθος ερευνητικών και εμπορικών προσπαθειών που έχουν σαν σκοπό την χρήση των Ασύρματων Δικτύων Αισθητήρων για την κατασκευή αποτελεσματικών συστημάτων ασφάλειας χώρων.

1.2 Ανασκόπηση λύσεων ασφάλειας χώρων με την χρήσης Ασύρματων Δικτύων Αισθητήρων.

Οι βασικές λειτουργίες ενός συστήματος ασφάλειας χώρων είναι ο έγκαιρος και ασφαλής εντοπισμός πιθανών απειλών αυτού. Το σύστημα θα πρέπει να είναι ικανό να ανιχνεύει, αναγνωρίζει και κατηγοριοποιεί έγκαιρα τις πιθανές απειλές που θα

εμφανιστούν. Η αποτελεσματικότητα ενός τέτοιο συστήματος έγκειται στον έγκαιρο εντοπισμό μιας απειλής σε απόσταση ασφαλείας, πριν αυτή γίνει εξαιρετικά επικίνδυνη για την ασφάλεια του χώρου.

Για την υλοποίηση συστημάτων επιτήρησης χώρου έχουν χρησιμοποιηθεί διάφοροι τύποι αισθητήρων, όπως είναι ακουστικοί και σεισμικοί αισθητήρες, οι οπτικοί αισθητήρες, υπέρυθροι και μαγνητικοί αισθητήρες, αλλά και συστήματα ραντάρ. Οι αισθητήρες αυτοί μπορούν να χρησιμοποιηθούν, από ένα σύστημα, είτε μόνοι τους, είτε σε συνδυασμό με άλλους τύπους αισθητήρων ώστε να δώσουν καλύτερα και πιο ακριβή αποτελέσματα.

Παρακάτω ακολουθεί, μια σύνοψη των συστημάτων, αλλά και των αισθητήρων που χρησιμοποιούν.

Οι ερευνητές στα [14-16] αρχικά κάνουν μια εκτενή μελέτη στους διάφορους διαθέσιμους τύπους αισθητήρων και στις ιδιότητες τους. Έπειτα καταλήγουνε στην χρήση των μαγνητικών αισθητήρων και ραντάρ. Ο λόγος της επιλογής τους αυτής είναι ότι οι συγκεκριμένοι τύποι αισθητήρων δεν χρειάζονται ιδιαίτερη συσκευασία, έχουν λογικές απαιτήσεις σε επεξεργασία ισχύ και έχουν παρουσιάζουν μεγάλη αποτελεσματικότητα καθώς έχουν χρησιμοποιηθεί ευρέως και επιτυχώς σε παλαιότερες εφαρμογές. Σε παρόμοιές εργασίες το ραντάρ αντικαθίσταται από χαμηλότερου κόστους λύσεις, όπως υπέρυθρους και ακουστικούς αισθητήρες [17],[18] ή παραμένουν μόνο οι μαγνητικοί και οι ακουστικοί [19].

Πολύ διαδομένη είναι επίσης η χρήση των υπέρυθρών αισθητήρων. Χρησιμοποιούνται συνήθως σε συνδυασμό με άλλους τύπους αισθητήρων, όπως είναι οι ακουστικοί και οι σεισμικοί.[20] Στην εργασία [21] οι συγγραφείς περιγράφουν την υλοποίηση του συστήματος VIPER. Πρόκειται για ένα σύστημα, το οποίο χρησιμοποίει υπέρυθρη κάμερα για τον εντοπισμό της λάμψης που δημιουργείται κατά την διάρκεια της εκπυρσοκρότησης ενός όπλου. Επιπλέον ένας ακουστικός αισθητήρας χρησιμοποιείται για τον εντοπισμό του ήχου που δημιουργείται κατά την εκπυρσοκρότηση ενός όπλου με σκοπό να γίνει υπολογισμός της απόστασης του συστήματός από την εκπυρσοκρότηση. Το μειονέκτημα του συγκεκριμένου συστήματος είναι η απαίτηση των αισθητήρων για ύπαρξη οπτικής επαφής με το σημείο της εκπυρσοκρότησης.[22]

Ο πιο διαδεδομένος συνδυασμός αισθητήρων, που επιτρέπει την αξιόπιστη αλλά και οικονομική ανίχνευση τόσο προσωπικού όσο και οχημάτων, παρέχοντας πληροφορίες για τη φύση του στόχου, για την κατεύθυνση κίνησης και την ταχύτητά του, είναι η χρήση ακουστικών ή/και σεισμικών αισθητήρων [8]. Οι ακουστικοί αισθητήρες αποτελούν την κυρίαρχη τεχνολογική λύση για τον εντοπισμό πυροβολισμών. Τοποθετούνται σε σταθερά σημεία (π.χ. οροφές κτηρίων) για την επιτήρηση ενός πεδίου μάχης, είτε σε οχήματα ώστε να συμβάλουν στην επιχειρησιακή αποτελεσματικότητα των φρουρών/στρατιωτικών.

Πλήθος εμπορικών [23-29] και ερευνητικών συστημάτων [34-36] τα οποία βασίζονται είτε σε ακουστικούς είτε σε σεισμικούς αισθητήρες, είτε σε συνδυασμό αυτών έχουν κατασκευαστεί. Τα συστήματα Pilar (κατασκευασμένο από τον στρατό των ΗΠΑ)[25] , SADS (Sniper Acoustic Detection Sensor, κατασκευασμένο από την εταιρεία Rafael)[26] και Boomerang (κατασκευασμένο από την εταιρεία BBN Technologies) [27] αποτελούν μικρού μεγέθους και εμβέλειας λύσεις για τον εντοπισμό της θέσης ελεύθερων σκοπευτών. Τα συστήματα ARTILOC (Artillery Location Acoustic System, κατασκευασμένο από τον εταιρεία Rafael)[28] και HALO (κατασκευασμένο από την

εταιρεία BAE System)[29] προορίζονται για την επιτήρηση μεγάλων περιοχών (έκτασης μέχρι 2000 τετραγωνικών χιλιομέτρων). Τα 2 αυτά συστήματα είναι αποτελεσματικά τόσο στον εντοπισμό του σημείου εκπυρσοκρότησης πυροβόλων όπλων (mortars and artillery fire) όσο και στον εντοπισμό του σημείου πρόσκρουσης της οβίδας.

Πολύ συχνός είναι ο συνδυασμός των ακουστικών αισθητήρων με άλλου τύπου αισθητήρων για την κατασκευή συστημάτων παρακολουθήσεις πεδίων μάχης. Το σύστημα REMBASS II (Remotely Monitored Battlefield Sensor Systems)[30] χρησιμοποιεί σεισμικούς, υπέρυθρους και μαγνητικούς αισθητήρες με σκοπό την παρακολούθηση μικρών χώρων (μικρότερους από 350 μέτρα).

Ακόμα τα συστήματα που χρησιμοποιούν ακουστικούς αισθητήρες μπορούν να χρησιμοποιηθούν σαν λύσεις για την εναέρια επιτήρηση. Το σύστημα RAFAEL Helispot [31] επιτυγχάνει πολύ καλή επίδοση στον εντοπισμό των ελικοπτέρων που πετάνε σε χαμηλό ύψος σε απόσταση μερικών χιλιομέτρων από το σύστημα, χωρίς την ύπαρξη οπτικής επαφής. Ο εντοπισμός και η πρόβλεψη της πορείας ενός αεροπλάνου μπορεί να επιτευχτεί με την χρήση ακουστικών αισθητήρων και πολύπλοκες διεργασίες επεξεργασίας σήματος. Τα τελευταία χρόνια, έχουν κατασκευαστεί μεγάλα δίκτυα παθητικών ακουστικών αισθητήρων για την παρακολούθηση αεροπλάνων, επιδεικνύοντας μεγάλη αποτελεσματικότητα, καθώς καταφέρνουν και αναλύουν αποτελεσματικά όλα τα φυσικά φαινόμενα (π.χ. Doppler) που οφείλονται ακουστική ακτινοβολία.

Παράλληλα, τα τελευταία χρόνια γίνονται πολλές έρευνες για την μείωση του μεγέθους των αισθητήρων ώστε να είναι δυνατή η ενσωμάτωσή τους ακόμα και στις στολές των στρατιωτών. Το [32] περιγράφει ένα σύστημα όπου οι ακουστικοί αισθητήρες θα είναι ενσωματωμένοι στο κράνος των στρατιωτών. Το ερευνητικό πρόγραμμα NEST (χρηματοδοτούμενο από το US DARPA)[33] αναπτύσσει ένα ακουστικό σύστημα επιτήρησης χώρων, στο οποίο οι αισθητήρες θα αποτελούν ένα μεγάλο κατανεμημένο δίκτυο.

Εικόνα 2: Εικόνες ακουστικών αισθητήρων συστημάτων επιτήρησης χώρων [155]

1.3 Αντικείμενο της διατριβής

Στην προηγούμενη παράγραφο παρουσιάστηκαν συστήματα τα οποία λύνουν το πρόβλημα επιτήρησης ενός χώρου. Κάθε ένα από τα συστήματα αυτά χρησιμοποιεί διαφορετικούς τύπους αισθητήρων και τεχνικών επεξεργασίας των δεδομένων ώστε να δημιουργήσει ένα σύστημα ικανό να εντοπίζει την ύπαρξη απειλών, όπως είναι η ύπαρξη ανθρώπων και οχημάτων. Τα συστήματα αυτά παρόλη την αποτελεσματικότητα τους στον εντοπισμό απειλών σε έναν χώρο, χαρακτηρίζονται από την χρήση ισχυρού υπολογιστικού συστήματος ικανού να συλλέγει και να επεξεργάζεται ταχύτατα μεγάλο όγκο δεδομένων, χωρίς κανένα ενεργειακό περιορισμό. [38][39] Τα συστήματα αυτά βασίζονται σε μεθόδους επεξεργασίας σήματος, οι οποία έχουν μεγάλες απαιτήσεις σε επεξεργαστική ισχύ, σε μνήμη, σε ενέργεια και στην ύπαρξη γρήγορης ασύρματης επικοινωνίας. Αυτό έχει σαν αποτέλεσμα την δημιουργία συστημάτων μεγάλου μεγέθους και με μεγάλες ενεργειακές απαιτήσεις, κάτι το οποίο τα εμποδίζει από την άμεση και γρήγορη τοποθέτηση τους, το οποίο πολλές φορές είναι ζωτικής σημασίας στο πεδίο της μάχης. Επιπλέον κανένα από τα παραπάνω συστήματα δεν δίνει έμφαση στην διαφύλαξη των συσκευών από εχθρικούς χρήστες. Οι συσκευές είναι εύκολα προσβάσιμες από εχθρικούς ή κακόβουλους χρήστες οι οποίο μπορούν να αποκτήσουν πρόσβαση στο σύστημα και να επηρεάσουν ή να αλλάξουν τις μετρήσεις, την ακρίβεια των μετρήσεων καθώς και την εύρυθμη λειτουργία ολόκληρου του συστήματος με συνέπεια την μείωση της αποτελεσματικότητας του.

Στην συγκεκριμένη διατριβή περιγράφεται ένα σύστημα επιτήρησης χώρου το οποίο χρησιμοποίει ακουστικούς αισθητήρες. Οι ακουστικοί αισθητήρες είναι ενσωματωμένοι σε ασύρματους κόμβους, οι οποίοι επικοινωνούν μεταξύ τους δημιουργώντας ένα Ασύρματο Δίκτυο Αισθητήρων. Οι ασύρματοι κόμβοι είναι μικροί σε μέγεθος ώστε να είναι εφικτή η τοποθέτησή τους πάνω στις στολές των στρατιωτών. Χρησιμοποιούνται μέθοδοι εντοπισμού και αναγνώρισης απειλών, οι οποίοι διακρίνονται για την χαμηλή πολυπλοκότητα τους, τις χαμηλές τους απαιτήσεις σε υπολογιστή ισχύ και ενέργεια, αλλά και την υψηλή τους αποτελεσματικότητα. Οι χαμηλές απαιτήσεις των μεθόδων αυτών, τις κάνει ικανές να υλοποιηθούν από ένα Ασύρματο Δίκτυο Αισθητήρων το οποίο χαρακτηρίζεται από τους περιορισμούς των κόμβων στο μέγεθος, στην επεξεργαστική ικανότητα, στον αποθηκευτικό χώρο, στην διαθέσιμη ενέργεια, στην επικοινωνία (τοπολογία, εμβέλεια, ρυθμός μετάδοσης, εύρος ζώνης) και στο μέγεθος του κώδικα. Επιπλέον οι κόμβοι του Ασύρματου Δικτύου Αισθητήρων εκτελούν ειδικούς χαμηλών απαιτήσεων αλγορίθμους οι οποίο εξασφαλίζουν την ασφάλεια των κόμβων και των μετρήσεων από κάθε προσπάθεια πρόσβασης σε αυτούς μη εξουσιοδοτημένου προσώπου. Στην περίπτωση που κάποιο μη-εξουσιοδοτημένο πρόσωπο καταφέρει και αποκτήσει πρόσβαση υπάρχει μηχανισμός έγκαιρης ειδοποίησης για την αποφυγής λήψης αλλοιωμένων μετρήσεων και την έκδοση λάθος συμπερασμάτων από το σύστημα.

Το σύστημα χρησιμοποιεί ακουστικούς αισθητήρες καθώς αποτελούν ένα αποτελεσματικό μέσο για τον εντοπισμό και τον χαρακτηρισμό των απειλών σε έναν χώρο χωρίς την ανάγκη ύπαρξης οπτικής επαφής με την ίδια την απειλή. Πο συγκεκριμένα:

- Οι ακουστικοί αισθητήρες είναι συσκευές χαμηλού κόστους με δυνατότητα πρόβλεψης ακριβείας ακόμα και χωρίς την ύπαρξη οπτικής επαφής με την πηγή το ήχου.

- Οι ακουστικοί αισθητήρες προσφέρουν καλύτερα αποτελέσματα και πιο ασφαλής μετρήσεις σε σχέση με αισθητήρες, όπως οι οπτικοί και οι υπέρυθροι, οι οποίοι κάλυψη μόνο σε μια μικρή περιοχή γύρω από αυτούς και έχουν πρόβλημα στην περίπτωση μη ύπαρξης οπτικής επαφής με την πηγή.

Πίνακας 1: Σύγκριση διαφορετικού τύπου αισθητήρων για τον εντοπισμό απειλών σε υπο-παρακολούθηση χώρο [154].

	GPS	Οπτικοί	Μικροκύματα	Ακουστικοί
Ακρίβεια	Υψηλή ακρίβεια εντοπισμού σε εξωτερικό χώρο	Υψηλή ακρίβεια εντοπισμού σε εξωτερικό χώρο χωρίς εμπόδια	Χαμηλή ακρίβεια εντοπισμού σε εξωτερικό και εσωτερικό χώρο	Ικανοποιητική ακρίβεια εντοπισμού σε εξωτερικό και εσωτερικό χώρο
Ανάγκη τοποθέτησης υλικού στον υπο παρακολούθηση κόμβο	Απαιτείται η τοποθέτηση πομποδέκτη	Καμία ανάγκη τοποθέτησης	Απαιτείται μία απλή συσκευή	Καμία ανάγκη τοποθέτησης
Ανάγκη τοποθέτησης υλικού στον κόμβο αναφοράς	Καμία απαίτηση	Απαιτείται μια κάμερας υψηλής ευκρίνειας	Απαιτείται μία απλή συσκευή	Απαιτείται ένας ακουστικός αισθητήρας
Κόστος	Υψηλό	Υψηλό	Χαμηλό	Μέτριο
Πυκνότητα κόμβων αναφοράς	Χαμηλό	Υψηλή πυκνότητα κόμβων αναφοράς ώστε να καλύπτεται όλος ο υπο παρακολούθηση χώρος	Μέτριο	Μέτριο
Ευκολία τοποθέτησης	Εύκολη για εξωτερικούς χώρους	Δύσκολή δια εσωτερικούς χώρους	Εύκολη	Μέτρια
Κατανάλωση ενέργειας	Υψηλή	Υψηλή	Χαμηλή	Μέτρια

1.4 Οργάνωση του τόμου

Στα κεφάλαια που θα ακολουθήσουν θα αναλυθούν οι ανωτέρω αναφερθείσες έννοιες, οι οποίες είναι αναγκαίες για την κατανόηση της ανάλυσης της υλοποίηση της εφαρμογής.

Συγκεκριμένα, στο Κεφάλαιο 2 γίνεται μια πλήρες έρευνα σχετικά με την φυσιολογία των ακουστικών κυμάτων καθώς και την επίδραση που έχουν οι περιβαλλοντικές συνθήκες στον τρόπο διάδοσής της. Το Κεφάλαιο 3 περιέχει μια αναλυτική περιγραφή των ασύρματων δικτύων αισθητήρων. Παρουσιάζονται οι ιδιαίτερες απαιτήσεις που έχουν αλλά και οι περιορισμοί που εισάγουν στην υλοποίηση και εκτέλεση λειτουργιών. Στην συνέχεια, το Κεφάλαιο 4 περιγράφει του ασύρματους κόμβου που θα χρησιμοποιηθούν στην ανάπτυξη του συγκεκριμένου πλαισίου λειτουργιών. Δίνεται ιδιαίτερη σημασία στα αισθητήρια όργανα που φέρουν αυτοί οι κόμβοι καθώς και στην ακρίβεια των μετρήσεών τους. Το Κεφάλαιο 5 εισάγει ένα

πλαίσιο λειτουργιών ασφαλείας. Το πλαίσιο αυτό παρέχει λειτουργικότητα αυθεντικοποίησης και εγκυροποίησης των κόμβων καθώς και κρυπτογράφησης της ασύρματης επικοινωνίας τους. Έπειτα στο Κεφάλαιο 6, ακολουθεί μια αναλυτική περιγραφή των λειτουργιών που απαιτούνται για την ανίχνευση μιας απειλής και τον ακριβή εντοπισμό της θέσης της. Το Κεφάλαιο 7 περιγράφει τις λειτουργίες κατηγοριοποίησης των απειλών. Οι ασύρματοι κόμβοι χρησιμοποιούν διάφορες τεχνικές προκειμένου να αναγνωρίσουν με ακρίβεια τον τύπο της απειλής που εντόπισαν. Τέλος στο 7^{ο} Κεφάλαιο γίνεται μια περιγραφή του συνόλου των λειτουργιών που παρέχει το πλαίσιο. Ακόμα περιγράφεται η εφαρμογή του πλαισίου λειτουργιών σε πραγματικούς κόμβους Mica2 και η δοκιμή τους σε πραγματικές συνθήκες. Τα αποτελέσματα αυτών των δοκιμών καθώς και η ακρίβεια εντοπισμού της θέσης και αναγνώρισης του τύπου της απειλής παρουσιάζονται στο τέλος αυτού του κεφαλαίου.

2 Χαρακτηριστικά του ήχου

2.1 Χαρακτηριστικά διάδοσης του ήχου στον χώρο

Ο ήχος μπορεί να οριστεί σαν μια κυματική κίνηση στον αέρα ή σε άλλα ελαστικά μέσα, κατά την οποία οι μεταβολές της πίεσης των ηχητικών κυμάτων υπερτίθενται στην επικρατούσα ατμοσφαιρική πίεση. Ο ήχος παράγεται όταν μια ηχητική πηγή ταλαντώνεται , δηλαδή κάνει παλμικές κινήσεις. Οι παλμικές κινήσεις αναγκάζουν τα κοντινά μόρια του αέρα να κάνουν και αυτά παλμικές κινήσεις, δημιουργώντας πυκνώματα και αραιώματα. Πυκνώματα έχουμε όταν σε κάποια σημεία συγκεντρώνονται πολλά μόρια και αραιώματα όταν συγκεντρώνονται λίγα μόρια του αέρα. Τα μόρια του αέρα μεταφέρουν τον ήχο στο αυτί μας και αναγκάζουν τη μεμβράνη που λέγεται τύμπανο να πάλλεται.[39]

2.1.1 Ακουστική Πίεση

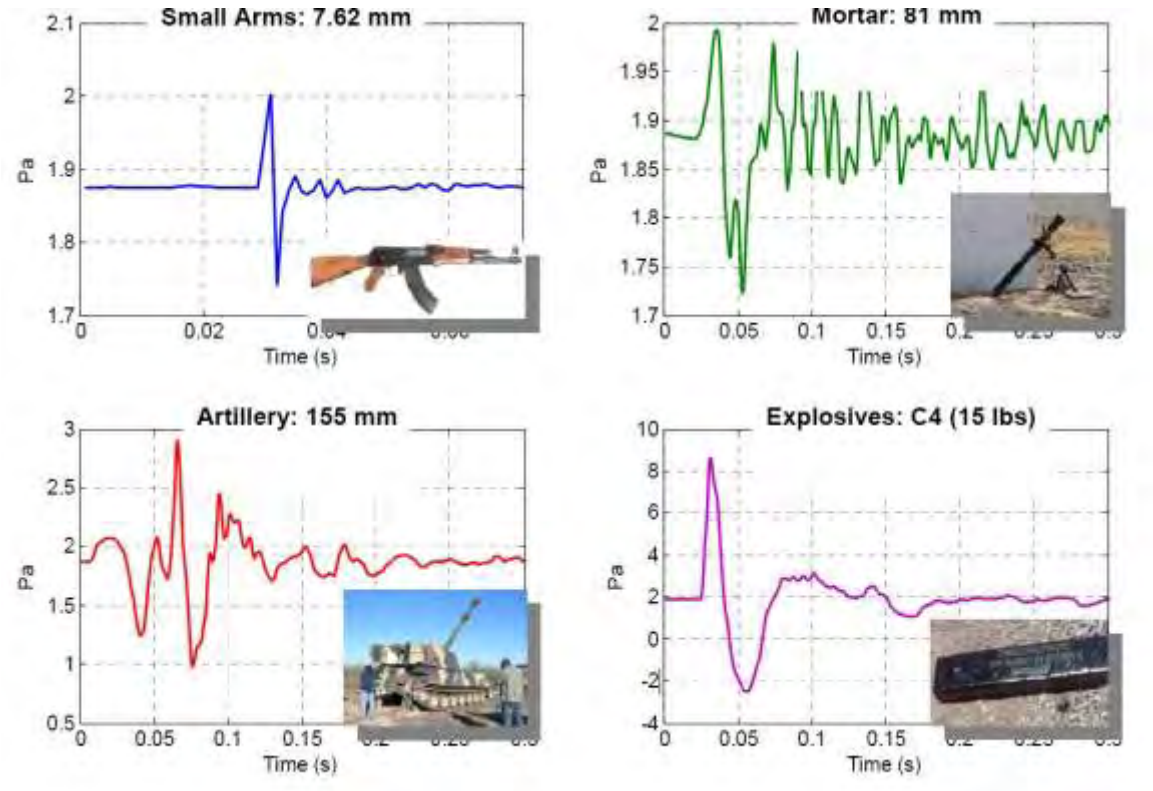
Η περιγραφή ενός ήχου μπορεί να γίνει από την μελέτη της ακουστικής πίεσης του. Σαν ακουστική πίεση ορίζεται η στιγμιαία μεταβολή της πίεσης των ηχητικών κυμάτων ως προς τη σταθερή πίεση του μέσου διάδοσης του κύματος (π.χ. αέρας). Οι τιμές τις ακουστικής πίεσης κυμαίνονται σε ένα μεγάλο εύρος τιμών, ανάλογα με το είδος της πηγής του ήχου. Στον παρακάτω πίνακα φαίνονται μερικά παραδείγματα ηχητικών πηγών και της αντίστοιχης ακουστικής πίεσης που δημιουργούν.

Πηγή ήχου	Πίεση ήχου (Pascal)	Στάθμη πίεσης ήχου (db)
Πύραυλος	200000	200
Πυραυλοκινητήρας	2000	160
Αεροσκάφος ελικοφόρο	200	140
Καρφωτικό εργαλείο	20	120
Βαρύ φορτηγό	2	100
Θορυβώδες γραφείο	0.2	80
Συζήτηση	0.02	60
Ήσυχη κατοικία	0.002	40
Θρόισμα φύλλων	0.0002	20

Πίνακας 2: Ηχητικές πηγές και οι αντίστοιχες πιέσεις ήχου που δημιουργούν

Η ακουστική πίεση ενός κύματος μπορεί να οριστεί και ως πλάτος του ηχητικού κύματος καθώς αναφέρεται στην διαφορά της πίεσης του ήχου από την πίεση του μέσο διάδοσης. Οι παραπάνω τιμές αναφέρονται σε μετρήσεις της ακουστικής πίεσης, που έχουν γίνει στην περιοχή της ακουστικής πηγής. Καθώς απομακρυνόμαστε από την ηχητική πηγή, το πλάτος του ηχητικού κύματος μειώνεται μέχρι τον πλήρη μηδενισμό του. Η μέγιστη απόσταση που μπορεί να διανύσει ένα κύμα, σε ιδανικές συνθήκες, μέχρι την πλήρη εξασθένισή του εξαρτάται από την ένταση I του ήχου. Σαν ένταση I του ήχου ορίζεται η μέση ροή ενέργειας ανά μονάδα επιφανείας κάθετης στην διεύθυνση διάδοσης. Είναι ανάλογη του τετραγώνου της πίεσης p και στην περίπτωση σφαιρικών κυμάτων απομακρυνόμενων από σημειακή πηγή μεταβάλλεται αντιστρόφως ανάλογα του τετραγώνου της απόστασης ($I \propto 1/r^2$, $p \propto 1/r$) [40]. Μία μέση τιμή της εξασθένισης του ηχητικού σήματος κατά την διάδοση του είναι: 6dB για κάθε διπλασιασμό της απόστασης ανάμεσα στην ηχητική πηγή και στον ακουστικό αισθητήρα.

Η μορφή του ηχητικού κύματος, γνωστή και ως ηχητική υπογραφή, που παράγει η κάθε διαφορετική ηχητική πηγή διαφέρει ως προς τις μεταβολές της ακουστικής πίεσης του στον χρόνο. Για παράδειγμα στις παρακάτω φωτογραφίες παρατηρούμε 4 διαφορετικές ηχητικές πηγές (4 διαφορετικά είδη όπλων) όπου η κάθε μια παράγει ένα χαρακτηριστικό ηχητικό κύμα διαφοροποιούμενο από όλα τα υπόλοιπα ως προς τις μεταβολές της ακουστικής πίεσης στον χρόνο.



Εικόνα 3: Χαρακτηριστικές μεταβολές πίεσης ηχητικών κυμάτων διαφορετικών ηχητικών πηγών [155].

Σε ιδανικό περιβάλλον χρησιμοποιώντας και μελετώντας την ιδιαίτερη μορφή του κάθε ηχητικού κύματος μπορούμε να εξάγουμε συμπεράσματα για τον τύπο της ηχητικής πηγής. Για την εξαγωγή συμπερασμάτων σε πραγματικό περιβάλλον χρειάζεται εκτός από την μελέτη της μορφής του ηχητικού κύματος να λάβουμε υπόψη και άλλες παραμέτρους οι οποίες επηρεάζουν σε μεγάλο βαθμό τον τρόπο διάδοσης ενός κύματος στον αέρα.

2.1.2 Επίδραση περιβαλλοντικών παραμέτρων στην διάδοση του ήχου

Οι ηχητικές υπογραφές επηρεάζονται σε μεγάλο βαθμό από τις περιβαλλοντικές συνθήκες, ιδιαίτερα το πεδίο των υψηλών συχνοτήτων των κυμάτων. Η επίδραση αυτή οφείλεται στον τρόπο διάδοσης των ηχητικών κυμάτων στον αέρα. Για παράδειγμα, κάτω από συγκεκριμένες περιβαλλοντικές συνθήκες αλλά και σε συγκεκριμένη απόσταση από τις ηχητικές πηγές, η εκπυρσοκρότηση μίας στρατιωτικής ρουκέτας μπορεί να έχει παρόμοιο ακουστική υπογραφή με αυτή μιας εκπυρσοκρότησης όπλου.

Καθώς μεταβάλλονται οι περιβαλλοντικές συνθήκες (συνθήκες του αέρα) επηρεάζονται διάφορες παράμετροι της διάδοσης του κύματος ,όπως είναι η ταχύτητα διάδοσης του. Ως ταχύτητα διάδοσης του ήχου ορίζεται η απόσταση που διανύει το ηχητικό κύμα σε ένα ελαστικό μέσο στην μονάδα του χρόνου. Η ταχύτητα του ήχου είναι ανάλογη με την περιβαλλοντική θερμοκρασία και υγρασία. Η μέση ταχύτητα του ήχου σε ξηρό αέρα (0% υγρασία αέρος), εκφρασμένη σε μέτρα το δευτερόλεπτο (m*s-1), και σε θερμοκρασία αέρα γύρω στους 0^oC, μπορεί να υπολογιστεί από τον τύπο:

$$c_{air} = \left(331.3 + \left(0.606°C^{-1} \cdot \vartheta\right)\right) m \cdot s^{-1} \quad (1)$$

όπου ϑ είναι η θερμοκρασία εκφρασμένη σε βαθμούς Celsius (^oC).
Η συγκεκριμένη συνάρτηση προκύπτει από τους 2 πρώτους όρους της σειράς Taylor της ακόλουθης πιο ακριβής/λεπτομερής συνάρτησης:

$$c_{air} = \left(331.3\, m \cdot s^{-1} \sqrt{1 + \frac{\vartheta}{273.15\,°C}}\right) \quad (2)$$

Επομένως, η ταχύτητα του ήχου σε ξηρό αέρα με θερμοκρασία στους 20^oC (68^oF) είναι 343.2 μέτρο το δευτερόλεπτο. Η τιμή της ταχύτητας του ήχου στους 0^oC θεωρούμε ότι είναι 331.3 m/s. Η εξαγωγή της ταχύτητας στους 0^oC βασίζεται σε μια σειρά από υποθέσεις και προσεγγίσεις, όπως είναι η υπόθεση ότι ο αέρας του περιβάλλοντος όταν βρίσκεται σε ατμοσφαιρική πίεση 1 atm έχει συμπεριφορά παρόμοια με αυτή ενός ιδανικού αερίου. Ανάλογα με τις υποθέσεις που παίρνουμε η ταχύτητα του ήχου στους 0^oC κυμαίνεται ανάμεσα σε 331.2 και 331.6 m/s. Ακόμα η χρήση του συγκεκριμένου τύπου για τον υπολογισμό της ταχύτητας του ήχου δεν λαμβάνει υπόψη την επίδραση των υδρατμών της ατμόσφαιρας, καθώς θεωρείται αμελητέα. Γενικά ο συγκεκριμένος τύπος υπολογίζει με μεγάλη ακρίβεια την ταχύτητα του ήχου όταν διαδίδεται σε σχετικά ξηρό, κρύο και χαμηλής πίεσης αέρα, όπως είναι η στρατόσφαιρα της Γης. Ο τύπος αποτυγχάνει στις περιπτώσεις ύπαρξης εξαιρετικά χαμηλής ατμοσφαιρικής πίεσης και μικρού μήκους κύματος του ήχου. Στην περίπτωση του μικρού μήκους κύματος η

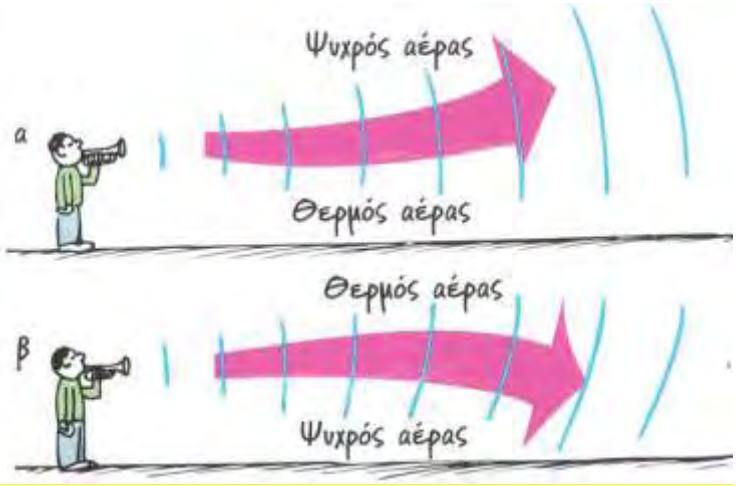
αποτυχία οφείλεται στην αρχική υπόθεση, ότι το μήκος κύματος του ήχου στον αέρα είναι πολύ μεγαλύτερο από την μέση απόσταση των μορίων του ίδιου του αερίου.

Η επίδραση των περιβαλλοντικών συνθηκών στην διάδοση του κύματος γίνεται αισθητή ακόμα και μερικά μέτρα (π.χ. 25 μέτρα) από την ηχητική πηγή, και αυξάνεται καθώς μειώνεται το ύψος του δέκτη του ηχητικού κύματος(π.χ. αυτί, ή ηχητικός αισθητήρας). Τα τρία πιο σημαντικά περιβαλλοντικά φαινόμενα που επηρεάζουν την διάδοση του κύματος είναι:

- Η διάθλαση
- Η σκέδαση από αναταράξεις
- Η ατμοσφαιρική απορρόφηση

2.1.2.1 Διάθλαση

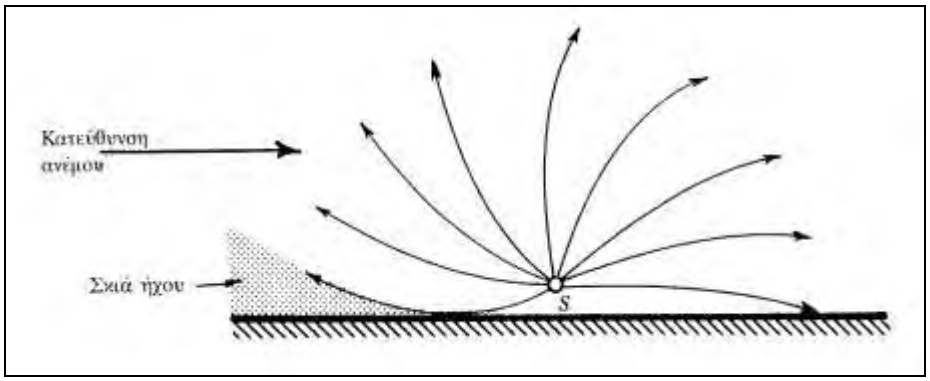
Η διάθλαση ενός ηχητικού κύματος ονομάζεται η «κάμψη» που παθαίνει το ηχητικό κύμα όταν τα διάφορα τμήματα των μετώπων του κύματος κινούνται με διαφορετικές ταχύτητες. Αυτό συμβαίνει όταν υπάρχουν μεταβλητοί άνεμοι ή όταν ο ήχος διαδίδεται σε αέρα με ανομοιόμορφη θερμοκρασία. Σε μία ζεστή ημέρα, ο αέρας κοντά στο έδαφος μπορεί να είναι σημαντικά θερμότερος από αυτό στα υψηλότερα στρώματα, οπότε η ταχύτητα του ήχου κοντά στο έδαφος είναι μεγαλύτερη. Στην περίπτωση αυτή, τα ηχητικά κύματα τείνουν να καμφθούν προς τα πάνω, με αποτέλεσμα ο ήχος να μη διαδίδεται καλά. Οι διαφορές στην ταχύτητα του ήχου προκαλούν διάθλαση [41].



Εικόνα 4: Τα ηχητική κύματα κάμπτονται όταν διαδίδονται σε αέρα με ανομοιόμορφη θερμοκρασία

Επίσης, η ταχύτητα του ήχου επηρεάζεται δραματικά από την ταχύτητα του ανέμου. Είναι γνωστό πως ο ήχος διαδίδεται ευκολότερα προς την κατεύθυνση του ανέμου παρά αντίθετα σε αυτόν. Ο αέρας είναι το μέσο διάδοσης του ήχου και συνεπώς αν ο άνεμος μετακινεί τον αέρα με μια ορισμένη ταχύτητα τότε είναι αναμενόμενο να επηρεάζεται η ταχύτητα του ήχου. Για παράδειγμα, αν ο ήχος κινείται με 347 μέτρα ανά δευτερόλεπτο και επικρατεί άνεμος 4.6 μέτρων ανά δευτερόλεπτο τότε η ταχύτητα του ήχου θα μεταβληθεί κατά περίπου 1%. Αυτό το ποσοστό μεταβολής είναι αρκετό για να επηρεάσει τη διάθλαση του ήχου. Στην εικόνα 4 φαίνεται η επίδραση του ανέμου στην περίπτωση της διάθλασης προς τα κάτω που έχει σαν αποτέλεσμα τη δημιουργία μιας

σκιάς στην αντίθετη κατεύθυνση του ανέμου ενώ ο ήχος στην κατεύθυνση του ανέμου διαθλάται προς τα πάνω.

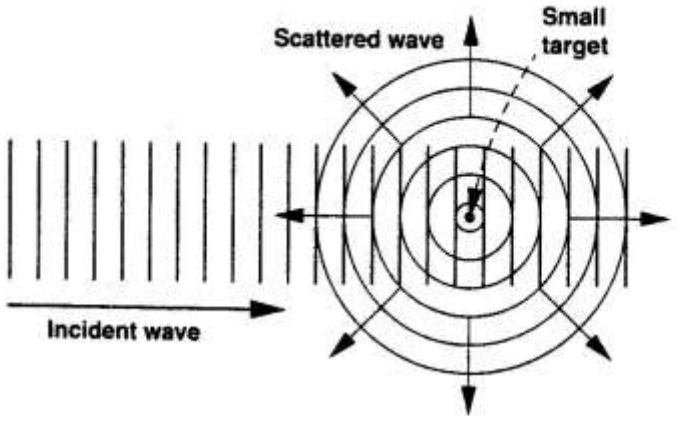


Εικόνα 5: Επίδραση του ανέμου στην ταχύτητα του ήχου

2.1.2.2 Σκέδαση

Το φαινόμενο της σκέδασης εμφανίζεται όταν ένα ακουστικό κύμα προσπέσει σε ένα ελαστικό σώμα που έχει ελαστικότητα πολύ διαφορετική από αυτή του μέσου διάδοσης (αέρας). Τότε το ακουστικό κύμα «χτυπάει» την επιφάνεια του σώματος και την υποχρεώνει σε ταλάντωση. Από την ταλάντωση παράγεται ένα σφαιρικό σκεδασμένο κύμα, το οποίο δεν έχει προς όλες τις κατευθύνσεις την ίδια ένταση [42].

Το σφαιρικό σκεδασμένο κύμα που προκαλείται συμβάλει με το κύριο ακουστικό κύμα με αποτέλεσμα την αλλοίωση ιδιοτήτων του ακουστικού κύματος, όπως είναι η φάση και η έντασή του. Αυτό έχει σαν αποτέλεσμα ο παραλήπτης του ακουστικού κύματος να λαμβάνει ένα ελαφρώς αλλοιωμένο και ενισχυμένο (σε συγκεκριμένες συχνότητες) σήμα. Οι επιδράσεις του συγκεκριμένου φαινομένου μπορούν να θεωρηθούν αμελητέες για ακουστικά κύματα χαμηλών συχνοτήτων και αποστάσεις μεγαλύτερες μερικών εκατοντάδων μέτρων από τις επιφάνειες πρόσκρουσης

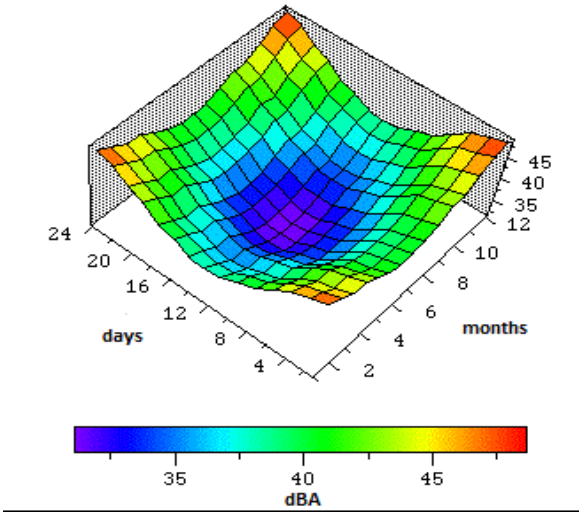


Εικόνα 6: Σκέδαση ακουστικού κύματος σε αντικείμενο [42].

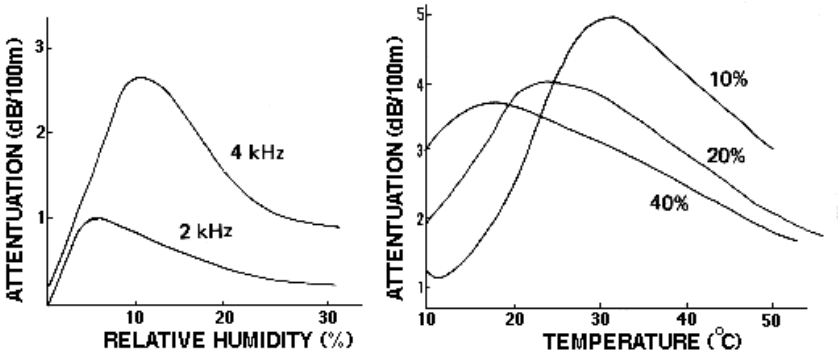
2.1.2.3 Ατμοσφαιρική απορρόφηση

Η εξασθένηση που προκαλεί ο αέρας σε ένα ηχητικό κύμα που διαδίδεται μέσα σε αυτόν εξαρτάται από την συχνότητα του ηχητικού κύματος, την σχετική υγρασία και

θερμοκρασία του περιβάλλοντος και την ατμοσφαιρική πίεση. Για την μέση συχνότητα της ανθρώπινης φωνής (2 kHz), η απόσβεση του ηχητικού κύματος είναι 0,25 dB/100m, σε συνθήκες 30% σχετική υγρασία περιβάλλοντος και 20^{O}C θερμοκρασία περιβάλλοντος. Ακόμα πρέπει να σημειωθεί ότι η εξασθένηση μπορεί να αυξηθεί σημαντικά, και να φτάσει την τιμή των 5 dB/100 m για ηχητικό κύμα συχνότητας 8 kHz και για περιβαλλοντικές συνθήκες, σχετική υγρασία περιβάλλοντος 10% και θερμοκρασία περιβάλλοντος 20^{O}C συνθήκες. Ακόμα, η εξασθένηση που προκαλείται στο κύμα από τον αέρα αυξάνεται γραμμικά με την απόσταση που διανύει το κύμα μέσα του. Στις ακραίες περιπτώσεις πολύ χαμηλών τιμών περιβαλλοντικής σχετικής υγρασίας και θερμοκρασίας παρατηρούνται πολύ μικρά ποσοστά εξασθένησης του κύματος. Τέλος αξίζει να σημειωθεί ότι οι διακυμάνσεις σε σχετική υγρασία και θερμοκρασία που παρατηρούνται κατά την διάρκεια μιας ημέρας ή και ένα μήνα επηρεάζουν το ποσοστό εξασθένησης ενός ηχητικού κύματος από τον αέρα.



Εικόνα 7: Τα επίπεδα θορύβου που λαμβάνουμε από μία σταθερή πηγή θορύβου κατά την διάρκεια ενός χρόνου



Εικόνα 8: (αριστερά) Το ποσό της εξασθένηση ενός ακουστικού κύματος συναρτήσει της σχετική υγρασίας στους 20°C.
(δεξιά) Το ποσό της εξασθένησης ενός ακουστικού κύματος σε συνάρτηση με την θερμοκρασία για διάφορα ποσοστά σχετική υγρασίας.

2.1.3 Περιβαλλοντικοί αισθητήρες

Όπως είδαμε παραπάνω οι ατμοσφαιρικές συνθήκες παίζουν σημαντικό ρόλο στον καθορισμό της ταχύτητας του ήχου, αλλά και τον γενικότερο τρόπο διάδοσής του στο περιβάλλον. Για τον ακριβή υπολογισμό της διάδοσης του ήχου θα πρέπει να ξέρουμε κάθε στιγμή, με ακρίβεια, την κατάσταση διάφορων περιβαλλοντικών παραμέτρους όπως είναι:

- Η θερμοκρασία
- Η υγρασία
- Η βαρομετρική πίεση
- Η ταχύτητα και η κατεύθυνση του αέρα.

Για την ακριβείας παρακολούθηση των παραπάνω περιβαλλοντικών παραμέτρων χρησιμοποιήθηκε η πλατφόρμα ασύρματων αισθητήρων iSense [49] (Κεφάλαιο 4.3). Η συγκεκριμένη πλατφόρμα προσφέρει μεγάλη ακρίβεια μετρήσεων. Συγκεκριμένα, ο αισθητήρας θερμοκρασίας που διαθέτει, προσφέρει μετρήσεις με 0.5 °C ακρίβεια και 0.1 °C ανάλυση. Με βάση τον τύπο (1) για τον υπολογισμό την ταχύτητας του ήχου, στους 25 °C η ακρίβεια του συγκεκριμένου αισθητήρα θερμοκρασίας προσφέρει 0.008% εύρος λάθους στον υπολογισμό την ταχύτητα. Το συγκεκριμένο εύρος λάθος είναι ανεκτό για τις απαιτήσεις της εφαρμογής που μελετάμε στην συγκεκριμένη εργασία.

2.2 Μορφή των ηχητικών κυμάτων

Ο ήχος που δημιουργείται από έναν άνθρωπο ή ένα όχημα προέρχεται από την κίνηση διάφορων επιμέρους εξαρτημάτων τους αλλά και από την επαφή τους με το έδαφος.

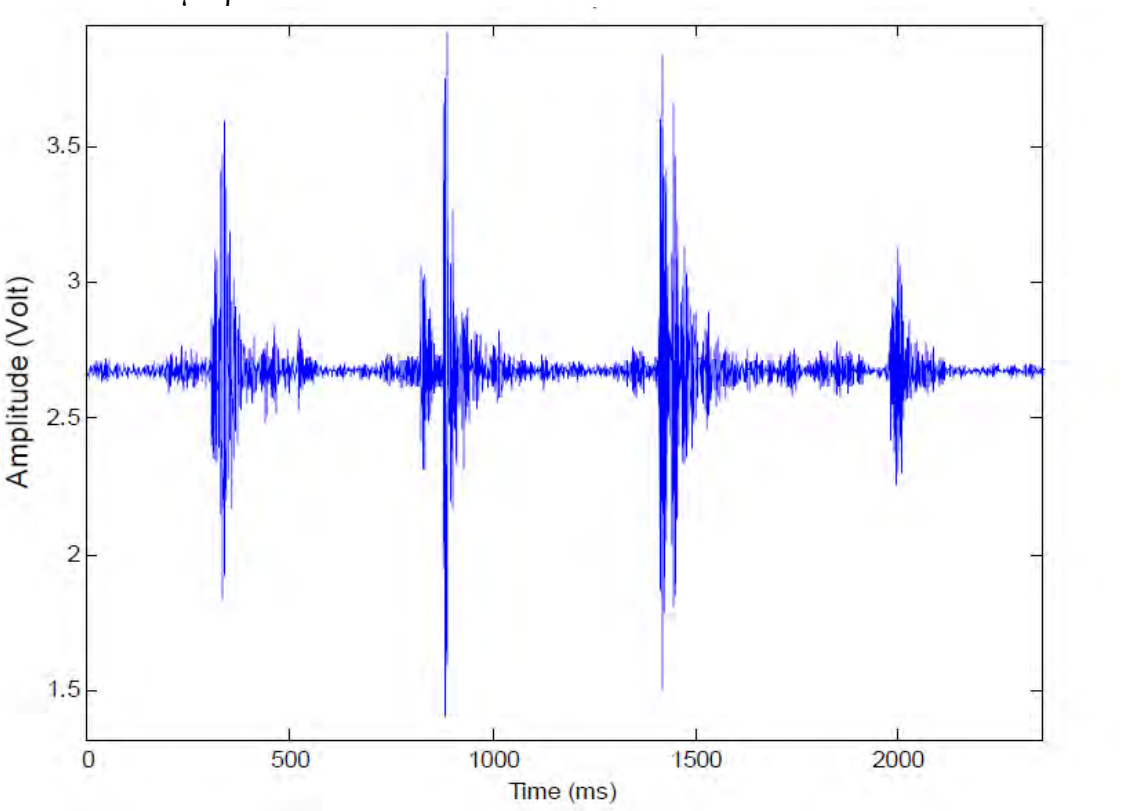
2.2.1 Χαρακτηριστικά ήχου που προέρχονται από άνθρωπο

Πιο συγκεκριμένα ο ήχος που προκαλείται από έναν άνθρωπο οφείλεται στο βάδισμά του και στην κίνηση/κρούση διάφορων αντικειμένων του, όπως είναι ένας σάκος διαβίωσης ή το όπλο του. Ο ήχος που προκαλείται από τα διάφορα επιμέρους αντικείμενα συμβαίνει σε τυχαίες στιγμές, είναι μικρής έντασης και δεν προσφέρεται η χρήση του για την παρατήρηση/παρακολούθηση της συμπεριφοράς του ίδιου του ανθρώπου. Από την άλλη, το βάδισμα δημιουργεί ένα χαρακτηριστικό ακουστικό και σεισμικό σήμα του οποίου η χρήση , με κατάλληλη επεξεργασία, προσφέρεται για την εντοπισμό/αναγνώριση ενός ανθρώπου. Το βάδισμα αποτελεί μια επαναλαμβανόμενη, ρυθμική κίνηση του σώματος, που σκοπό έχει να το μετακινήσει από το σημείο επαφής του με το έδαφος. Η διαδικασία του βαδίσματος μπορεί να χωριστεί σε 2 κύριες φάσεις:

- Την **στάση:** πρόκειται για την χρονική διάρκεια που μεσολαβεί ανάμεσα στην $1^{η}$ και την τελευταία επαφή του ποδιού με το έδαφος (όταν η φτέρνα ακουμπά το έδαφος) κατά την διάρκεια ενός βήματος. Η βάση της στάσης δηλαδή ξεκινάει όταν ακουμπήσει η φτέρνα στο έδαφος και τελειώνει την στιγμή όπου τα δάκτυλα του ποδιού αφήνουν το έδαφος.
- Την **ταλάντωση**: πρόκειται για την χρονική διάρκεια που μεσολαβεί ανάμεσα σε 2 στάσεις.

Οι δύο αυτές φάσεις επαναλαμβάνονται περιοδικά, ανάλογα με τον ρυθμό του βαδίσματος ή τρεξίματος [43].

Οι περιοδικές επαφές του πέλματος με το έδαφος (περιοδικές φάσεις **στάσης**) προκαλούν ένα χαρακτηριστικό ακουστικό και σεισμικό σήμα. Το χαρακτηριστικό αυτό σήμα μπορεί να ανιχνευτεί είτε με ακουστικούς είτε με σεισμικούς αισθητήρες. Συγκεκριμένα, σύμφωνα με την εργασία [44] η χρήση σεισμικών αισθητήρων (γεώφωνα) μπορεί να επιτύχει απόσταση ανίχνευσης του χαρακτηριστικού σήματος ίση με 64 μέτρα για την περίπτωση βαδίσματος και 84 μέτρα για την περίπτωση τρεξίματος. Σε περίπτωση προσεκτικού βαδίσματος η απόσταση αξιόπιστου εντοπισμού μπορεί να πέσει και κάτω από τα 10 μέτρα.



Εικόνα 9: Χαρακτηριστική μορφή ακουστικού/σεισμικού σήματος ανθρώπινου βαδίσματος

2.2.2 Χαρακτηριστικά ήχου που προέρχονται από όχημα

Σχεδόν οποιοδήποτε όχημα που κινείται προκαλεί ένα είδος ήχου. Οχήματα του ίδιου τύπου που λειτουργούν σε παρόμοιες συνθήκες παράγουν παρόμοιας μορφής ακουστικό σήμα (παρόμοια ηχητική υπογραφή). Ο ήχος αυτός οφείλεται σε ένα συνδυασμό πηγών όπως τα διάφορα κινούμενα μέρη του συστήματος μετάδοσης, οι προσκρούσεις και οι τριβές των ελαστικών με το έδαφος, ο άνεμος που δημιουργείται κατά την κίνηση του οχήματος, η εξάτμιση και κυρίως τα κινούμενα εξαρτήματα και οι λειτουργίες της μηχανής. [8,45,46]

Ως εκ τούτου, η μελέτη της λειτουργίας και της δομής της μηχανής ενός οχήματος μας δίνει χρήσιμες πληροφορίες για την μορφή του ακουστικού σήματος που προκαλεί. Η μηχανή ενός οχήματος εκτελεί κυρίως τρείς περιοδικές λειτουργίες, την συμπίεση, την καύση και δημιουργία των καυσαερίων. Από αυτές τις λειτουργίες η καύση και η έξοδος των καυσαερίων αποτελούν την κύρια πηγή θορύβου καθώς προκαλούν περιοδικές απότομες αυξομειώσεις του ήχου. Σημαντική επίδραση στον θορύβου αποτελεί το είδος

και το σχήμα της εξάτμισής καθώς αποτελεί το σημείο από όπου βγαίνουν με μεγάλη πίεση τα καυσαέρια. [18,46]

Το μεγαλύτερο ποσοστό της ενέργειας της ακουστικής υπογραφής ενός οχήματος βρίσκεται στο εύρος των 50 – 2000 Hz και το φασματικό της περιεχόμενο εξαρτάται άμεσα από την μορφή του αμαξώματος του αυτοκινήτου, τον τύπο του κινητήρα (βενζινοκινητήρας ή πετρελαιοκινητήρας), τον αριθμό των κυλίνδρων που διαθέτει, την ταχύτητα, αλλά και το είδος κίνησης του οχήματος (σε στάση, σε κίνηση, σε επιτάχυνση). Ο συνδυασμός όλων των παραπάνω συνθέτει την ηχητική υπογραφή ενός οχήματος. Η ηχητική υπογραφή χαρακτηρίζει ένα όχημα ή ένα τύπο οχήματος και μπορεί να χρησιμοποιηθεί για την τόσο για την, από απόσταση, αναγνώριση του όσο και για την διάκρισή του από κάποιο άλλο όχημα [47]

Σύμφωνα με την μελέτη [48] η ισχύς του ακουστικό σήμα που παράγεται από ένα μεγάλο όχημα (φορτηγό) που διαθέτει πετρελαιοκινητήρα και δεν είναι εφοδιασμένο με σιγαστήρα στην εξάτμιση είναι τόσο μεγάλη ώστε να είναι δυνατή η ανίχνευση του οχήματος σε μεγάλες αποστάσεις, όπως είναι 1000-1500 μέτρα κατά την διάρκεια της ημέρας και 3000-4000 μέτρα κατά την διάρκεια της νύχτας. Από την άλλη, το ακουστικό σήμα που παράγεται από ένα σύγχρονο αυτοκίνητο οφείλεται κυρίως στην κύλιση των τροχών και στην επαφή τους με το έδαφος, με αποτέλεσμα να είναι πιο δύσκολο ο εντοπισμός του. Η απόσταση ανίχνευσης ενός σύγχρονου αυτοκινήτου με βάση το ακουστικό σήμα του είναι 200-400 μέτρα.

2.3 Ακουστικοί Αισθητήρες

Βασικός παράγοντας για την αποτελεσματική και αξιόπιστη λειτουργία του συστήματος αποτελούν οι ακουστικοί αισθητήρες που θα χρησιμοποιηθούν για την καταγραφή των ακουστικών σημάτων. Ο όρος, ακουστικός αισθητήρας ή μικρόφωνο αναφέρεται σε μία συσκευή, που μετατρέπει την ακουστική ενέργεια σε ηλεκτρική. Η μετατροπή αυτή γίνεται μέσω μιας ευαίσθητη επιφάνια που διαθέτει το μικρόφωνο. Η ευαίσθητη αυτή επιφάνεια πάλετε από τα ακουστικά κύματα που μεταδίδονται στον αέρα και προσπίπτουν πάνω της. Η κίνηση αυτή της ευαίσθητης επιφάνειας μεταφράζεται στο αντίστοιχο ηλεκτρικό σήμα.

Τα μικρόφωνα μπορεί να ταξινομηθούν σε τρείς κύριες κατηγορίες ανάλογα με την αρχή λειτουργίας τους:

- Ηλεκτρο-δυναμικά
- Πυκνωτικά
- Πιεζοηλεκτρικά

Συνήθως σε στρατιωτικές εφαρμογές, παρόμοιες με αυτή που περιγράφουμε στην συγκεκριμένη εργασία, χρησιμοποιούνται τα πυκνωτικά μικρόφωνα καθώς προσφέρουν μεγάλη αξιοπιστία και ακρίβεια μετρήσεων. Η αρχή λειτουργίας των πυκνωτικών μικροφώνων στηρίζεται στο ηλεκτροστατικό πεδίο. Τα πυκνωτικά μικρόφωνα έχουν ένα κινούμενο μεταλλικό διάφραγμα που δέχεται τις μεταβολές της πίεσης. Το διάφραγμα αυτό είναι ουσιαστικά ο ένας από τους δύο οπλισμούς ενός φορτισμένου πυκνωτή ενώ ο άλλος οπλισμός είναι σταθερός. Οι μετακινήσεις του ενός οπλισμού προκαλούν μεταβολές στη χωρητικότητα του πυκνωτή, και αφού το φορτίο διατηρείται σταθερό,

προκαλούνται μεταβολές της τάσης στα άκρα του ανάλογες της πίεσης του ηχητικού κύματος [50].

Τα πλεονεκτήματα της χρήσης πυκνωτικών μικροφώνων είναι ότι εμφανίζουν μεγάλη ευαισθησία σε απότομες μεταβολές της ακουστικής πίεσης και ότι έχουν επίπεδη απόκριση συχνότητας. Από την άλλη τα πυκνωτικά μικρόφωνα απαιτούν εξωτερική τροφοδοσία και είναι σχετικά ακριβά σε σχέση με δυναμικά.

Τα μικρόφωνα εκτός από τον τύπο τους μπορούν να ταξινομηθούν και με βάση κάποια επιπλέον χαρακτηριστικά, όπως είναι: η ευαισθησία τους, η απόκριση συχνοτήτων τους και η κατευθυντικότητα τους.

Για το εφαρμογή που περιγράφεται στην συγκεκριμένη εργασία οι προδιαγραφές που θα πρέπει να καλύπτει ένα μικρόφωνο είναι:

- *Υψηλό εύρος συχνοτήτων*: η περιοχή των συχνοτήτων που καλύπτει θα πρέπει να είναι 0-1000Hz καθώς θα πρέπει να είναι δυνατή η καταγραφή παλμικών ηχητικών κυμάτων που οφείλονται σε εκπυρσοκρότηση, έκρηξη κλπ.
- *Ομοιογενής κατευθυντικότητα*: ώστε να είναι δυνατή η καταγραφή των ηχητικών σημάτων που προέρχονται από οποιαδήποτε κατεύθυνση.

Επιπλέον, μια σημαντική λεπτομέρεια για την αποτελεσματική καταγραφή των ήχων σε εξωτερικό χώρο είναι η χρήση κατάλληλων ανεμοπετασμάτων, τα οποία εξαλείφουν θορύβους του περιβάλλοντος, όπως είναι ο άνεμος.

Ένα παράδειγμα που καλύπτει τις παραπάνω προδιαγραφές είναι το WM-62A της Panasonic. Πρόκειται για ένα μικρόφωνο το οποίο έχει σχετικά χαμηλό κόστος, μεγάλη αξιοπιστία και ακρίβεια μετρήσεων και χρησιμοποιείται ευρέως. Διατίθεται ενσωματωμένο πάνω στην πλακέτα αισθητήρων MTS-310, η οποία είναι συμβατή με τους ασύρματους κόμβους Mica2.

3 *Ασύρματα Δίκτυα Αισθητήρων*

Ένα ασύρματο δίκτυο αισθητήρων (Α.Δ.Α.) αποτελείται από χωρικά κατανεμημένες αυτόνομες συσκευές. που φέρουν ενσωματωμένους αισθητήρες με σκοπό την παρατήρηση διάφορων φυσικών ή περιβαλλοντικών παραμέτρων, όπως είναι η θερμοκρασία, η υγρασία, η πίεση, ο ήχος , η δόνηση, η κίνηση ή οι ρύποι. Κάθε κόμβος έχει ικανότητα ασύρματης επικοινωνίας, δυνατότητες επεξεργασίας σήματος και δικτύωσης των στοιχείων. Τα Α.Δ.Α. χαρακτηρίζονται από

- Αυτοργάνωση
- Αυτοιασιμώτητα
- Χαμηλό κόστος
- Χαμηλές ενεργειακές απαιτήσεις

Πρόκειται για μια ειδίκευση των απλών ad-hoc mesh δικτύων κληρονομώντας έτσι μια σειρά από χαρακτηριστικά από αυτά, από τα οποία όμως άλλα επεκτείνονται και άλλα προσαρμόζονται στις ιδιαιτερότητες των Α.Δ.Α. και στις απαιτήσεις των εφαρμογών που εφαρμόζονται [6,7]. Μια σύνοψη των χαρακτηριστικών των Α.Δ.Α. φαίνεται στον Πίνακα 3.

Πίνακας 3: Τα χαρακτηριστικά των Ασύρματων Δικτύων Αισθητήρων [51]

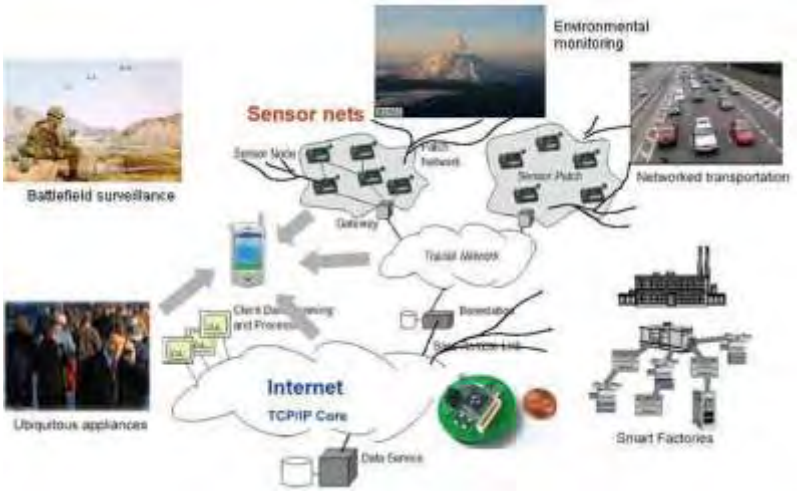
Αισθητήρες	**Μέγεθος**	μικρό (π.χ. μικρο-ηλεκτρονικές μηχανικές συσκευές (MEMS)) , μεγάλο (π.χ. radars και δορυφόροι)
	Πλήθος	μικρό, μεγάλο
	Τύπος	παθητικοί (π.χ. ακουστικοί, σεισμικοί, μαγνητικοί, υπέρυθροι), ενεργητικοί (π.χ. radar)
	Σύνθεση	ομοιογενής (ίδιος τύπος αισθητήρων) , ετερογενής (διαφορετικός τύπος αισθητήρων)
	Χωρική Κάλυψη	αραιά, πυκνή
	Τοποθέτηση	σε σταθερά προκαθορισμένα σημεία (π.χ. δίκτυο ενός εργοστασίου) , δυναμική (ad-hoc, π.χ. στην περίπτωση όπου ρίχνονται από αέρος)
Τύπος Μετρήσιμων Ποσοτήτων	**Εύρος**	κατανεμημένο (π.χ. παρακολούθηση περιβαλλοντικών συνθηκών), στοχευόμενο (π.χ. παρακολούθηση ενός στόχου)
	Κινητικότητα	στατικές, δυναμικές
	Φύση	συνεργαζόμενες (π.χ. έλεγχος της εναέριας κυκλοφορίας), μη-συνεργαζόμενες (π.χ. παρακολούθηση ενός στρατιωτικού στόχου)
Περιβάλλον Λειτουργίας	Φιλικό (π.χ. το πάτωμα ενός εργοστασίου), εχθρικό (π.χ. το πεδίο της μάχης)	
Επικοινωνία	**Τύπος**	ενσύρματη, ασύρματη

	επικοινωνίας	
	Εύρος ζώνης επικοινωνίας	υψηλό, χαμηλό
Τύπος Επεξεργασίας	Κεντρικοποιημένος (όλα τα δεδομένα στέλνονται σε ένα κεντρικό σημείο επεξεργασίας), κατανεμημένο (τα δεδομένα επεξεργάζονται τοπικά σε κάθε κόμβο), υβριδικός	
Διαθεσιμότητα Ενέργειας	Περιορισμένη (π.χ. σε αισθητήρες μικρού μεγέθους), μη περιορισμένη (π.χ. σε αισθητήρες μεγαλύτερου μεγέθους με μεγαλύτερο χώρο για συσσωρευτές ενέργειας)	

3.1 Ιστορική αναδρομή των Ασύρματων Δικτύων Αισθητήρων

Η ανάπτυξη των ασύρματων δικτύων αισθητήρων παρακινήθηκε αρχικά από τι στρατιωτικές εφαρμογές, όπως η επιτήρηση πεδίων μαχών. Η πρώτη γνωστή εφαρμογή ενός δικτύου αισθητήρων υπήρξε περίπου το 1950 Πρόκειται για το πρόγραμμα SOSUS (Sound Surveillance System) [52] το οποίο είχε κατασκευαστεί κατά την διάρκεια του Ψυχρού πολέμου με σκοπό τον εντοπισμό υποβρυχίων με την βοήθεια υποθαλάσσιων ακουστικών αισθητήρων. Η επόμενη εφαρμογή των Ασύρματων Δικτύων Αισθητήρων που καταγράφεται, αναπτύχτηκε από την DARPA (Defense Advanced Research Projects Agency) το 1980. Πρόκειται για το πρόγραμμα DSN (Distributed Sensor Networks)

Η ραγδαία ανάπτυξη των ασύρματων επικοινωνιών, της μικροηλεκτρονικής και της μικρομηχανικής συντέλεσαν στην ανάπτυξη συσκευών μικρού κόστους, μικρού μεγέθους αλλά μεγάλης επεξεργαστικής ισχύς. Το γεγονός αυτό βοήθησε την ανάπτυξη και διάδοση των Α.Δ.Α. με αποτέλεσμα σήμερα να συναντάμε πλήθος εφαρμογών του σε πολλούς πολιτικούς τομείς, συμπεριλαμβανομένου του περιβάλλοντος και της παρακολούθησης βιότοπων, των εφαρμογών υγειονομικής περίθαλψης, της οικιακής αυτοματοποίησης και του ελέγχου της κυκλοφορίας [53].



Εικόνα 10: Εφαρμογές των Ασύρματων Δικτύων Αισθητήρων

3.2 Στόχοι και απαιτήσεις ενός Ασύρματου Δικτύου Αισθητήρων

Παραπάνω αναφερθήκαμε σε μερικά από τα ιδιαίτερα χαρακτηριστικά των Α.Δ.Α. Παρόλα αυτά όμως η πολυδιάστατη φύση των πεδίων εφαρμογής τους όμως αναγκάζει τα δίκτυα αισθητήρων να προσαρμόζονται στις απαιτήσεις, στις ανάγκες και στις ιδιαιτερότητες της κάθε εφαρμογής.

Οι στόχοι ενός Α.Δ.Α. εξαρτώνται γενικά από την εφαρμογή για την οποία χρησιμοποιείται, αλλά μπορούμε να τους συνοψίζουμε σε τρείς βασικές κατηγορίες:

- **Καθορισμός της αξίας κάποιας παραμέτρου**
  Ένα Α.Δ.Α. μπορεί να ενημερώνει περιοδικά για την τιμή κάποιων περιβαλλοντικών παραμέτρων, π.χ. θερμοκρασία, που επικρατούν στα σημεία όπου έχουν εγκατασταθεί κόμβοι του.
- **Ανίχνευση της πραγματοποίησης ενός καθορισμένου γεγονότος.**
  Ένα Α.Δ.Α. μπορεί να επιτηρεί τις συνθήκες του χώρου όπου είναι εγκατεστημένο και να ενημερώνει αν και όταν συμβεί κάποιο προκαθορισμένο γεγονός. π.χ. εμφάνιση πάγου στα χωράφια, εντοπισμός ανθρώπινης κίνησης σε ελεγχόμενη περιοχή
- **Ταξινόμηση ενός αντικειμένου**
  Ένα Α.Δ.Α. μπορεί να παρατηρεί τις συνθήκες του χώρου όπου είναι εγκατεστημένο, να εκτελεί σύνθετες επεξεργασίες πάνω σε αυτές τις μετρήσεις και να βγάζει πολύπλοκα συμπεράσματα. Π.χ. ένα Α.Δ.Α. επιτήρησης μιας ελεγχόμενης περιοχής μπορεί να εντοπίζει ένα κινούμενο όχημα, ν το χαρακτηρίσει και να παρακολουθήσει την πορεία του.

Οι απαιτήσεις ενός Α.Δ.Α. αφορούν κυρίως τεχνικά χαρακτηριστικά τους τα οποία αποτελούν ταυτόχρονα και δείκτες απόδοσης του Α.Δ.Α. Μερικές από τις πιο σημαντικές απαιτήσεις ενός Α.Δ.Α. είναι οι εξής:

- **Χαμηλές ενεργειακές απαιτήσεις**
  Δεδομένου ότι σε πολλές εφαρμογές οι κόμβοι αισθητήρων θα τοποθετηθούν σε μια απομακρυσμένη περιοχή, η τροφοδότηση ενός κόμβου μπορεί να μην είναι δυνατή. Σε αυτήν την περίπτωση, η διάρκεια ζωής ενός κόμβου μπορεί να καθοριστεί από τη ζωή μπαταριών, για αυτό τον λόγο απαιτείται η ελαχιστοποίηση τω ενεργειακών δαπανών.
- **Μικρό μέγεθος και κόστος κόμβου**
  Η μείωση του μεγέθους και του κόστους κάθε κόμβου είναι μια ακόμα βασική απαίτηση για τον σχεδιασμό ενός Α.Δ.Α. Μειώνοντας το μέγεθος του κόμβου διευκολύνεται η τοποθέτηση των κόμβων, ενώ επίσης μειώνεται το κόστος και η κατανάλωση ενέργειας. Μειώνοντας το κόστος κάθε κόμβου μειώνεται και το συνολικό κόστος του δικτύου κάτι το οποίο είναι ιδιαίτερα κρίσιμο όταν έχουμε να κάνουμε με ένα Α.Δ.Α. πολλών κόμβων εγκατεστημένο σε δύσβατα ή εχθρικά περιβάλλοντα όπου κόμβοι σε περίπτωση βλάβης δεν μπορούν να ξαναχρησιμοποιηθούν.
- **Ποιότητα Υπηρεσιών (Quality of Service)**
  Στην πλειοψηφία τους, οι εφαρμογές των Α.Δ.Α. είναι δίκτυα πολλών κόμβων εγκατεστημένα σε δύσβατες περιοχές, όπου η πρόσβαση σε αυτές πολλές

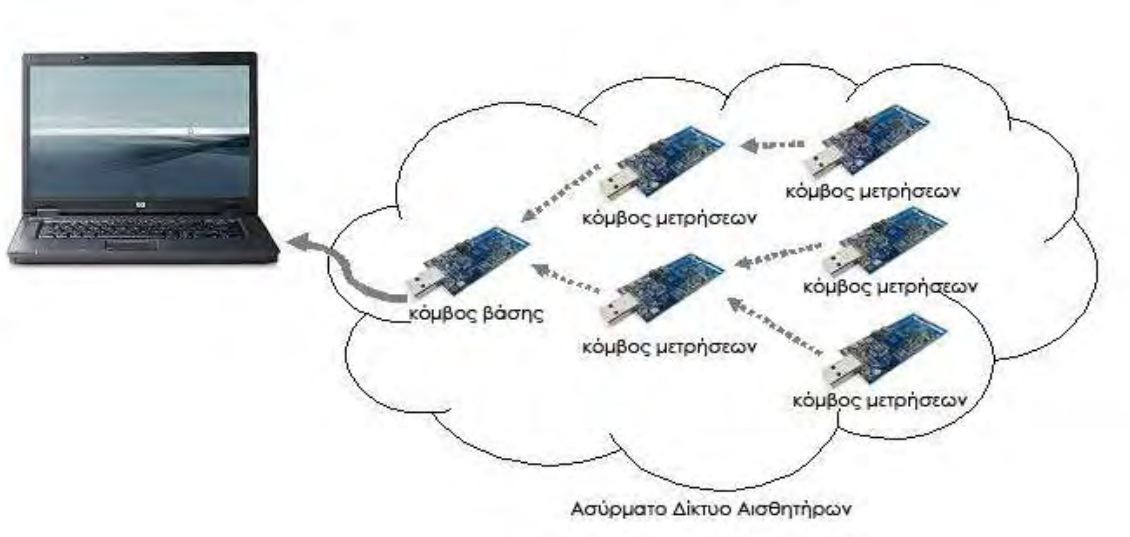
φορές δεν είναι εύκολη. Έτσι τα Α.Δ.Α. θα πρέπει να έχουν την δυνατότητα να αυτό-οργώνονται ώστε να μπορούν να συνεχίσουν την αποδοτική λειτουργία τους ακόμα και στις περιπτώσεις εμφανίσεις διαφόρων κρίσιμων καταστάσεων, όπως είναι η πτώση της μπαταρίας ή η εμφάνιση βλάβης σε κάποιους κόμβους, η εμφάνιση προβλημάτων επικοινωνίας ανάμεσα σε κόμβους κλπ. Τα Α.Δ.Α θα πρέπει να μπορεί να οργανώνει τους πόρους του ώστε να διατηρεί αμετάβλητη την ποιότητα και αποδοτικότητα των υπηρεσιών που προσφέρει.

- **Επεκτασιμότητα**
  Σε πολλές εφαρμογές το μέγεθος των Α.Δ.Α μπορεί να αποτελείται από μερικές εκατοντάδες ή και χιλιάδες κόμβους. Το μεγάλο αυτό πλήθος κόμβων επιφέρει μεγάλη πολυπλοκότητα στην αποδοτική λειτουργία και διαχείριση τους. Το γεγονός αυτό πρέπει να λαμβάνεται υπόψη κατά την διάρκεια ανάπτυξης των πρωτοκόλλων επικοινωνίας και προγραμματισμού των κόμβων, ώστε να υπάρχουν οι κατάλληλες δομές και πρωτόκολλα διαχείρισης μεγάλου όγκου πληροφοριών από και προς τους κόμβους των Α.Δ.Α.
- **Ασφάλεια**
  Λόγω της φύσης του πεδίου ανάπτυξης ενός Α.Δ.Α. κάθε κόμβος θα πρέπει να διαθέτει μηχανισμούς για την αποτροπή παρεμβολών λειτουργίας του. Αυτές οι παρεμβολές-επιθέσεις μπορεί να εμφανιστούν σε διάφορα επίπεδα όπως στο φυσικό (καταστροφή ή αλλοίωση της συσκευής), στο μέσο μετάδοσης (παρεμβολές στο φάσμα RF που χρησιμοποιεί το κανάλι), ή/και στο επίπεδο ζεύξης και δικτύου (DoS attacks, spoofing). Απαιτείται λοιπόν η ανά επίπεδο ανάπτυξη διάφορων αντιμέτρων προκειμένου να εξασφαλιστεί απρόσκοπτα η ομαλή λειτουργία. Αντιστοίχως λοιπόν, παραλλαγή, κέλυφος προστασίας, τεχνικές διαμόρφωσης σήματος, κρυπτασφάλιση και αυθεντικοποίηση είναι μεταξύ άλλων τα αντίμετρα που θα αποτρέψουν τις όποιες επιθέσεις επιχειρηθούν. [7,9,51,53]

3.3 Δομή ενός Ασύρματου Δικτύου Αισθητήρων

Όπως αναφέραμε και παραπάνω, ένα Α.Δ.Α αποτελείται από ένα πλήθος ασύρματων κόμβων αισθητήρων οι οποίοι είναι χωρικά διατεταγμένοι. Η τοπολογία του δικτύου μπορεί να ποικίλει από ένα απλό δίκτυο τοπολογίας αστέρα μέχρι ένα εξελιγμένο multihop πρωτόκολλο καθώς εξαρτάται από πολλές παραμέτρους , όπως είναι το είδος της εφαρμογής, η εμβέλεια των ασύρματων κόμβων, ο χώρος όπου είναι διατεταγμένοι οι κόμβο. Παρόλη την εξάρτηση των παραμέτρων του δικτύου από την κάθε εκάστοτε εφαρμογή, μπορούμε να διακρίνουμε δύο γενικούς τύπους κόμβων σύμφωνα με το είδος των λειτουργιών που εκτελούν. Οι δύο αυτοί τύποι κόμβων είναι

- ο κόμβος βάσης
- ο κόμβος μετρήσεων.



Εικόνα 11: Ο κόμβος βάσης και οι κόμβοι μετρήσεων ενός ασύρματου δικτύου αισθητήρων [9]

3.3.1 Κόμβος Βάσης

Ο κόμβος βάσης αποτελεί ένα κομβικό σημείο ενός Α.Δ.Α. Αποτελεί το μέσο επικοινωνίας ανάμεσα στο Α.Δ.Α. και στους χρήστες της εφαρμογής. Πρόκειται για τον κόμβος δηλαδή ο οποίος λειτουργεί σαν γέφυρα για την μεταφορά των μετρήσεων από τους κόμβους μετρήσεων του Α.Δ.Α. προς κάποιο χρήστη ή σύστημα καταγραφής, αλλά και για την μεταφορά δεδομένων και εντολών από τους χρήστες και την εφαρμογή του Α.Δ.Α προς τους ίδιους τους κόμβους μετρήσεων με σκοπό την πιο αποτελεσματική λειτουργία τους. Όπως είναι φανερό, ο κόμβος βάσης συγκεντρώνει μεγάλο πλήθος δεδομένων τα οποία πρέπει να τα λάβει, να τα επεξεργαστεί και να τα στείλει από και προς το δίκτυο. Συνήθως ο κόμβος βάσης για να ανταπεξέλθει σε αυτές τις απαιτήσεις, διαθέτει συνεχή τροφοδοσία ενέργειας, μεγάλης εμβέλειας κεραία ασύρματης επικοινωνίας, αυξημένη χωρητικότητα μνήμης και επεξεργαστικής ισχύς.

3.3.2 Κόμβος Μετρήσεων

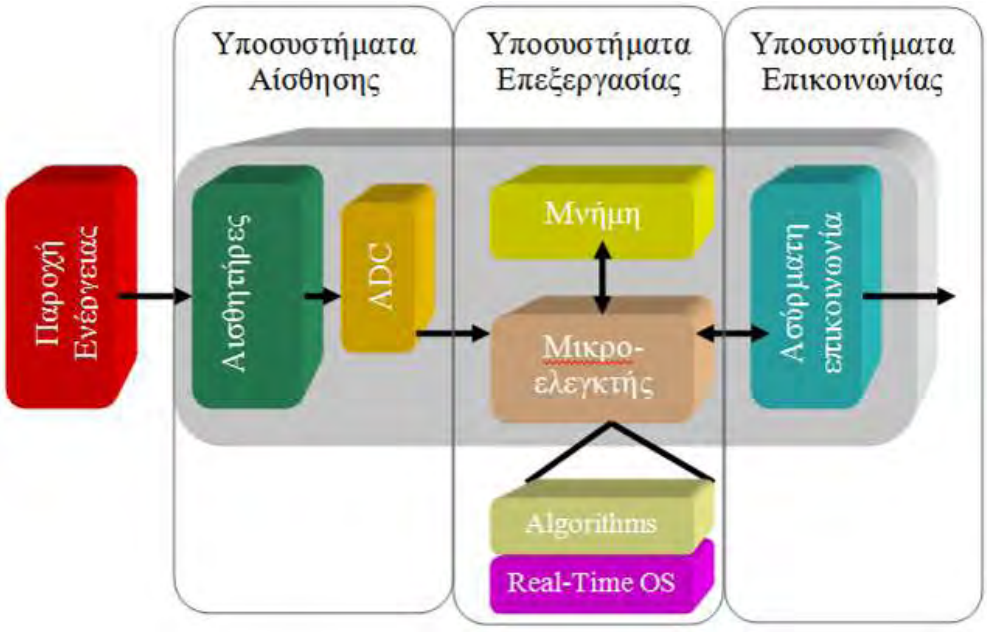
Ο κόμβος μετρήσεων αποτελεί το βασικό δομικό υλικό για την δημιουργία ενός Α.Δ.Α. Πρόκειται για ασύρματους κόμβους οι οποίοι είναι διατεταγμένοι μέσα στον προς παρακολούθηση χώρο και διαθέτουν ειδικά αισθητήρια όργανα για την διενέργεια μετρήσεων σε αυτό. Διαθέτουν ασύρματη κεραία επικοινωνίας ώστε να είναι δυνατή τόσο η μεταξύ τους επικοινωνία, όσο και η επικοινωνίας τους με τον κόμβο βάσης με σκοπό την μεταφορά των μετρήσεων και άλλων διαχειριστικών δεδομένων. Συνήθως δεν έχουν κάποια συνεχόμενη παροχή ενέργειας, αλλά χρησιμοποιούν κάποια ανεξάρτητη πηγή όπως είναι μια μπαταρία ή κάποιο ηλιακό πάνελ. Η χαμηλή διαθεσιμότητα σε ενέργεια που έχουν, αναγκάζει τους ασύρματους κόμβους μετρήσεων να έχουν χαμηλή επεξεργαστική ισχύ και χαμηλή χωρητικότητα μνήμης ώστε να επιτύχουν την ελάχιστη δυνατή κατανάλωση ενέργειας. Η μείωση της κατανάλωσης της ενέργειάς τους συνεπάγεται την αύξηση της διαθεσιμότητας τους στον χρόνο. Επιπλέον, χρησιμοποιούν ειδικά πρωτόκολλα ασύρματης επικοινωνίας και δρομολόγησης τα οποία λαμβάνουν υπόψη τις ιδιαιτερότητες τους με σκοπό να ελαχιστοποιήσουν την κατανάλωση ενέργειάς τους.

4 Πλατφόρμες Αισθητήρων

4.1 Δομή ενός Ασύρματου Κόμβου Αισθητήρων

Οι κόμβοι αισθητήρων που χρησιμοποιούνται σε ένα δίκτυο αισθητήρων μπορούν να χαρακτηριστούν ως μικροί υπολογιστές. Στην ουσία, ο κάθε κόμβος είναι μια μικρή κινητή ηλεκτρονική διάταξη η οποία έχει επεξεργαστική ισχύ, ικανότητα για ασύρματη επικοινωνία, μονάδα παροχής ενέργειας (π.χ. μπαταρία) και ενσωματωμένους αισθητήρες. Το μέγεθος ενός κόμβου αισθητήρων μπορεί να ποικίλει από δεκάδες εκατοστά, ως συσκευές με μέγεθος κόκκου σκόνης [54]. Το κόστος των κόμβων αισθητήρων είναι ομοίως μεταβλητό, κυμαινόμενο από εκατοντάδες δολάρια ως μερικά σεντς, ανάλογα με το μέγεθος του δικτύου αισθητήρων και της πολυπλοκότητας που απαιτείται από τους μεμονωμένους κόμβους αισθητήρων. Περιορισμοί μεγέθους και κόστους στους κόμβους αισθητήρων οδηγούν σε αντίστοιχους περιορισμούς σε πόρους όπως η ενέργεια, η μνήμη, η υπολογιστική ταχύτητα και το εύρος ζώνης [55-56].

Πιο συγκεκριμένα, η αρχιτεκτονική ενός κόμβου ενός ασύρματου δικτύου αισθητήρων καθώς και τα υποσυστήματα από τα οποία αποτελείται περιγράφονται στην Εικόνα 12.



Εικόνα 12: Δομή ενός κόμβου ασύρματου δικτύου αισθητήρων

(εικόνα από http://www.ee.unimelb.edu.au/sen_net/multimedia/research_prog/intsens.gif)

Τα υποσυστήματα αυτά είναι:

- **Αισθητήρας**
  Το υποσύστημα του αισθητήρα αποτελεί το μέσο με το οποίο ο κόμβος αισθάνεται τον περιβάλλοντα χώρο του. Συνήθως πρόκειται για έναν ηλεκτρονικό αισθητήρα ο οποίο αναλαμβάνει την μετατροπή ενός φυσικού ή χημικού μεγέθους του περιβάλλοντος σε ηλεκτρικό σήμα. Στην συνέχεια, αυτό το ηλεκτρικό σήμα, το οποίο συνήθως είναι εκφρασμένο με την μορφή αναλογικής τάσης, περνάει μέσα από ένα Αναλογικό σε Ψηφιακό μετατροπέα (Analog to Digital Converter). Αυτός ο μετατροπέας αναλαμβάνει να μετατρέψει τις αναλογικές μετρήσεις (σήματα) σε ψηφιακές, ώστε να είναι σε κατανοητή μορφή από τα υπόλοιπα υποσυστήματα του κόμβου για την περαιτέρω επεξεργασία τους.
  Σημαντικά χαρακτηριστικά που επηρεάζουν την επίδοση ενός αισθητήρα είναι η ακρίβεια μετρήσεων του, η κατανάλωση ενέργειάς και το μέγεθός του.
- **Μικρο-ελεγκτής (Micro-Processor)**
  Κάθε ασύρματος κόμβος είναι «χτισμένος» γύρω από έναν μικρο-ελεγκτή. Πρόκειται για την καρδία του κόμβου, το υποσύστημα δηλαδή το οποίο είναι αρμόδιο για την επεξεργασία των δεδομένων που συλλέγονται από τα αισθητήρια όργανα, τον συντονισμό των υπόλοιπων υποσυστημάτων του δικτύου και την αποστολή των δεδομένων μέσω της υλοποίησης κατάλληλων πρωτοκόλλων.
  Ένα μικρο-ελεγκτής για να μπορέσει να λειτουργήσει αποδοτικά σε ένα ασύρματο κόμβο θα πρέπει να ικανοποιεί ορισμένα λειτουργικά χαρακτηριστικά, όπως είναι η επεξεργαστική του ισχύς, η κατανάλωση ενέργειας, η εσωτερική μνήμη που διαθέτει, η ικανότητα πολλαπλών επιπέδων λειτουργίας και ο χρόνος εναλλαγής ανάμεσα σε αυτά τα επίπεδα.
  Σαν λειτουργία πολλαπλών επιπέδων εννοούμε την ικανότητα που μπορεί να έχει ο μικρο-ελεγκτής να μεταβάλει την επεξεργαστική του ισχύ, καθώς και να απενεργοποίει τα διάφορα συνδεμένα περιφερειακά συστήματα που διαθέτει. Αυτές οι εναλλαγές γίνονται με σκοπό την μείωση της κατανάλωσης ενέργειας, ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής. Η μείωση της κατανάλωσης ενέργειας ενός μικρο-ελεγκτής που βρίσκεται σε κατάσταση «ύπνωσης» (sleep mode), δηλαδή σε κατάσταση χαμηλής λειτουργίας και με απενεργοποιημένα όλα τα περιφερειακά του συστήματα, κυμαίνεται γύρω στο 90% (Πίνακας 4). Οι μικροεπεξεργαστές που χρησιμοποιούνται σήμερα περισσότερο στους κόμβους αισθητήρων είναι οι AVR, ATMega, και Mega της Atmel, η οικογένεια των HCS της Motorola και οι παλαιότεροι StrongArm της Intel.
  Ο επόμενο πίνακας περιέχει τα χαρακτηριστικά μερικών επιλεγμένων μικροεπεξεργαστών:

Πίνακας 4: Χαρακτηριστικά επιλεγμένων μικρό-ελεγκτών

Μικροελεγκτής	Μνήμη	Κατάσταση λειτουργίας & Τυπικές Τιμές Λειτουργίας		Παρατηρήσεις
		Ενεργή -Active	Αναμονής (Idle) - Sleep / Off	
ATMEL 8535	512B RAM 8K Flash	60mW	.036mW	TinyOS
ATmega103L AVR	128KB Flash 4KB EEPROM 4KB SRAM	5.5mA	1.6mA - < .1μA	TinyOS
ATMEGA 128	4K RAM 128K Flash	60mW	.036mW	TinyOS
ATMEL Mega 128L 7.328Mhz	128KB Flash 4KB EEPROM 4KB SRAM	285mW	50mW	TinyOS - IEEE 802.15.4
Motorola HC908	4K RAM	32mW	.001mW	IEEE 802.15.4
Intel StongArm 1100	16 MB FLASH 32 MB SDRAM (100 MHz)	400mW	50 – 0.16mW	-

- **Μνήμη**
  Η μνήμη είναι απαραίτητη στον ασύρματο κόμβο για δύο λόγους:
  - Για την αποθήκευση του λειτουργικού συστήματος αλλά και του εκτελέσιμου προγράμματος όπου εκτελεί ο κόμβος
  - Για την προσωρινή αποθήκευση των μετρήσεων από τα αισθητήρια όργανα, των επεξεργασμένων μετρήσεων αλλά και άλλων δομών που είναι χρήσιμες για την εκτέλεση των αλγορίθμων επεξεργασίας.

  Οι περισσότεροι μικρο-ελεγκτές διαθέτουν από 1 έως 128KB μνήμη τύπου FLASH για την αποθήκευση του κώδικα του λειτουργικού και 128 Bytes έως 32KB μνήμη RAM. Επίσης ορισμένοι διαθέτουν μνήμη τύπου EEPROM για την μόνιμη αποθήκευση κάποιων δεδομένων [8].
- **Ασύρματη επικοινωνία**
  Κάθε κόμβος ο οποίος ανήκει σε ένα Α.Δ.Α θα πρέπει να διαθέτει ένα υποσύστημα ασύρματη επικοινωνίας ώστε να είναι δυνατή η επικοινωνία, ο συντονισμός και η αποστολή μετρήσεων ανάμεσα στους κόμβους. Το βασικό μέρος ενός υποσυστήματος ασύρματης επικοινωνίας είναι ο πομποδέκτης. Οι πλειοψηφία των πομποδεκτών που χρησιμοποιούνται από ασύρματους κόμβους αισθητήρων λειτουργούν στην ISM (Industrial, Scientific, Medical) μπάντα, στις συχνότητες των 433.5 – 437.9 MHz, 868.0 – 868.6 MHz και 2400 – 2483.5 MHz. Η ακτίνα επικοινωνίας κυμαίνεται από τα 25 – 200 m, με το μέγιστο να επιτυγχάνεται στην περίπτωση όπου υπάρχει απευθείας οπτική επαφή με τον πομποδέκτη σε εξωτερικό χώρο. Τέλος οι ρυθμοί μετάδοσης που επιτυγχάνουν είναι της τάξης των 10 – 100Kbps [58,59].
  Όπως αναφέραμε σε προηγούμενα κεφάλαια, οι λειτουργικές απαιτήσεις ενός Α.Δ.Α. επηρεάζονται κάθε φορά από τις ιδιαιτερότητες της εκάστοτε εφαρμογής όπου λειτουργούν. Έτσι ανάλογα την εφαρμογή, οι κομβόι θα πρέπει να έχουν την δυνατότητα αξιόπιστης και ασφαλής επικοινωνίας, την

δυνατότητας προώθησης των μηνυμάτων προς κόμβους οι οποίοι βρίσκονται εκτός εμβέλειας του αρχικού αποστολέα του μηνύματος (π.χ. one hop / multihop) καθώς και την δυνατότητα εκτέλεσης έξυπνων μεθόδων δρομολόγησης των πακέτων ανάμεσα στους κόμβους με σκοπό την ελάττωση της συνολικής κατανάλωσης ενέργειας του δικτύου, αλλά και του κάθε κόμβου ξεχωριστά. Για την ικανοποίηση αυτών των απαιτήσεων οι ασύρματοι κόμβοι, αλλά και οι πομποδέκτες συγκεκριμένα χρησιμοποιούν εξειδικευμένα πρωτόκολλα ασύρματης επικοινωνίας τα οποία φροντίζουν για την ομαλή αλλά και χαμηλής κατανάλωσης επικοινωνία ανάμεσα στους κόμβους ενός Α.Δ.Α.[6]

- **Παροχή ενέργειας**

  Η διαθέσιμη σε ένα κόμβο ενέργεια προς κατανάλωση, αποτελεί κυρίαρχο περιορισμό στην κατασκευή του, στον ωφέλιμο χρόνο ζωής του καθώς και στις επιλογές που σχετίζονται τόσο με το υλικό που τον απαρτίζει όσο και στις επιλογές σχετικά με τους αλγορίθμους και το μοντέλο δικτύου που θα υλοποιηθεί. Ο βασικός στόχος στην επιλογή της παροχής ενέργειας σε έναν κόμβο είναι η παροχή όσο το δυνατόν περισσότερης ενέργειας με όσο το δυνατόν μικρότερο κόστος, όγκο, βάρος, χρόνο επαναφόρτισης και χρόνο ζωής.

  Η πιο συνηθισμένη και εύκολα χρησιμοποιήσιμη τεχνολογία παροχής ενέργειας στα δίκτυα ασύρματων αισθητήρων είναι αυτή των ηλεκτροχημικών συσσωρευτών, τις κλασσικές δηλαδή μπαταρίες. Οι ηλεκτροχημικοί συσσωρευτές διατίθενται σε διάφορες εκδώσεις, ανάλογα με τα χημικά στοιχεία που περιέχουν (π.χ. Carbon-Zinc, Alcaline, Silver Oxide (AgO), Lithium (LiSOCl2 και LiMnO2), NiCad, NiMH, Li-Ion). Ο χρόνος ζωής κάθε συσσωρευτή εξαρτάται από την χημική του σύνθεση, αλλά γενικότερα μπορούμε να πούμε ότι οι ηλεκτροχημικοί συσσωρευτές χαρακτηρίζονται από μεγάλη ενεργειακή πυκνότητα και μικρό ρυθμό αποφόρτισης. Επιπλέον έχουν μικρό κόστος, όγκο και μερικές από αυτές είναι επαναχρησιμοποιήσιμες (επαναφορτιζόμενες) μειώνοντας έτσι το συνολικό κόστος του δικτύου.

  Εναλλακτικοί τρόποι για την αντιμετώπιση του προβλήματος της παροχής επαρκούς ενέργειας στα δίκτυα ασυρμάτων αισθητήρων είναι:

  - Η χρήση μεθόδων για την διανομή ενέργειας στους κόμβους από απόσταση.
  - Η χρήση τεχνολογιών οι οποίες θα επιτρέπουν σε ένα κόμβο να παράγει μόνος του ή να συλλέγει ενέργεια από το περιβάλλον. Παραδείγματα τέτοιων μεθόδων είναι οι θερμικές μηχανές τεχνολογίας MEMS [60], οι φωτοβολταικές ή ηλιακές κυψέλες [61], οι μηχανές παραγωγής ενέργειας μέσω της μηχανικής ταλάντωσης, οι μηχανές παραγωγής ενέργειας μέσω της ροής αέρα αλλά και μέσω των διακυμάνσεων της ατμοσφαιρικής πίεσης [62].

  Τέλος εκτός της χρήση κατάλληλων συσσωρευτών και μηχανών παραγωγής ενέργειας, σημαντικό ρόλο στην αντιμετώπιση του προβλήματος ενέργειας στα δίκτυα αισθητήρων παίζει και η κατάλληλη διαχείριση ενέργειας μέσω της χρήση κατάλληλων αλγορίθμων για την διαχείριση των

επιμέρους υποσυστημάτων των κόμβων, των πρωτοκόλλων επικοινωνίας και των πρωτοκόλλων δειγματοληψίας. Οι διάφοροι αλγόριθμοι και τα πρωτόκολλα που εκτελούνται στο εσωτερικό των κόμβων θα πρέπει να είναι χαμηλών ενεργειακών απαιτήσεων και να λαμβάνουν υπόψη τις ενεργειακές ιδιαιτερότητες του κάθε κόμβου και εφαρμογής. Για παράδειγμα, στην περίπτωση χρήσης ηλεκτροχημικών συσσωρευτών θα πρέπει να λαμβάνονται υπόψη τα φαινόμενα "κλιμακωτής χωρητικότητας" – (rated capacity effect) και "επανάκτησης"- (recovery effect).

4.2 Ακουστικοί Αισθητήρες

Σύμφωνα με τις προδιαγραφές του συστήματος, ασύρματοι κόμβοι θα πρέπει να βρίσκονται διάσπαρτοι στον επιβλέποντα χώρο (είτε στατικοί, είτε κινητοί πάνω στις στολές των στρατιωτών.). Αυτοί οι κόμβοι θα πρέπει να έχουν την δυνατότητα: α) καταγραφής του ακουστικού ήχου μέσω ενός κατάλληλου αισθητήριου οργάνου (μικρόφωνο), β) επεξεργασίας του ήχου , γ) ασύρματης επικοινωνίας με σκοπό την ανταλλαγή δεδομένων με τους υπόλοιπους κόμβους του συστήματος.

Υπάρχει μια πληθώρα εμπορικών αλλά και ερευνητικών κόμβων που μπορούν να ικανοποιήσουν τις παραπάνω απαιτήσεις. Στον παρακάτω πίνακα γίνεται μια παρουσίαση και σύγκριση των γενικών χαρακτηριστικών των πιο σημαντικών, από αυτούς, ασύρματων κόμβων.

Οι Πίνακες 3 & 4 παρουσιάζουν πληροφορίες για 5 κόμβους ασύρματων δικτύων αισθητήρων. Πρόκειται κυρίως για εμπορικούς κόμβους τελευταίας τεχνολογίας οι οποίοι χαρακτηρίζονται για τις αποδόσεις τους, τις χαμηλές ενεργειακές απαιτήσεις τους, καθώς και την δυνατότητα ενσωμάτωσης διάφορων αισθητήριων οργάνων και γενικότερα την καταλληλότητα τους για εφαρμογές δικτύων αισθητήρων. Οι 5 αυτοί κόμβοι είναι:

- Ο κόμβος Mica2 της εταιρείας CrossBow [10]
- Ο κόμβος Mica2Dot της εταιρείας CrossBow (πρόκειται για μια "mini" έκδοση του κόμβου Mica2)
- Ο κόμβος Tmote Sky της εταιρείας Sentilla (προέρχεται από ερευνητικό πρόγραμμα του Πανεπιστημίου Berkeley)
- Ο κόμβος Imote της εταιρείας CrossBow.
- Ο κόμβος iSense της εταιρείας Coalesenses (προέρχεται από ερευνητικό πρόγραμμα του Πανεπιστημίου Lübeck)

Πίνακας 5: Παρουσίαση των γενικών χαρακτηριστικών κόμβων ασύρματων δικτύων αισθητήρων [63-64]

Πλατφόρμα	Mica2	Mica2Dot	Tmote Sky	Imote	iSense
Μικροελεγκτής	AtMega128L	AtMega128L	MSP430F	ARM7	JN5148
Αρχιτεκτονική	8-bit	8-bit	16-bit	32-bit	32-bit
Συχνότητα (MHz)	7.3728	4	8	12	4-32
Μνήμη Προγράμματος (kB)	128	128	48	512	128
Μνήμη RAM (kB)	4	4	10	11	128
Μνήμη FLASH (kB)	512	512	1024	-	512
Ακρίβεια A/D	10-bit	10-bit	12-bit	-	12-bit
Είσοδοι / Έξοδοι	51	18	16	30	10
Ενσωματωμένοι Αισθητήρες	2	2	5	0	1
Αλληλεπίδραση με τον Χρήστη	3 LED	1 LED	3 LED, 1 Κουμπί	1 LED	1 LED
Τρόπος Προγραμματισμού	ISP, JTAG, Bootloader	ISP, JTAG, Bootloader	USB,JTAG	JTAG	ISP, JTAG
Μέγεθος (mm^2)	1856	492	2621	900	1350

Πίνακας 6: Παρουσίαση των χαρακτηριστικών πομποδέκτη κόμβων ασύρματων δικτύων αισθητήρων [63-64]

Πλατφόρμα	Mica2	Mica2Dot	Tmote Sky	Imote	iSense
Πλακέτα	Chipcon CC1000	Chipcon CC1000	Chipcon CC2420	Zeevo TC2001	JN5148
Πρότυπο Επικοινωνίας	ISM	ISM	IEEE 802.15.4	Bluetooth 1.1	IEEE 802.15.4
Εύρος Συχνοτήτων	315-916 MHz	315-916 MHz	2.4 GHz	2.4 GHz	2.4 GHz

Ρυθμός Μετάδοσης	38.4 kbps	38.4 kbps	250 kbps	723.2 kbps	250- 667[1] kBit/s
TX Power	-/+10dBm	-/+10 dBm	-3/+0 dBm	+0.5/+4 dBm	+2.5dBm
Ευαισθησία	101 dBm	101 dBm	94 dBm	80 dBm	-95dBm
Εσωτερική Κεραία	-	Wire	Embed. PIFA	GigaAnt	integrated PCB antenna
Εξωτερική Κεραία	MMCX Connector	-	SMA Connector	U.FL Connector	μFl connector
Εμβέλεια Εξωτερικού Χώρου	150 m	150 m	125 m	30 m	600 m
Εμβέλεια Εσωτερικού Χώρου	40 m	40 m	50 m	30 m	100 m

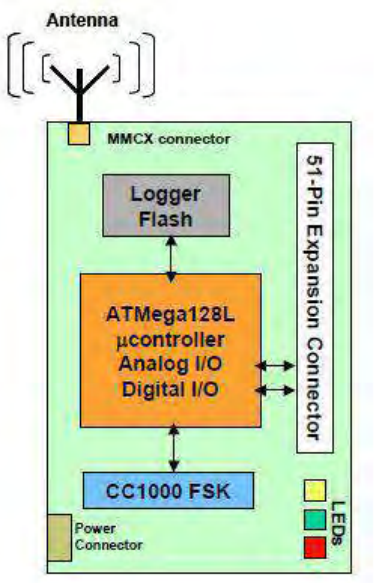
1. ***Για το πρότυπο IEEE 802.15.4 ισχύει ο ρυθμός μετάδοσης των 250 Kbits/s. Για μεγαλύτερους ρυθμούς μετάδοσης μειώνεται η ευαισθησία.***

Πίνακας 7: Παρουσίαση των ενεργειακών απαιτήσεων κόμβων ασύρματων δικτύων αισθητήρων [63-64]

Πλατφόρμα	**Mica2**	**Mica2Dot**	**Tmote Sky**	**Imote**	**iSense**
Τύπος Μπαταρίας	2AA cells	1 coin cell	2 AA cells	2 CR2 cells	2 AA cells
Ελάχιστη Τάση	2.7 V	2.7 V	2.1 V	3.0 V	2.0 V
Χωρητικότητα Μπαταρίας	2000 mAh	560 mAh	2900 mAh	1600 mAh	2900 mAh
Ρυθμιζόμενη Τροφοδοσία	OXI	OXI	OXI	NAI	NAI
Κατανάλωση με CPU σε sleep mode & κεραία κλειστή	0.054 mW	0.054 mW	0.0153 mW	9 mW	0.0123 mW
Κατανάλωση με CPU σε normal mode & κεραία κλειστή	36 mW	36 mW	5.4 mW	27 mW	19.8 mW
Κατανάλωση με CPU σε normal mode & κεραία να ανταλλάσει δεδομένα (RX/TX)	117 mW	117 mW	58.5 mW	112.5 mW	52.8 mW

4.2.1 Ασύρματος Κόμβος Mica2

Ο κόμβος που χρησιμοποιήθηκε για την εκτέλεση των παραπάνω λειτουργιών είναι ο κόμβος Mica2 της εταιρείας CrossBow [65]. Πρόκειται για ασύρματο κόμβο αισθητήρων τρίτης γενιάς που προήλθαν από την ερευνητική ομάδα του David Culler στο Πανεπιστήμιο του Berkeley το 2000 και πλέον διατίθεται από την εταιρία Crossbow. . Οι καρδιά του κόμβου βρίσκεται ένας μικρο-ελεγκτής ATMega128L της εταιρίας Atmel, ο οποίος είναι χρονισμένος στα 7.3728 MHz και διαθέτει μνήμη flash μεγέθους 512 kB. Η ασύρματη επικοινωνία από και προς τον κόμβο επιτυγχάνεται με την χρήση του ολοκληρωμένου CC1000 της εταιρείας Chipcon. Με την χρήση του συγκεκριμένου ολοκληρωμένου δικτύωσης ο κόμβος επιτυγχάνει ρυθμό μετάδοσης 38,400 bps στην μπάντα των 868/916 MHz χρησιμοποιώντας διαμόρφωση τύπου FSK.



Εικόνα 13: Το σχηματικό διάγραμμα του κόμβου Mica2

Όπως γίνεται φανερό και από τους παραπάνω Πίνακες 3 & 4 & 5 ο κόμβος Mica2 που χρησιμοποιήθηκε δεν αποτελεί την βέλτιστη λύση από άποψη επεξεργαστικής ισχύς και κατανάλωσης ενέργειας. Για παράδειγμα, στον Πίνακα 5 βλέπουμε ότι η κατανάλωση ενέργειας του κόμβου Mica2 σε κατάσταση κανονικής λειτουργίας και ασύρματης ανταλλαγής δεδομένων έχει σχεδόν την διπλάσια κατανάλωση ενέργειας *(117 mW)* από ότι έχουν οι κόμβοι Tmote Sky & iSense στην παρόμοια κατάσταση λειτουργίας *(58.5 mW & 52.8 mW αντίστοιχα)*. Παρόλα αυτά, στην εργασία που περιγράφεται, γίνεται χρήση των κόμβος Mica2 καθώς αντικείμενο της εργασίας είναι κυρίως η περιγραφή τεχνικών εξοικονόμησης ενέργειας, που μπορούν να επιτευχθούν με ένα δεδομένο υλικό και αφορούν στο υποσύστημα του αισθητήρα αλλά και του λογισμικού της εφαρμογής (μέθοδοι επεξεργασίας σήματος, ενεργειακή πολιτική, επικοινωνιακή πολιτική). Θεωρούμε λοιπόν ότι η χρήση του κόμβου Mica2 δεν βλάπτει την γενικότητα των προτεινόμενων μεθόδων ενώ ταυτόχρονα λειτουργεί και σαν

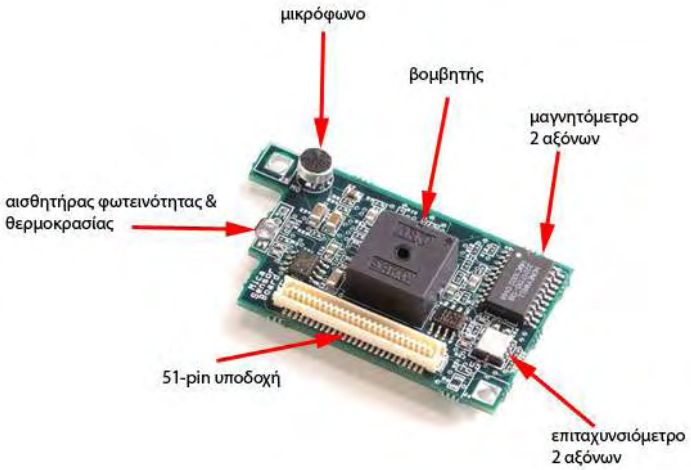
χειρότερη περίπτωση (worst-case scenario) για την μέτρηση της αποδοτικότητας των μεθόδων αυτών.

Εικόνα 14: Ο κόμβος Mica2

4.2.2 Πλατφόρμα αισθητήρων MTS310

Όπως φαίνεται και στην Εικόνα 14, ο κόμβος Mica2 διαθέτει μια υποδοχή με 51-pin, ώστε να είναι δυνατή η επέκτασή του. Με αυτή την υποδοχή μπορούν να ενσωματωθούν στον κόμβο Mica2 πλακέτες επέκτασης προσαρμοσμένες στις ανάγκες τις εκάστοτε εφαρμογής. Τέτοιες πλακέτες μπορεί να είναι οι πλακέτες αισθητήρων, οι πλακέτες λήψης δεδομένων, οι πλακέτες με ενσωματωμένο δέκτη GPS ή ακόμα και οι πλακέτες με ενσωματωμένο πομποδέκτη μεγαλύτερης εμβέλειας. Στη περίπτωση του συστήματος επιτήρησης χώρων που περιγράφεται, είναι απαραίτητη η ενσωμάτωση στους κόμβους και χρήση μικροφώνων όπου θα ακούν τους ήχους του περιβάλλοντα χώρου.

Για την ικανοποίηση των αναγκών του συστήματος, χρησιμοποιήσαμε τις πλακέτες επέκτασης MTS310 της εταιρείας CrossBow [66]. Πρόκειται για μια πλακέτα αισθητήρων ειδικά σχεδιασμένη για την λειτουργία της με του κόμβους Mica2. Διαθέτει πέντε αισθητήρια όργανα και ένα βομβητή.



Εικόνα 15: Η πλακέτα αισθητήρων MTS310

Πιο αναλυτικά τα αισθητήρια όργανα που φέρει η πλακέτα MTS310 είναι:

1. **Μικρόφωνο.**
   Πρόκειται για έναν ακουστικό αισθητήρα τύπου LM567 της εταιρείας National Semiconductor. Παρουσιάζει ιδιαίτερη ευαισθησία στις συχνότητες από 0.01 Hz έως 500 kHz ενώ παράλληλα παρέχει δύο επίπεδα ενίσχυσης του σήματος κάνοντας το έτσι ιδανικό για χρήση σε εφαρμογές ηχο-εντοπισμού, καταγραφής και μέτρησης ηχητικών σημάτων. Τα δύο επίπεδα ενίσχυσης του σήματος περιλαμβάνουν: στο $1^{ο}$ επίπεδο έναν προενισχυτή και στο $2^{ο}$ επίπεδο έναν ενισχυτή/ψηφιακό ποτενσιόμετρο.
2. **Επιταχυνσιόμετρο δύο αξόνων**
   Είναι ένα επιταχυνσιόμετρο τύπου ADXL202 της εταιρείας ADI. Πρόκειται για μια MEMS συσκευή χαμηλής ισχύος (<1mA) που καταγράφει την επιτάχυνση σε δύο άξονες σε εύρος ±2g και με ακρίβεια 2 mg.
3. **Μαγνητόμετρο δύο αξόνων**
   Πρόκειται για το μαγνητόμετρο HMC1002 της εταιρείας Honeywell. Αποτελεί έναν αισθητήρα πυριτίου που συνίσταται από υπερευαίσθητες στρώσεις σιδηρονικελίου (*NiFe*) με δυνατότητα ανίχνευσης της μαγνητικής απόκλισης. Χρησιμοποιείται κυρίως σε εφαρμογής παρακολούθησης οχημάτων, καθώς μπορεί να ανιχνεύσει όχημα σε απόσταση 15 μέτρων από τον αισθητήρα.
4. **Αισθητήρας θερμοκρασίας και φωτεινότητας**
   Ο αισθητήρας θερμοκρασίας είναι ο ERT-J1VR103J της εταιρείας Panasonic. Πρόκειται για έναν αισθητήρα θερμοκρασία με χαμηλή κατανάλωση ενέργειας, και μεγάλη ακρίβεια (~0.5 ^{o}C)
   Όσον αφορά τον αισθητήρα φωτεινότητας, πρόκειται για μια φωτοκυψέλη καδμοσεληνίτη (*CdSe*), η οποία παρουσιάζει μέγιστη ευαισθησία για τα μήκη κύματος της τάξης των 690 nm.
5. **Βομβητής**
   Ο βομβητής που είναι ενσωματωμένος πάνω στην πλακέτα MTS310 είναι ένα πιεζοηλεκτρικό αντηχείο (piezoelectric resonator) ο οποίος λειτουργία σε μία απλή σταθερή συχνότητα. Η συχνότητα αυτή είναι τα 4 kHz.

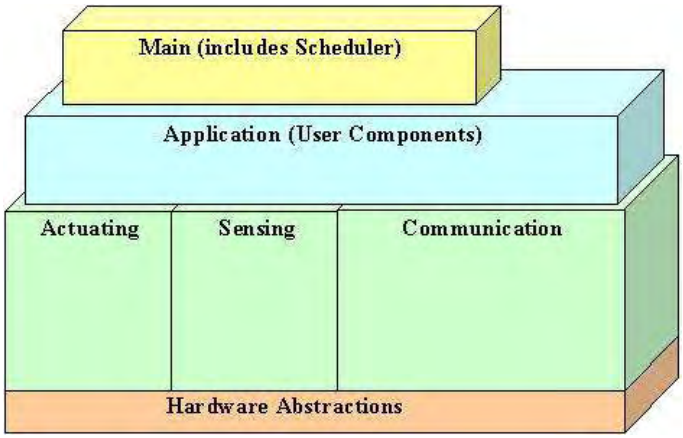
4.2.3 Το λειτουργικό σύστημα Tinyos

Η εκτέλεση των λειτουργιών των κόμβων Mica2 βασίζεται στην χρήση ενός ειδικού λειτουργικού συστήματος. Το ειδικό αυτό λειτουργικό σύστημα είναι το Tiny Micro Operating System, γνωστό και ως Tinyos. Πρόκειται για ένα ελαφρύ λειτουργικό ανοιχτού κώδικα το οποίο αναπτύχτηκε από την συνεργασία του Πανεπιστημίου της Καλιφόρνια, του Πανεπιστημίου Berkeley και 2 εταιρειών, της Intel και της Crossbow. Είναι ειδικά σχεδιασμένο να καλύπτει τις ανάγκες και τις απαιτήσεις των ασύρματων κ κόμβων αισθητήρων, όπως είναι:

1. Η χαμηλή κατανάλωση ενέργειας.
2. Οι ιδιαίτερα υψηλές απαιτήσεις για πολυπλεξία, συγχρονισμό και ευέλικτη διαχείριση των πόρων του κόμβου, καθώς υπάρχει συνεχής ροή πληροφοριών από πολλές πηγές (αισθητήρες, πομποδέκτης) σε αντίθεση με την μικρή

μνήμη του κόμβου που περιορίζει την δυνατότητα προσωρινής αποθήκευσης των δεδομένων.
3. Μικρές απαιτήσεις σε μνήμη.
4. Η σχεδίαση να είναι modular ώστε να είναι δυνατή η χρήση του από πολλούς και διαφορετικούς τύπους ασύρματων κόμβων με πλήθος διαφορετικών αισθητήριων οργάνων. [56, 68]

Μια απλοποιημένη εκδοχή της αρχιτεκτονικής του TinyOS φαίνεται στο παρακάτω σχήμα:



Εικόνα 16: Η αρχιτεκτονική του Tinyos [56].

Πρόκειται για ένα ενσωματωμένο λειτουργικό σύστημα δομημένο σε ένα σύνολο επιμέρους δοκιμών στοιχείων (component-based) ενώ η εκτέλεσή του βασίζεται σε συμβάντα (event-based). Στο TinyOS δεν υπάρχει καθόλου η έννοια της διεργασίας (process) όπως την έχουμε συνηθίσει στα σύγχρονα λειτουργικά συστήματα. Αντίθετα, υπάρχει η κυρίαρχη έννοια του component, το οποίο είναι κατά κάποιο τρόπο η αφαίρεση ενός λειτουργικού module του συστήματος. Κατ' ουσία είναι ένα πεπερασμένο αυτόματο και θυμίζει τα module που συναντάμε σε γλώσσες περιγραφής υλικού όπως η Verilog και η VHDL, αν και υπάρχουν αρκετές διαφορές. Αν και τα περισσότερα component είναι software modules, μερικά απλά χρησιμοποιούνται ως ένα απλό interface για το hardware του συστήματος

Το TinyOs είναι υλοποιημένο στην γλώσσα nesC, μία διάλεκτο της γλώσσας προγραμματισμού C ειδικά βελτιστοποιημένη για τον λιγοστό χώρο μνήμης των ασύρματων κόμβων αισθητήρων. Όταν ένας κόμβος εκτελεί μία εφαρμογή που βασίζεται στο λειτουργικό TinyOS, σημαίνει ότι έχει εγκατεστημένο στη flash μνήμη του ένα binary εκτελέσιμο της εφαρμογής μαζί με τις βιβλιοθήκες του TinyOS που χρειάζεται. Αυτό έχει σαν απαίτηση η μεταγλώττιση του λειτουργικού συστήματος TinyOs και των εκάστοτε εφαρμογών των κόμβων αισθητήρων γίνεται εκτός των κόμβων (σε κάποιο βοηθητικό υπολογιστή) και σε αυτούς να μεταφέρεται μόνο το τελικό μεταγλωττισμένο εκτελέσιμο. Αυτό έχει σαν αποτέλεσμα την ανάγκη χρήσης μερικών συμπληρωματικών εργαλείων που βοηθούν στην μεταγλώττιση των εφαρμογών και την εγκατάστασή τους στην μνήμη των κόμβων. Τα συμπληρωματικά αυτά εργαλεία είναι υλοποιημένα κυρίως σε γλώσσα Java και shell scripts, ενώ ο μεταγλωττιστής και τα

εργαλεία διαχείρισης των μικρο-ελεγκτών των κόμβων Mica2 είναι σε γλώσσα C [56, 67-70].

4.3 Περιβαλλοντικοί Αισθητήρες

Στο Κεφάλαιο 2 είδαμε ότι οι περιβαλλοντικές συνθήκες και ιδιαίτερα η θερμοκρασία, η υγρασία και η ατμοσφαιρική πίεση παίζουν σημαντικό ρόλο στον τρόπο και στην ταχύτητα διάδοσης των ηχητικών κυμάτων στον αέρα. Επιπλέον η ταχύτητα του ανέμου επηρεάζει σε σημαντικό βαθμό τα επίπεδα θορύβου στην περιοχή. Έτσι κρίνεται επιτακτική η μέτρηση αυτών των παραμέτρων σε πραγματικό χρόνο. Η μέτρηση και καταγραφή τους θα γίνεται με την χρήση ενός δικτύου ασύρματων κόμβων αισθητήρων.

Εκτός από την χρήση του δικτύου αισθητήρων που είναι επιφορτισμένο με την καταγραφή των ηχητικών κυμάτων του επιβλέποντα χώρου (Κεφάλαιο 4.2), το σύστημα θα κάνει χρήση και ενός επιπλέον ανεξάρτητου δικτύου ασύρματων αισθητήρων. Το επιπλέον αυτό δίκτυο θα αναλάβει:

1. Την μέτρηση και καταγραφή των περιβαλλοντικών συνθηκών που ισχύουν κάθε στιγμή στον επιβλέποντα χώρο. Το δίκτυο αυτό μπορεί να αποτελείται είτε από σταθερούς, είτε από κινητούς κόμβους, είτε από συνδυασμό τους, ανάλογα την επιθυμητή ακρίβεια και τις ιδιαιτερότητες του χώρου. Σε κάθε περίπτωση πάντως είναι απαραίτητη η γνωστοποίηση της ακριβή θέσης των κόμβων του δικτύου κάθε στιγμή.
2. Έτσι το νέο δίκτυο επιφορτίζεται με μια επιπλέον λειτουργία, αυτή της καταγραφής της θέσης των κόμβων κάθε στιγμή. Ο εντοπισμός της θέσης των κόμβων γίνεται με την χρήση ενός δέκτη GPS ο οποίος καταγράφει ανά τακτά διαστήματα της συντεταγμένες του κόμβου. Η συγκεκριμένη λειτουργία είναι χρήσιμη για:
    a. τον εντοπισμό της θέσης των κόμβων που ασχολούνται με την καταγραφή των ακουστικών κυμάτων. (στην περίπτωση όπου οι κόμβοι αυτοί είναι ενσωματωμένοι στις στολές των φυλάκων που κινούνται/επιτηρούν τον επιβλέποντα χώρο.)
    b. τον εντοπισμό της θέσης των κόμβων που ασχολούνται με την καταγραφή των περιβαλλοντικών συνθηκών. (στην περίπτωση όπου και ατοί οι κόμβοι είναι ενσωματωμένοι στις στολές των φυλάκων που κινούνται/επιτηρούν τον επιβλέποντα χώρο.)

4.3.1 Πλατφόρμα ISense

Ο κόμβος που επιλέχθηκε να συγκροτήσει αυτό το δίκτυο καταγραφής περιβαλλοντικών συνθηκών και εντοπισμού της θέσης είναι ο iSense Core Module 2 [73]. Πρόκειται για μια πλατφόρμα αισθητήρων η οποία αναπτύσσεται από την εταιρεία Coalesense σε συνεργασία με το Πανεπιστήμιο του Lübeck. Ο πυρήνας του κόμβου αποτελείται από τον μικρο-ελεγκτή JN5148 της εταιρείας Jennic [72]. Ο JN5148 είναι ένας 32-bit μικρο-ελεγκτής αρχιτεκτονικής RISC ο οποίος έχει δυνατότητα χρονισμού στο εύρος 4 έως 32 MHz. Διαθέτει μνήμη RAM μεγέθους 128 kB που διατίθεται για την αποθήκευση τόσο των εκτελέσιμων όσο και των δεδομένων, δίνοντας έτσι την

δυνατότητα καλύτερης διαχείρισης της μνήμης. Επιπλέον διαθέτει μνήμη Flash μεγέθους 512 kB.

Η ιδιαιτερότητα του μικρο-ελεγκτή JN5148 είναι διαθέτει ενσωματωμένο έναν ασύρματο πομποδέκτη συνδυάζοντας έτσι τις συνήθης λειτουργίες ενός μικρο-ελεγκτή με αυτές τις ασύρματης αποστολής και λήψης δεδομένων. Ο ενσωματωμένος πομποδέκτης λειτουργεί σύμφωνα με το πρότυπο IEEE 802.15.4 [71]. Προσφέρει υψηλούς ρυθμούς μετάδοσης δεδομένων, της τάξης των 250kBit/s. Η ακτίνα εμβέλειας του είναι στα 600 μέτρα σε εξωτερικό χώρο, ενώ ιδιαίτερα σημαντική είναι η δυνατότητα AES κρυπτογράφησης της ασύρματης επικοινωνίας.

Τέλος παρέχει πλήθος περιφερειακών διεπαφών όπως είναι 4 κανάλια αναλογικών εισόδων με 11-bit ADC, 2 κανάλια 10-bit DAC , 2 UARTs και τα πρωτόκολλα επικοινωνίας συσκευών I2C και SPI. Επιπλέον υπάρχει ενσωματωμένη ειδική υποδοχή για την σύνδεση του κόμβου με διάφορες πλακέτες επέκτασης που προσφέρονται από την ίδια την εταιρεία. Με αυτό τον τρόπο ο κόμβος αποκτάει μεγάλη επεκτασιμότητα και μεγάλο εύρος εφαρμογών.

Εικόνα 17: Ο κόμβος iSense Core Module 2.

4.3.2 Πλακέτες επέκτασης του κόμβου iSense

Βασικό χαρακτηριστικό των κόμβων iSense είναι το γεγονός ότι η δομή τους βασίζεται σε ένα πλήθος διαφορετικών μονάδων (modules). Η κάθε μονάδα/πλακέτα έχει τα δικά της ιδιαίτερα χαρακτηριστικά ώστε ο συνδυασμός αυτών να καλύπτει και τις πιο απαιτητικές εφαρμογές. Η μονάδα που αποτελεί των πυρήνα πάνω στον οποίο συνδέονται οι υπόλοιπες είναι ο iSense Core Module 2 (*περιγράφεται στην προηγούμενη παράγραφο*). Οι επιπλέον μονάδες/πλακέτες που διατίθενται από τις εταιρεία Coalesense καλύπτουν ένα ευρύ φάσμα λειτουργιών, παρόλα αυτά στις παρακάτω παραγράφους γίνεται αναφορά στις μονάδες που ικανοποιούν τις ανάγκες της εφαρμογής που περιγράφουμε.

4.3.2.1 Weather Module

Η μονάδα iSense Weather Module ανήκει στο σύνολο των μονάδων που μπορούν να ενσωματωθούν πάνω στον κεντρικό κόμβο iSense Core Module 2 και να του επεκτείνουν τις λειτουργικές του δυνατότητες. Πιο συγκεκριμένα η μονάδα iSense Weather Module παρέχει μετρήσεις υψηλής ακρίβειας για τις συνθήκες του περιβάλλοντος όπως είναι:

1. Η θερμοκρασία
2. Η σχετική υγρασία
3. Η βαρομετρική πίεση.

Εικόνα 18: Η μονάδα περιβαλλοντικών μετρήσεων iSense Weather Module

Τα χαρακτηριστικά της συγκεκριμένης μονάδας φαίνονται στον παρακάτω πίνακα:

Πίνακας 8: Χαρακτηριστικά της μονάδας περιβαλλοντικών μετρήσεων iSense Weather Module

Θερμοκρασία και σχετική υγρασία	
Ακρίβεια (t/rh)	1°C/3%
Ανάλυση (t/rh)	0.1°C/0.1%
Εύρος (t/rh)	-20 .. +70°C/0..100%
Κατανάλωση σε κατάσταση λειτουργίας	~800μA
Κατανάλωση σε κατάσταση αναμονής	~0.5μA
Βαρομετρική πίεση	
Εύρος	10..1100 mbar
Ανάλυση	0.1 mbar
Ακρίβεια	1.5mbar
Συχνότητα	1Hz
Κατανάλωση σε κατάσταση λειτουργίας	~1mA
Κατανάλωση σε κατάσταση αναμονής	<0.1μA

4.3.2.2 GPS Module

Ο εντοπισμός της θέσης των κόμβων γίνεται με την χρήση του iSense GPS Module. Πρόκειται για μια μονάδα επέκτασης του κόμβου iSense Core Module όπου του δίνει την δυνατότητα χρήσης ενός GPS δέκτη. Η μονάδα iSense GPS Module βασίζεται στο ολοκληρωμένο SiRF Star 3. Παρέχει δεδομένα μεγάλης ακριβείας και μπορεί να συνεργαστεί αποδοτικά με συστήματα όπως το SBAS (WAAS, EGNOS, MSAS). Η μονάδα αποτελείται από έναν δέκτη μεγάλης απόδοσης, μια ενσωματωμένη μικρο-μπαταρία η οποία χρησιμοποιείται για την διατήρηση προσωρινών δεδομένων που βοηθούν στην άμεση επικοινωνία με τους δορυφόρους και ένα LED το οποίο παρέχει τις απαραίτητες ενδείξεις για την επικοινωνία με τους δορυφόρους.

Εικόνα 19: Η μονάδα iSense GPS Module

Τα χαρακτηριστικά της μονάδας iSense GPS Module φαίνονται στον παρακάτω πίνακα:

Πίνακας 9: Χαρακτηριστικά της μονάδας εντοπισμού θέσης iSense GPS Module

Δέκτης GPS	
Ολοκληρωμένο	SiRF Star 3 GSC3f
Κανάλια	20
Συχνότητα ανανέωσης	1 Hz
Χρόνος λήψης δεδομένων (open sky)	
Hot start	< 2 s
Cold start (typical)	30 s
Ακρίβεια	
Autonomous	< 10 m (2D RMS)
SBAS	< 5 m (2D RMS)
Ηλεκτρικά χαρακτηριστικά	
Τάσης τροφοδοσίας	3.3 V
Κατανάλωση σε κατάσταση λειτουργίας	~ 50 mA
Κατανάλωση σε κατάσταση αναμονής	0 mA

4.3.2.3 Ανεμόμετρο

Για την καταγραφή της ταχύτητας και της κατεύθυνσης του ανέμου δεν παρέχεται κάποιο έτοιμο module από το iSense. Παρόλα αυτά από την εταιρεία παρέχεται μια ειδική πλακέτα επέκτασης γενικού τύπου, η iSense Measurement Module. Η συγκεκριμένη πλακέτα γενικού τύπου διαθέτει ένα σύνολο από 34 υποδοχές οι οποίες μπορούν να χρησιμοποιηθούν για καταγραφή σημάτων από εξωτερικούς αισθητήρες.

Την καταγραφή των ιδιοτήτων του ανέμου την αναλαμβάνει ένα ανεμόμετρο τύπου model7911 της εταιρείας Davis Instruments. Το συγκεκριμένο ανεμόμετρο περιλαμβάνει αισθητήρες μέτρησης της ταχύτητας και της κατεύθυνσης του ανέμου. Η ευαισθησία των αισθητήρων καταγραφής καθώς και η κατασκευή του κάνει το συγκεκριμένο ανεμόμετρο ικανό να παρέχει ακριβής μετρήσεις για όλους τους τύπους ανέμου, από ένα ήρεμο αεράκι μέχρι και έναν δυνατό τυφώνα.

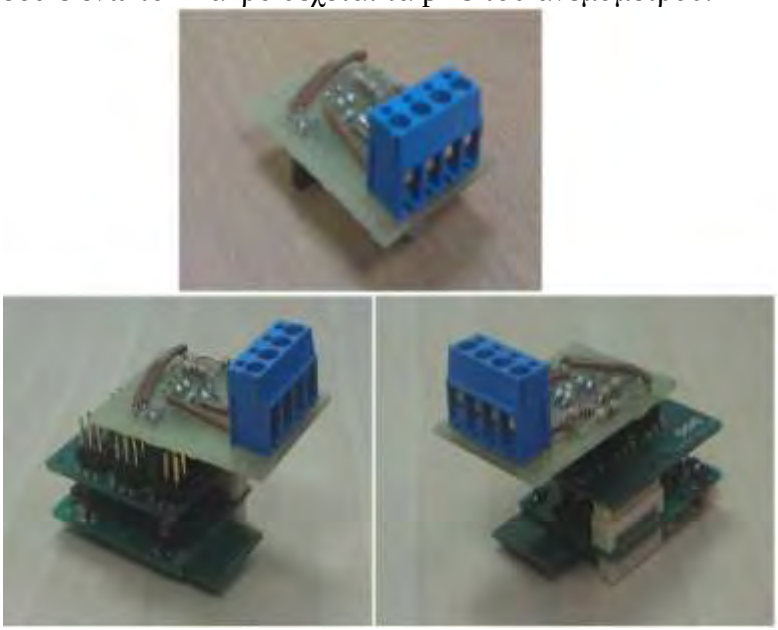
Εικόνα 20: Η πλακέτα επέκτασης γενικού τύπου iSense Core Module

Πίνακας 10: Χαρακτηριστικά του ανεμομέτρου model7911 της εταιρείας Davis Instruments.

Ταχύτητα Ανέμου	
Εύρος	3 - 175 mph, 3 - 150 knots, 1.5 - 79 m/s, 5 - 282 km/h
Ακρίβεια	±3 mph (3 kts, 5 km/h, 1.5 m/s)
Ανάλυση	±3 mph (3 kts, 5 km/h, 1.5 m/s
Κατεύθυνση Ανέμου	
Εύρος	0° - 360°
Ακρίβεια	±7°
Ανάλυση	1° (0° - 355°)
Μηχανικά Χαρακτηριστικά	
Διαστάσεις	18.5" x 7.5" x 4.75" (470 mm x 191 mm x 121 mm)
Βάρος	2 lbs. 15 oz. (1.332 kg)

Εικόνα 21: Το ανεμόμετρο model7911 της εταιρείας Davis Instruments

Η ενσωμάτωση του ανεμομέτρου στις αντίστοιχες υποδοχές (pins) της πλακέτας iSense Measurement Module επιτυγχάνεται με την υλοποίηση μια ειδικής διεπαφής. Η συγκεκριμένη διεπαφή διαθέτει 2 άκρα. Το ένα άκρο της τοποθετείται πάνω στα pins του Measurement Module ενώ το $2^{ο}$ άκρο δέχεται τα pins του ανεμομέτρου.



Εικόνα 22: Η διεπαφή διασύνδεσης του ανεμομέτρου με την πλακέτα επέκτασης iSense Measurement Module

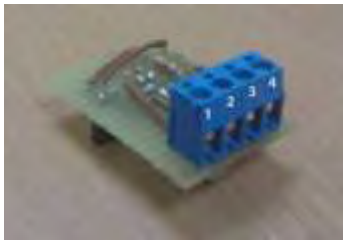
Το ανεμόμετρο διαθέτει τέσσερις υποδοχές (pins):

1. Την έξοδο του αισθητήρα καταγραφής της ταχύτητας του ανέμου. (παράγει έξοδο τάσης 0 – 2.5V).
2. Την έξοδο του αισθητήρα καταγραφής της κατεύθυνσης του ανέμου. (παράγει έξοδο τάσης 0 – 2.5V).
3. Την υποδοχή της γείωσης.
4. Την υποδοχής της τάσης. Δέχεται 2.5V.

Η διεπαφή αναλαμβάνει να υλοποιήσει τις παρακάτω συνδέσεις:

- το pin 1 με την $1^{η}$ αναλογική είσοδο του Measurement Module
- το pin 2 με την $1^{η}$ αναλογική είσοδο του Measurement Module

- το pin 3 με την γείωση του Measurement Module
- το pin 4 με την τάση του Measurement Module. Επειδή η τάση που δίνει το iSense είναι 3.3 V και η τάση που χρειάζεται το ανεμόμετρο είναι 2.5 V, χρησιμοποιήθηκε μια διάταξη για την πτώση της τάσης από τα 3.3 στα 2.5.



Εικόνα 23: Οι υποδοχές της διεπαφής διασύνδεσης του ανεμομέτρου με την πλακέτα iSense Measurements Module

Επιπλέον το 4 συνδέεται με την 3η αναλογική είσοδο του Measurement Module. Αυτό γίνεται για να μπορούμε να έχουμε κάθε στιγμή την τάση τροφοδοσίας του ανεμομέτρου. Η νέα τάση μπορεί να μεταβάλλεται, ανάλογα με την διακύμανση της τάσης που παρέχουν οι μπαταρίες.

Οι μετρήσεις που καταγράφονται από τις 2 αναλογικές εισόδου του Measurement Module αφορούν την τάση που βγάζουν στα άκρα τους τα δύο αισθητήρια όργανα του ανεμομέτρου (ταχύτητα & κατεύθυνση ανέμου). Η μετατροπή αυτών των τάσεων σε κατάλληλες μονάδες μέτρησης γίνεται με τις παρακάτω συναρτήσεις μετατροπής.

Ταχύτητα ανέμου

Για την μέτρηση της ταχύτητας του ανέμου, σε κάθε στροφή της φτερωτής καταγράφεται ένας παλμός. Τον παλμό αυτό, τον λαμβάνουμε μέσω της 1ης αναλογικής εισόδου του Measurement Module. Τον πλήθος των παλμών σε κάποιο συγκεκριμένο χρονικό διάστημα, εκφράζει την ταχύτητα του ανέμου. Έτσι η μέση ταχύτητα του ανέμου **(**όπου μετράμε το πλήθος των παλμών για 30 sec) υπολογίζεται από τον τύπο:

$$wind\_speed = \frac{counter * 3.62}{3} + 0.5$$

,όπου counter είναι το πλήθος των παλμών και η ταχύτητα του ανέμου εκφράζεται σε kph.

Κατεύθυνση ανέμου

Για την μέτρηση της κατεύθυνσης του ανέμου, καταγράφεται η τάση στο άκρου του αισθητήριου οργάνου. Η τάση αυτή αντιστοιχεί στην γωνία κατεύθυνσης του ανέμου. Αυτή την τάση την λαμβάνεται από την 2η αναλογική είσοδο του Measurement Module. Για την μετατροπή της τάσης σε μοίρες χρησιμοποιούμαι τον τύπο:

$$wind\_direction = \frac{value * 356}{voltage} + 0.5$$

,όπου value είναι η τιμή που διαβάζουμε από την 2η αναλογική είσοδο, και voltage είναι η τιμή της τάσης τροφοδοσίας του ανεμομέτρου, την οποία διαβάσουμε από την 3η αναλογική είσοδο του Measurement Module.

Εικόνα 24:Ο ασύρματος κόμβος καταγραφής των συνθηκών του ανέμου

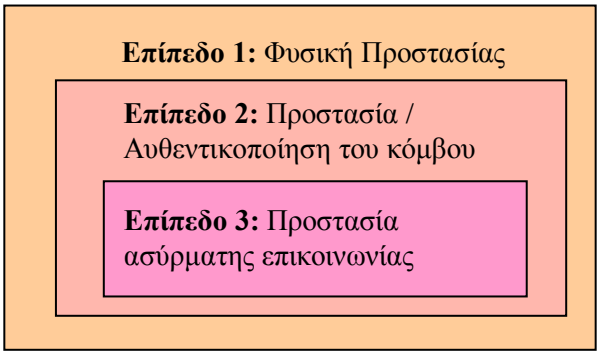
5 *Πλαίσιο Υπηρεσιών Ασφάλειας των κόμβων*

Σημαντικό ρόλο στην δημιουργία ενός αποτελεσματικού συστήματος επιτήρησης χώρων αποτελεί και η διαφύλαξη του ίδιου του συστήματος από εχθρικούς ή κακόβουλους χρήστες. Όπως αναφέραμε παραπάνω, το σύστημα θα βασίζεται στην χρήση κόμβων που θα βρίσκονται διάχυτοι στον χώρο και πάνω στις στολές των στρατιωτών και θα επικοινωνούν ασύρματα δημιουργώντας ένα ασύρματο δίκτυο αισθητήρων. Αυτή η ενσωμάτωση των κόμβων στον , προς επιτήρηση, χώρο έχει σα αποτέλεσμα οι κόμβοι να είναι εύκολα προσβάσιμοι από εχθρικούς ή κακόβουλους χρήστες οι οποίοι μπορούν να αποκτήσουν πρόσβαση στο σύστημα και να επηρεάσουν ή να αλλάξουν τις μετρήσεις, την ακρίβεια των μετρήσεων καθώς και την εύρυθμη λειτουργία ολόκληρου του συστήματος.

Η διαφύλαξη των κόμβων από μη-εξουσιοδοτημένους χρήστες καθώς και η προστασίας της ασύρματης τους επικοινωνίας αποτελεί μια πρόκληση, λόγω των ελάχιστων πόρων που διαθέτουν. Η χρήση υπαρχόντων τεχνικών ασφάλειας που είναι διαδεδομένες στους υπολογιστές και στα ad-hoc δίκτυα αποτελούν απαγορευμένες λύσεις για τα δίκτυα ασύρματων αισθητήρων εξαιτίας των λειτουργικών περιορισμών που έχουν οι κόμβοι, όπως είναι: η μειωμένη επεξεργαστική τους ικανότητα, το μικρό μέγεθος της μνήμης που διαθέτουν καθώς και η μειωμένη τους διαθεσιμότητα σε ενέργεια.

Στις παρακάτω παραγράφους περιγράφεται ένα πλαίσιο υπηρεσιών ασφαλείας το οποίο λαμβάνει υπόψη τους περιορισμούς των κόμβων. Πρόκειται για ένα σύνολο αλγορίθμων με χαμηλές απαιτήσεις οι οποίοι εξασφαλίζουν την ασφάλεια των κόμβων και των μετρήσεων τους από κάθε προσπάθεια μη-εξουσιοδοτημένης πρόσβασης. Επιπλέον προσφέρουν την δυνατότητα έγκαιρης ειδοποίησης στην περίπτωση που κάποιος μη-εξουσιοδοτημένος χρήστης καταφέρει και αποκτήσεις πρόσβαση. Ουσιαστικά, πρόκειται για ένα πολύ-επίπεδο σύνολο λειτουργιών ασφαλείας το οποίο βασίζεται στην:

1. Φυσική προστασία του κόμβου
2. Προστασία και αυθεντικοποίηση των εκτελέσιμων προγραμμάτων του κόμβου μέσω της χρήσης “sand-boxing” τεχνικών.
3. Προστασία της ασύρματης επικοινωνίας μέσω τεχνικών κρυπτογράφησης [113].



Εικόνα 25: Πολύ-επίπεδο πλαίσιο προστασίας

5.1 Υφιστάμενοι Μέθοδοι

Οι επιθέσεις στα δίκτυα αισθητήρων μπορούν να ταξινομηθούν στις κατηγορίες:

1. Φυσικές επιθέσεις στους κόμβους αισθητήρων. Επιθέσεις που ανήκουν στην κατηγορία αυτή είναι η καταστροφή του κόμβου, η ανάλυση και ο επαναπρογραμματισμός του.
2. Επιθέσεις με σκοπό την παρεμπόδιση βασικών λειτουργιών του δικτύου, όπως είναι οι λειτουργίες δρομολόγησης και εντοπισμού των κόμβων του δικτύου.
3. Επιθέσεις με σκοπό τα δεδομένα, όπως είναι η παρακολούθηση την ανταλλαγής δεδομένων αλλά και η αλλοίωση τους.
4. Επιθέσεις με σκοπό την δέσμευση και κατανάλωση των πόρων των κόμβων με σκοπό την παρεμπόδιση της λειτουργίας τους και την πρόωρη καταστροφή του δικτύου. (denial-of-service attacks)

Μια από τις πιο σοβαρές επιθέσεις σε δίκτυα αισθητήρων που βρίσκονται σε μη προστατευόμενο χώρο είναι η φυσική πρόσβαση σε αυτά και η αλλοίωση τους από μη-εξουσιοδοτημένα άτομα. Ένας κακόβουλος χρήστης μπορεί εύκολα να αποκτήσει πρόσβαση στον κόμβο, να τον αναλύσει, να αναλύσει τα προγράμματα που εκτελεί και τέλος να τοποθετήσει δικά του προγράμματα δημιουργώντας έτσι έναν «χειραγωγημένο» - ελέγξιμο, από τον κακόβουλο χρήστη, κόμβο. Με αυτόν τον τρόπο, ο κακόβουλος χρήστης μπορεί να παρακολουθεί όλα τα δεδομένα που υπάρχουν στο δίκτυο, να τα αλλοιώνει, να δημιουργεί ψεύτικα δεδομένα αλλά και να παρεμποδίζει την λειτουργία των υπόλοιπων κόμβων του δικτύου.

Παραδοσιακά, η θωράκιση των συσκευών από κακόβουλους χρήστες βασίζεται στην χρήση κατάλληλου υλικού [74,75]. Παρόλα αυτά η χρήση θωράκισης που βασίζεται σε ειδικευμένο υλικό δεν είναι αποδεκτή σε δίκτυα αισθητήρων καθώς: α) η λειτουργία του εξειδικευμένου υλικού είναι αρκετά ενεργοβόρα καθιστώντας την έτσι ακατάλληλη για χρήση στα δίκτυα αισθητήρων. β) η χρήση εξειδικευμένου υλικού προστασίας δεν είναι πάντοτε ασφαλής λύση λόγω των διάφορων τεχνικών προσπέλασης των κόμβων που υπάρχουν [74,76,77]

Εναλλακτικά στην χρήση εξειδικευμένου υλικού προστασίας, υπάρχουν διάφορες προσεγγίσεις θωράκισης των κόμβων με την χρήση κατάλληλων λογισμικών. Οι προσεγγίσεις αυτές μπορούν να χωριστούν στις κατηγορίες:

1. Μετάλλαξη του κώδικά, ώστε να είναι δύσκολη η ανάλυση και η επεξεργασία του (code obfuscation technique) [78-81]
2. Ο έλεγχος της εγκυρότητας ενδιάμεσων αποτελεσμάτων που παράγουν τα προγράμματα (result checking technique) [82-84]
3. Η χρήση κρυπτογραφημένων προγραμμάτων, τα οποία αποκρυπτογραφούνται ακριβώς πριν την εκτέλεση τους (self-decrypting programs) [85-86]
4. Η ενσωμάτωση ειδικού λογισμικού ελέγχου μέσα στην εφαρμογή. Αυτός ο ελεγκτικός μηχανισμός ελέγχει διάφορες τιμές/μεταβλητές της εφαρμογής, όπως είναι ο αριθμός hash της, με σκοπό τον έλεγχο της ακεραιότητάς της. (self-checking code) [85,87,88]
5. Η χρήση ειδικού λογισμικού επιβεβαίωσης με σκοπό τον απομακρυσμένο έλεγχο της ακεραιότητας του λογισμικού του κόμβου (software based Attestation) [93]

Παρόλα αυτά, οι περισσότερες από τις προαναφερθέντες προσεγγίσεις δεν βρίσκουν εφαρμογή στα δίκτυα αισθητήρων εξαιτίας των υψηλών επεξεργαστικών απαιτήσεων που έχουν.

Το ειδικό λογισμικό επιβεβαίωσης αναφέρεται σε ένα πρωτόκολλο ερωταπόκρισης (challenge –response protocol). Στο πρωτόκολλο αυτό λαμβάνουν μέρος δύο ρόλοι, αυτός του εξεταστή (verifier) και αυτός του εξεταζόμενου (attester). Ο εξεταστής (π.χ. ένας σταθμός βάσης) στέλνει μια αίτηση επιβεβαίωσης στο εξεταζόμενο κόμβο, ζητώντας του συγκεκριμένες πληροφορίες σχετικά με την κατάσταση λειτουργίας του. Οι πληροφορίες αυτές θα χρησιμοποιηθούν σαν αποδεικτικά στοιχεία για την ακεραιότητα του εξεταζόμενου, καθώς μπορούν να υπολογισθούν σωστά μόνο στην περίπτωση όπου ο εξεταζόμενος είναι «ακέραιος». Έπειτα, ο εξεταστής λαμβάνει την απάντηση του εξεταζόμενου και συγκρίνει τα δεδομένα που έλαβε με τα δικά του γνωστά και έγκυρα δεδομένα. Στην περίπτωση όπου ο έλεγχος είναι επιτυχής, το δίκτυο συνεχίζει κανονικά την λειτουργία του καθώς δεν υπάρχει πρόβλημα με την ακεραιότητα του εξεταζόμενου, εναλλακτικά το δίκτυο «αποβάλει» τον κόμβο καθώς κάποιος έχει αποκτήσει πρόσβαση στο λογισμικό του. [90-93]

Η φυσική κάλυψη ενός κόμβου αποτελεί το πρώτο εμπόδιο που καλείται να υπερβεί κάποιος επιτιθέμενος ώστε να αποκτήσει πρόσβαση στο εσωτερικό του. Συνήθως αυτή η φυσική κάλυψη αποτελείται από παθητικούς μηχανισμούς προστασίας, όπως είναι οι διάφορες προστατευτικές επενδύσεις και οι σφραγίδες πρόσβασης. Οι μηχανισμοί αυτοί είναι εφαρμόσιμοι στα δίκτυα αισθητήρων καθώς δεν απαιτούν κάποιο επιπλέον κύκλωμα και δεν έχουν καμία ενεργειακή απαίτηση για την λειτουργία τους. Ο κύριος στόχος αυτών των μηχανισμών είναι να δυσκολέψει τον εισβολέα, ώστε να είναι πολύ σπάταλη από άποψη χρόνου και προσπάθειας η απόκτηση πρόσβασης στον κόμβο. [112]

5.2 Επίπεδα Ασφαλείας

Το σύστημα μπορεί να δεχτεί πολλά και διαφορετικά είδη επιθέσεων, όπως είναι η φυσική πρόσβαση στον κόμβο και η λήψη και αλλοίωση των δεδομένων τους. Η

προστασία του κόμβου από αυτές τις διαφορετικού τύπου επιθέσεις επιβάλει την εφαρμογή διαφορετικών μεθόδων αντιμετώπισης τους. Το σύνολο αυτών των λειτουργιών και πρωτοκόλλων συγκροτεί ένα πολύ-επίπεδο πλαίσιο λειτουργιών ασφαλείας, το οποίο είναι ικανό είτε να αντιμετωπίσει, είτε να ανιχνεύσει τις επιθέσεις αυτές. Παρακάτω γίνεται μια περιγραφή των επιπέδων αυτών.

5.2.1 Επίπεδο ασφάλειας της φυσικής πρόσβασης

Το πρώτο επίπεδο αναλαμβάνει να εμποδίσει τους κακόβουλους χρήστες να αποκτήσουν άμεση πρόσβαση στον κόμβο. Η χρήση παθητικών μηχανισμών προστασίας θεωρούνται ως η καλύτερη λύση σε αυτό το επίπεδο, καθώς η απουσία οποιουδήποτε κυκλώματος για την λειτουργία τους εκμηδενίζει τις ενεργειακές τους απαιτήσεις. Βέβαια η αποτελεσματικότητά τους στην παροχή ασφάλειας είναι χαμηλή, για αυτό και δεν θεωρείται ιδιαίτερα ασφαλή λύση για την παροχή προστασίας της φυσικής πρόσβασης στα ασύρματα δίκτυα αισθητήρων. Παρόλα αυτά αποτελεί το πρώτο επίπεδο του πλαισίου ασφαλείας μας έχοντας στόχο την παρεμπόδιση των μη-εξειδικευμένων αλλά και την καθυστέρηση των εξειδικευμένων εχθρών.

5.2.2 Επίπεδο αυθεντικοποίησης και ακεραιότητας του κόμβου

Το δεύτερο επίπεδο ασφάλειας αναλαμβάνει τη εκτέλεση διάφορων τεχνικών εξόρυξης πληροφοριών με σκοπό την εξαγωγή συμπεράσματος σχετικά με την αυθεντικοποίηση και τη ακεραιότητα των κόμβων σε πραγματικό χρόνο. Πιο συγκεκριμένα, το επίπεδο αυτό ελέγχει την αυθεντικότητα και την ακεραιότητα των προγραμμάτων που εκτελούνται από τον κάθε κόμβο. Ο έλεγχος των προγραμμάτων γίνεται μέσα από μια διαδικασία η οποία είναι ειδικά σχεδιασμένη ώστε:

1. Να αποτρέπει την αλλοίωση / την χρήση / τον επαναπρογραμματισμό των κόμβων.
2. Να βασίζεται αποκλειστικά σε λογισμικό. Να μην απαιτεί, δηλαδή, την ύπαρξη κάποιου εξειδικευμένου υλικού.
3. Να λειτουργεί αποδοτικά σε συσκευές με περιορισμένους πόρους.
4. Η εκτέλεση των διάφορων ελέγχων να μην προσθέτει μεγάλο φόρτο στις συσκευές και στα κανάλια επικοινωνίας.

Η εκτέλεση των λειτουργιών αυθεντικοποίησης και ακεραιότητας στηρίζεται πάνω στον μηχανισμό του sandbox. Πρόκειται για έναν μηχανισμό ασφάλειας όπου επιτρέπει τον διαχωρισμό προγραμμάτων που εκτελούνται ταυτόχρονα σε μια συσκευή. Χρησιμοποιείται πολύ συχνά για την εκτέλεση δοκιμαστικών ή μη-έμπιστων προγραμμάτων. Ουσιαστικά, παρέχει ένα πλήρως ελεγχόμενο σύνολο πόρων όπως ορισμένο χώρο στον δίσκο και στην μνήμη της συσκευής με σκοπό την εκτέλεση προγραμμάτων στο εσωτερικό τους.

Το πλαίσιο ασφαλείας που περιγράφεται χρησιμοποιεί την τεχνική sandbox ώστε να χωρίσει τον χώρο εκτέλεσης των προγραμμάτων των κόμβων σε ξεχωριστά ανεξάρτητα κομμάτια. *(Τα ανεξάρτητα αυτά κομμάτια πλέον στο κείμενο να αναφέρονται με τον όρο isolates.)*

Υπάρχουν δύο ειδών isolates [99]:

1. Τα isolates που χρησιμοποιούνται για λειτουργίες ασφαλείας. (Security-Dedicated Isolates. *Πλέον στο κείμενο θα αναφέρονται ως SDI*)
2. Τα isolates που χρησιμοποιούνται για την εκτέλεση των συνηθισμένων λειτουργιών του κόμβου. (Work-Dedicated Isolates. *Πλέον στο κείμενο θα αναφέρονται ως WDI*)

Στο σύστημα υπάρχει, επιπλέον, ένας εξυπηρετητής εγκυροποίησης των isolates (Isolate Verification Server, *Πλέον στο κείμενο θα αναφέρεται ως IVS*). Ο IVS αναλαμβάνει να ελέγχει τη εγκυρότητα και την γνησιότητα των διάφορων WDI των κόμβων. Ο έλεγχος της εγκυρότητας των WDI βασίζεται:

1. Στην λήψη στιγμιότυπων της μνήμης RAM των WDI (RAM dumping technique)
2. Σε hashing τεχνικές

5.2.3 Επίπεδο κρυπτογραφίας

Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιήθηκε στο σύστημα ανήκει στην οικογένεια αλγορίθμων κρυπτογράφησης Tiny Encryption Algorithm (TEA). Πρόκειται για έναν αλγόριθμο κρυπτογράφησης ο οποίος είναι σχεδιασμένος με σκοπό την ελαχιστοποίηση των απαιτήσεων σε μνήμη και την μεγιστοποίηση της ταχύτητας εκτέλεσης του [104]. Η οικογένεια των TEA αλγορίθμων κρυπτογράφησης από τελείται από 3 αλγορίθμους: τον βασικό TEA καθώς και 2 επεκτάσεις του βασικού, του XTEA και XXTEA. Παρόλο την πολύ καλή αποδοτικότητα του βασικού αλγορίθμου, οι 2 επεκτάσεις του προσφέρουν πιο ασφαλή κρυπτογραφικά αποτελέσματα. Στις επόμενες παραγράφους θα γίνει μια λεπτομερή περιγραφή των αλγορίθμων, των αδυναμιών που έχουν, της αποτελεσματικότητάς τους στα δίκτυα αισθητήρων καθώς και την ενσωμάτωσή τους στο σύστημα με σκοπό την ασφάλιση του επιπέδου επικοινωνίας των κόμβων [100-102].

Οι αλγόριθμοι κρυπτογράφησης TEA μπορούν να χαρακτηριστούν ως πραγματικά "αδιάσπαστοι" όταν ισχύουν οι παρακάτω συνθήκες:

- Η διαμοίραση των κλειδιών να έχει γίνει σε όλους του κόμβους με ασφαλή τρόπο.
- Κάθε μήνυμα να κρυπτογραφείτε με ένα ασφαλές μοναδικό κλειδί.
- Η γεννήτρια κλειδιών να λειτουργεί με πραγματικά τυχαίο τρόπο.

Η αποδοτική χρήση των TEA αλγορίθμων κρυπτογράφησης από το σύστημα επιβάλει την ικανοποίηση των παραπάνω συνθηκών. Για αυτό τον σκοπό, κάθε κόμβος χρησιμοποιεί μια αποθήκη μοναδικών κλειδιών. Η αποθήκη αυτή αποτελείται από 120 κλειδιά τα οποία έχουν δημιουργηθεί από μια γεννήτρια τυχαίων αριθμών. Η αποθήκη αυτή έχει δημιουργηθεί μια φορά, κατά την διάρκεια αρχικοποίησης του συστήματος, είναι κοινή για όλους τους κόμβους του συστήματος και μεταφέρεται σε ασφαλή μνήμη στο εσωτερικό των κόμβων κατά την διάρκεια του προγραμματισμού τους.

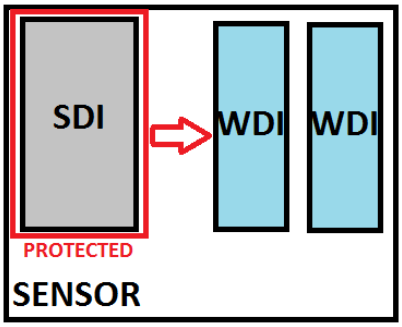
Η δημιουργία πραγματικά τυχαίων αριθμών επιτυγχάνεται με την χρήση μιας γεννήτριας τυχαίων αριθμών η οποία έχει σχεδιαστεί από το Πανεπιστήμιο του Trinity [98]. Η τυχαιότητα της συγκεκριμένης γεννήτριας βασίζεται στο γεγονός ότι χρησιμοποιεί ως πηγή εντροπίας τον ατμοσφαιρικό θόρυβο. Ο συγκεκριμένος θόρυβος

καταγράφεται από μια κεραία η οποία είναι συντονισμένη σε μια ασύρματη συχνότητα, την οποία δεν χρησιμοποιεί κανένας άλλος. Στην συνέχεια ο θόρυβος ψηφιοποιείται σε ένα σήμα ανάλυσης 8-bit με συχνότητα δειγματοληψίας τα 8KHz. Από τα 8bit του κάθε στιγμιότυπου του σήματος κρατιέται μόνο το τελευταίο bit το οποίο συνδυάζεται με τα αντίστοιχα τελευταία bit των υπόλοιπων στιγμιότυπων του σήματος. Το αποτέλεσμα αυτής της διαδικασίας είναι η δημιουργία μιας σειράς από bits με εξαιρετικά μεγάλη εντροπία.

5.3 Πλαίσιο Λειτουργιών Ασφαλείας

5.3.1 Η τεχνική sandbox

Η προστασία των κόμβων από την εκτέλεση malicious προγραμμάτων επιτυγχάνεται με την χρήση της τεχνικής sandbox. Η χρήση της συγκεκριμένης τεχνικής ορίζει τον διαχωρισμό των χώρων εκτέλεσης των διάφορων προγραμμάτων του κόμβου, ώστε να εκτελούνται ανεξάρτητα. Όπως αναφέραμε παραπάνω, υπάρχουν δύο κατηγορίες προγραμμάτων, τα “SDI” και τα “WDI”. Παρόλο που σε έναν κόμβο μπορούν να εκτελούνται ταυτόχρονα περισσότερα από ένα SDI στο πλαίσιο λειτουργιών ασφαλείας που περιγράφεται χρησιμοποιείται μόνο ένα ανά κόμβο. Από την άλλη, περισσότερα από ένα WDI εκτελέσιμα λειτουργούν στο εσωτερικό ενός κόμβου εκτελώντας διάφορες λειτουργίες (Εικόνα 21). Η διεργασία του ελέγχου της ακεραιότητας του κόμβου επαφίεται στον έλεγχο των WDI εκτελέσιμων. Έτσι στη περίπτωση όπου κάποιο από τα WDI του κόμβου δεν αποδειχθεί έγκυρο, αυτόματα και ο ίδιος ο κόμβος θεωρείται επικίνδυνος.



Εικόνα 26: Τα isolates ενός κόμβου αισθητήρων

5.3.2 Εκτελέσιμο ασφάλειας – Security Dedicated Isolates – SDI

Το SDI αποτελεί στην ουσία ένα εργαλείο παρακολούθησης και ανάλυσης στοιχείων ειδικά σχεδιασμένο για την χρήση σε κόμβους αισθητήρων. Εκτελείται είτε περιοδικά είτε έπειτα από απαίτηση και καλείται να συμπεράνει σχετικά με το αν κάποιος κόμβος έχει καταληφθεί ή όχι. Κάθε SDI διαθέτει ένα μοναδικό αναγνωριστικό/κλειδί, το SDI_ID, το οποίο χρησιμοποιείται για την επικοινωνία του SDI του κόμβου με τον εξυπηρετητή εγκυροποίησης των εκτελέσιμων (IVS). Κατά την διάρκεια της πρώτης εκτέλεσης του SDI στον κόμβο, γίνεται λήψη ενός αποτυπώματος της μνήμης του και

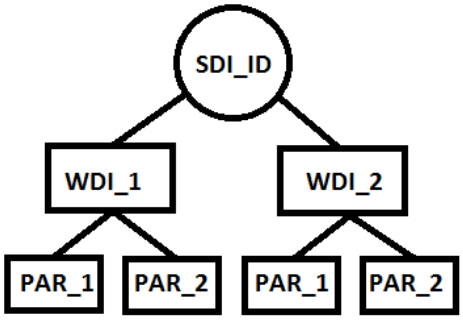
υπολογισμός της κατάσταση του. Αυτά τα αποτελέσματα στέλνονται στον IVS όπου και αποθηκεύονται σε μια κατάλληλη βάση, την Isolate Verification Database (IVDB). Τα περιεχόμενα αυτής της βάσης αποτελούν τις έγκυρες πληροφορίες που θα χρησιμοποιεί ο IVS ώστε να συγκρίνει την εγκυρότητα των κόμβων του δικτύου κατά την διάρκεια της κανονικής τους εκτέλεσης.

Οι λειτουργίες για τις οποίες είναι υπεύθυνο το SDI είναι:

1. Να επικοινωνεί με ασφάλεια με τον IVS
2. Να ελέγχει τα WDI
3. Να ενεργεί ελέγχους για την ανίχνευση εισβολέων

5.3.3 Εκτελέσιμο εργασίας – Work Dedicated Isolates – WDI

Το WDI αναλαμβάνει την εκτέλεση των καθημερινών λειτουργιών ενός κόμβου αισθητήρων. Εξαιτίας της τεχνολογία sandbox, περισσότερα από ένα WDI μπορούν να εκτελούνται ταυτόχρονα στο εσωτερικό ενός κόμβου (Εικόνα 22). Κάθε WDI που εκτελείται από κάποιο κόμβο ελέγχεται για την εγκυρότητα του. Η μη επαλήθευσή κάποιου WDI οδηγεί αυτόματα στην λήψη αντίμετρων από το SDI του κόμβου.



Εικόνα 27: Κάθε WDI του κόμβου συνδυάζεται με τις παραμέτρους εκτέλεσής του και το μοναδικό αναγνωριστικό SDI_ID του κόμβου.

Το αποτύπωμα του κάθε WDI εκτελέσιμου μαζί με τις απαραίτητες παραμέτρους του βρίσκονται αποθηκευμένα στη βάση IVDB. Στην βάση το αποτύπωμα κάθε WDI συνδυάζεται με το SDI_ID αναγνωριστικό του αντίστοιχου SDI. Η δημιουργία του αποτυπώματος του κάθε WDI γίνεται με την χρήση των παρακάτω τεχνικών:

1. Λήψη στιγμιότυπου της μνήμης RAM του εκτελέσιμου και
2. Υπολογισμός της hash τιμής του.

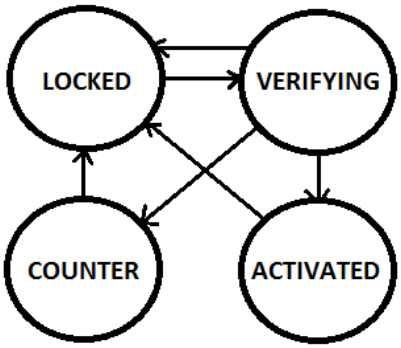
5.3.4 Διάγραμμα εναλλαγής καταστάσεων

Κάθε κόμβος αισθητήρων, στον οποίο εφαρμόζεται το συγκεκριμένο πλαίσιο ασφαλείας, κατά την λειτουργία του βρίσκεται σε μια από τις τέσσερις παρακάτω καταστάσεις:

1. “LOCKED” – (ΚΛΕΙΔΩΜΕΝΟ)
2. “VERIFYING” – (ΕΛΕΓΧΌΜΕΝΟ)
3. “ACTIVATED” – (ΕΝΕΡΓΟΠΟΙΗΜΕΝΟ)

4. “COUNTERMEASURES” – (ΥΠΟ ΕΠΙΤΗΡΗΣΗ)

Κατά την εκκίνησή του, κάθε κόμβος του δικτύου βρίσκεται στην κατάσταση LOCKED. Παραμένει σε αυτή την κατάσταση μέχρι να ολοκληρωθεί με επιτυχία η διαδικασία αυθεντικοποίησης του από τον IVS. Πριν την επιτυχή ολοκλήρωση της αυθεντικοποίησης καμία άλλη λειτουργία δεν μπορεί να εκτελεστεί από τον κόμβο. Αφού ολοκληρωθεί με επιτυχία η διαδικασία αυθεντικοποίησης, η κατάσταση του κόμβου αλλάζει στην VERIFYING. Σε αυτή την κατάσταση, ο κόμβος ελέγχεται για την ακεραιότητα του από τον IVS. Εκτελούνται οι διάφορες μέθοδοι και τα αποτελέσματα αποστέλλονται στον IVS όπου και συγκρίνονται με τα σωστά αποτελέσματα που βρίσκονται αποθηκευμένα στην IVDB βάση. Αν η σύγκριση αποτύχει, ο κόμβος επιστρέφει στην κατάσταση LOCKED και αποκλείεται από το δίκτυο. Από την άλλη, όταν η σύγκριση είναι επιτυχής, ο κόμβος πηγαίνει στην κατάσταση ACTIVATED και τα WDI του κόμβου ξεκινούν κανονικά την εκτέλεσή τους. Περιοδικά το SDI του κόμβου εκτελεί διαδικασίες επανελέγχου της εγκυρότητάς του. Αυτοί οι περιοδικοί επανέλεγχοι μπορούν είτε να διατηρήσουν τον κόμβο στην κατάσταση ACTIVATED (περίπτωση επιτυχής ελέγχου) είτε να θέσουν τον κόμβο στις καταστάσεις LOCKED και COUNTERMEASURES (περιπτώσεις ανεπιτυχούς ελέγχου). Κάποιος κόμβος μπαίνει στην κατάσταση COUNTERMEASURES όταν αρχικά έχει περάσει τους ελέγχους και έχει γίνει δεκτός στο δίκτυο και έπειτα καταλαμβάνεται από κάποιον κακόβουλο χρήστη. Η κατάσταση COUNTERMEASURES ουσιαστικά είναι μια ενδιάμεση κατάσταση όπου χρησιμοποιείται κυρίως για την αντιμετώπιση συντονισμένων επιθέσεων σε όλους τους κόμβους του δικτύου. Στην περίπτωση, δηλαδή, μιας επίθεσης τύπου παρεμπόδισης της λειτουργίας (denial-of-service attack) , η κατάληψη πολλών κόμβων του δικτύου θα σήμαινε την αλλαγή της κατάστασης του σε LOCKED κάτι το οποίο θα μπορούσε να είναι καταστροφικό για την λειτουργία ολόκληρου του δικτύου. Αντίθετα στην άμεση μετάβαση των κόμβων στην κατάσταση LOCKED, χρησιμοποιείται η προσωρινή κατάσταση COUNTERMEASURES. Σε αυτή την κατάσταση οι καταληφθέντες κόμβοι προσπαθούν να αναγνωρίσουν το είδος της επίθεσης που δέχονται μέσω ειδικών μηχανισμών. Μετά την ολοκλήρωση των ειδικών αυτών μηχανισμών, όλοι οι καταληφθέντες κόμβοι περνάνε στην κατάσταση LOCKED. Την ίδια στιγμή οι ακέραιοι κόμβοι του δικτύου λαμβάνουν ειδικό μήνυμα/ειδοποίηση αγνόησης των καταληφθέντων κόμβων από το IVS. Το διάγραμμα μεταβάσεων των τεσσάρων καταστάσεων φαίνεται στην παρακάτω εικόνα.



Εικόνα 28: Το διάγραμμα μεταβάσεων των τεσσάρων καταστάσεων του κόμβου.

5.4 Πρωτόκολλο αυθεντικοποίησης

Το πρωτόκολλο αυθεντικοποίησης αποτελείται από τρείς φάσεις. Αυτές οι φάσεις αποτελούν ενέργειες που γίνονται πριν την τοποθέτηση των κόμβων στον χώρο επίβλεψης, κατά την διάρκεια αρχικοποίησης/εκκίνησης των κόμβων και κατά την διάρκεια κανονικής λειτουργίας τους. Πρέπει να σημειωθεί ότι όλα τα μηνύματα που ανταλλάσσονται ανάμεσα στους κόμβους του δικτύου κατά την διάρκεια των φάσεων του πρωτοκόλλου είναι κρυπτογραφημένα με τον αλγόριθμό XTEA. Για την κρυπτογράφηση τω μηνυμάτων χρησιμοποιείται το σύνολο των κλειδιών που δημιουργείται και αποθηκεύεται στους κόμβους κατά την διάρκεια της $1^{ης}$ φάσης του πρωτοκόλλου.

5.4.1 Φάση πριν την τοποθέτηση των κόμβων

Κατά την διάρκεια αυτής της φάσης ο σταθμός βάσης του δικτύου δημιουργεί ένα σύνολο τυχαίων αριθμών/κλειδιών. Το σύνολο αυτό είναι κοινό για όλους τους κόμβους του δικτύου, μεταφέρεται σε αυτούς και αποθηκεύεται σε μια ασφαλή περιοχή της μνήμης τους. Το σύνολο αυτών των αριθμών/κλειδιών θα λειτουργεί σαν αποθήκη κλειδιών από όπου οι κόμβοι και ο σταθμός βάσης του δικτύου θα επιλέγουν κάθε φορά διαφορετικό κλειδί για την κρυπτογράφηση της επικοινωνίας τους.

Η δημιουργία του συνόλου των κλειδιών σε αυτή την φάση έχει σαν αποτέλεσμα την εξοικονόμηση μεγάλων ποσοτήτων ενέργειας από τους κόμβους. Αυτό οφείλεται στο γεγονός ότι το σύνολο των κλειδιών δημιουργείται από τον σταθμό βάσης, ο οποίος συνήθως διαθέτει μόνιμη παροχή ρεύματος και αυξημένη επεξεργαστική ισχύ. Με αυτόν τον τρόπο αποφεύγεται η εκτέλεση των απαιτούμενων πολύπλοκων μαθηματικών υπολογισμών για την δημιουργία ενός συνόλου ισχυρών πραγματικά τυχαίων κλειδιών από τους κόμβους. Τέλος σε αυτή την φάση, οι κόμβοι δεν έχουν τοποθετηθεί ακόμα στον χώρο, οπότε είναι εύκολη και ενεργειακά αποδοτική η άμεση μεταφορά του συνόλου των κλειδιών στους κόμβους.

5.4.2 Φάση αρχικοποίησης

Οι κόμβοι του δικτύου τοποθετούνται στον χώρο επίβλεψης και μπαίνουν σε λειτουργία. Σε αυτή την φάση θα πρέπει να εκτελεστούν τα παρακάτω βήματα:

1. Αρχικοποίηση: Αυτό το βήμα ξεκινά το πρωτόκολλο αυθεντικοποίησης ανάμεσα στο SDI εκτελέσιμο ενός κόμβου του δικτύου και στο σταθμό βάσης/IVS. Οι δύο συμμετέχοντες στην διαδικασία ανταλλάσουν τα αντίστοιχα αναγνωριστικά τους, το SDI_ID και το IVS_ID. Ο IVS συγκρίνει το αναγνωριστικό του κόμβου που έλαβε με αυτό που έχει αποθηκευμένο στην IVDB βάση του. Αν ο έλεγχος αποτύχει, το πρωτόκολλο τερματίζεται.

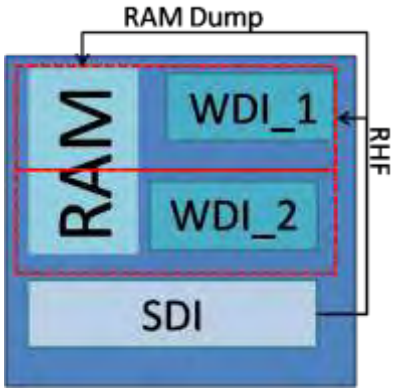
2. Στην περίπτωση όπου ο έλεγχος είναι επιτυχής, το SDI του κόμβου ξεκινάει τις διαδικασίες υπολογισμού των δεδομένων που είναι απαραίτητα για την επιβεβαίωση της ακεραιότητάς του.
3. Τα δεδομένα αυτά αποστέλλονται στον IVS. Ο IVS λαμβάνει τα στοιχεία, τα συγκρίνει με τα σωστά δεδομένα που έχει αποθηκευμένα στην IVDB βάση του. Το αποτέλεσμα του ελέγχου αποθηκεύεται στην βάση και παράλληλα αποστέλλεται στον κόμβο.
4. Ο κόμβος ανάλογα με το αποτέλεσμα του ελέγχου είτε μεταβαίνει στην κατάσταση ACTIVATED όπου και εκτελεί κανονικά τις λειτουργίες του, είτε παραμένει στην κατάσταση LOCKED και αγνοείται από το υπόλοιπο δίκτυο.

5.4.3 Φάση εκτέλεσης λειτουργιών

Αφού ολοκληρωθεί η φάση της αρχικοποίησης και έχουν ολοκληρωθεί με επιτυχία όλοι οι έλεγχοι, ο κόμβος μπορεί να εκτελέσει με ασφάλεια τις λειτουργίες του όπως είναι η συλλογή των δεδομένων, η κρυπτογράφησή τους και η αποστολή τους στον σταθμό βάσης.

5.5 Τεχνικές επιβεβαίωσης της ακεραιότητας

Ο έλεγχος της ακεραιότητας των κόμβων επιτυγχάνεται με την χρήση δύο τεχνικών: 1) του υπολογισμού ενός hash αριθμού (RHF) και 2) την δημιουργία στιγμιότυπου της μνήμης RAM για κάθε WDI ενός κόμβου.



Εικόνα 29: Το αποτύπωμα ενός WDI εκτελέσιμου.

5.5.1 Δημιουργία αριθμού Hash

Κάθε WDI εκτελέσιμο έχει ένα μοναδικό hash αριθμό, ο οποίος μπορεί να υπολογισθεί εύκολα μέσω μιας ειδικής συνάρτησης (Randomized Hashing Function - RHF) [89]. Αφού ολοκληρωθεί ο υπολογισμός του, ο αριθμός αυτός συνδυάζεται με το

αντίστοιχο SDI_ID αναγνωριστικό του κόμβου και το αποτέλεσμα αποθηκεύεται στην IVDB βάση του IVS, δημιουργώντας έτσι ένα μοναδικό "αποτύπωμα" του κόμβου.

5.5.2 Λήψη στιγμιότυπου τη μνήμης RAM

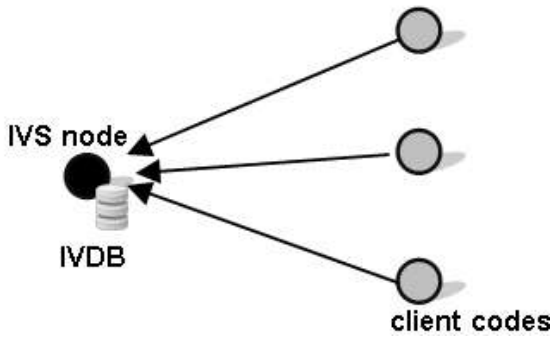
Κάθε διεργασία που εκτελείται σε ένα σύστημα αφήνει ένα χαρακτηριστικό αποτύπωμα στην μνήμη RAM του. Στην περίπτωση των κόμβων αισθητήρων που χρησιμοποιούν το πλαίσιο ασφαλείας, κάθε WDI εκτελέσιμο που λειτουργεί στον κόμβο αφήνει και το αντίστοιχο χαρακτηριστικό αποτύπωμα στην μνήμη RAM του. Πιο αναλυτικά, το πλαίσιο λειτουργιών ασφαλείας χρησιμοποιεί το χαρακτηριστικό αποτύπωμα των WDI με τον παρακάτω τρόπο. Το εκτελέσιμο SDI διαβάζει τα περιεχόμενα της μνήμης RAM των εκτελέσιμων WDI που λειτουργούν σε έναν κόμβο. Τα περιεχόμενα αυτά της μνήμης παίρνανε από μια hash συνάρτηση, ώστε να μετατραπούν σε συγκεκριμένο, χαρακτηριστικό για το κάθε WDI, αριθμό.

Αρχικά, πριν οι κόμβοι τοποθετηθούν στον επιβλέποντα χώρο, γίνεται υπολογισμός των χαρακτηριστικών hash αριθμών που αντιστοιχούν στα αποτυπώματα των WDI εκτελέσιμων του κάθε κόμβου. Αυτοί οι αριθμοί μαζί με τα SDI_ID αναγνωριστικά των κόμβων αποθηκεύονται στην βάση IVDB του σταθμού βάσης του δικτύου. Έτσι στην επόμενη φάση, είναι δυνατή η χρήση αυτών των τιμών για τον έλεγχο της ακεραιότητας των κόμβων.

5.6 Αρχιτεκτονική του Πλαισίου Ασφαλείας

5.6.1 Κεντρικοποιημένο σύστημα

Ένα τυπικό δίκτυο αισθητήρων αποτελείται από έναν IVS, μία IVDB και πλήθος κόμβων αισθητήρων οι οποίοι περιέχουν ένα SDI και ένα ή περισσότερα WDI (Εικόνα 25). Το SDI αποτελεί το πρόγραμμα που εκτελείται κατά τη εκκίνηση του κόμβου και αναλαμβάνει τον έλεγχο εγκυρότητα των υπόλοιπων εκτελέσιμων του κόμβου. Είναι υπεύθυνος για την επικοινωνία με τον IVS.



Εικόνα 30: Το κεντρικοποιημένο σχήμα όπου μετέχουν ένας IVS και πολλαπλοί κόμβοι αισθητήρων

Ο ρόλος του IVS είναι:

1. Να επικοινωνεί με το SDI εκτελέσιμο του κάθε κόμβου.
2. Να ανανεώνει και να διαχειρίζεται την τοπική IVDB βάση.
3. Να λειτουργεί σαν κάποια τρίτη αξιόπιστη πηγή.

Το κεντρικοποιημένο σχήμα διακρίνεται για την απλότητα του και ενδείκνυται κυρίως για χρήση σε μη-κρίσιμες εφαρμογές και σε εφαρμογές με μικρό αριθμό κόμβων αισθητήρων. Από την άλλη, η χρήση ενός μόνο IVS στο δίκτυο αποτελεί μοναδικό σημείο αστοχίας (single point of failure) και μοναδικό σημείο συσσώρευσης όλης την "κίνησης" του δικτύου (performance bottleneck). Επιπλέον, στην περίπτωση όπου κάποιος κακόβουλος χρήστης καταφέρει να αποκτήσει πρόσβαση στον μοναδικό IVS του συστήματος, όλες οι πληροφορίες που αφορούν την κρυπτογραφημένη επικοινωνίας και την αυθεντικοποιήση των κόμβων θα είναι διαθέσιμες σε αυτόν.

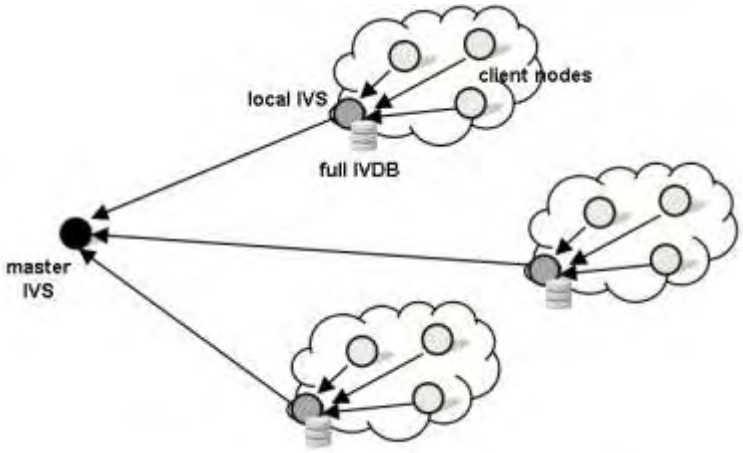
5.6.2 Μη-κεντρικοποιημένο σχήμα – Χρήσης συστάδων (Clustering)

Τα ιεραρχικά σχήματα αποτελούν αποδοτικό, εύκολα επεκτάσιμο και ενεργειακά βέλτιστο τρόπο διαδικτυακής διαχείρισης των ασύρματων δικτύων αισθητήρων. Στις ιεραρχικές αρχιτεκτονικές, οι κόμβοι έχουν διαφορετικούς ρόλους μέσα στο ίδιο δίκτυο και τυπικά είναι οργανωμένοι σε συστάδες (clusters). Η συγκρότηση σε συστάδες είναι μια μέθοδος όπου οι κόμβοι του δικτύου οργανώνονται σε ομάδες σύμφωνα με κάποια συγκεκριμένη ιδιότητα. Ένας κόμβος σε κάθε συστάδα αναλαμβάνει τον ρόλο του επικεφαλή της συστάδα, γνωστός ως cluster-head [111].

Στο προτεινόμενο πλαίσιο λειτουργιών ασφαλείας, κάθε επικεφαλής συστάδας εκτελεί και τις λειτουργίες ενός IVS. Έτσι κάθε επικεφαλής διαθέτει και ένα τοπικό αντίγραφο της βάσης IVDB, ώστε να διαχειρίζεται μόνο τους υπόλοιπους κόμβους της συστάδας. Με αυτόν τον τρόπο δημιουργείται ένα αποκεντρικοποιημένο μοντέλο προστασίας των κόμβων.

5.6.2.1 Δομή συστάδων – Πλήρες αντίγραφο της βάσης IVDB

Η δομή του σχήματος περιγράφεται στην Εικόνα 26. Πρόκειται για μια δομή συστάδων όπου κάθε κόμβος επικεφαλής/IVS έχει ένα πλήρες αντίγραφο της βάσης IVDB. Ο ρόλος του κάθε κόμβου επικεφαλή/IVS είναι να ελέγχει τους κόμβους που ανήκουν στην συστάδα του. Έτσι, στην περίπτωση όπου κάποιος κόμβος αντιμετωπίσει πρόβλημα με την διαδικασία εγκυροποίησης του, ο τοπικός επικεφαλής/IVS αναλαμβάνει να ενημερώσει όλους του επικεφαλής/IVS των υπόλοιπων συστάδων του δικτύου σχετικά με την ύπαρξη του πιθανού "εχθρικού" κόμβου.



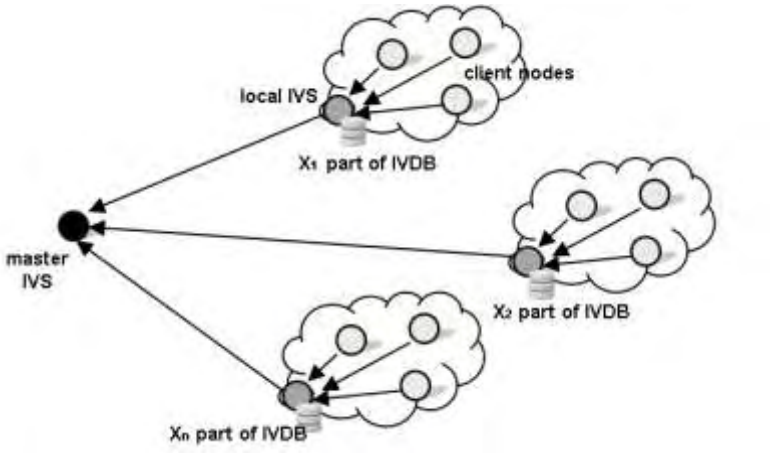
Εικόνα 31: Η δομή συστάδων όπου κάθε επικεφαλής κόμβος λειτουργεί και σαν τοπικός IVS. Κάθε τοπικός IVS έχει από ένα πλήρες αντίγραφο της IVDB βάσης

Το πρωτόκολλο αυθεντικοποίησης απαιτεί την μεταφορά δεδομένων κυρίως ανάμεσα στους κόμβους της ίδιας συστάδας (επικοινωνία ανάμεσα στον επικεφαλή/IVS και σε κάθε κόμβο της συστάδας). Η μόνη περίπτωση όπου απαιτείται επικοινωνία ανάμεσα στους επικεφαλής διαφορετικών συστάδων είναι όταν ανιχνευτεί κάποιος πιθανός εχθρικός κόμβος. Η συγκεκριμένη δομή αυξάνει την ικανότητα επεκτασιμότητας και τον χρόνο ζωής του δικτύου καθώς εξαλείφει το πρόβλημα της συσσωρευμένης κίνησης σε ένα μόνο σημείο του (performance bottleneck). Ακόμα μειώνει τον αριθμό των δεδομένων που μεταφέρονται στο δίκτυο, βελτιώνοντας έτσι την διαχείριση ενέργειας των κόμβων.

Από την άλλη, κάθε τοπικός επικεφαλής/IVS θα πρέπει να διαθέτει έναν ισχυρό μικρο-ελεγκτή και αρκετή μνήμη ώστε να διαχειρίζεται αποδοτικά το τοπικό πλήρες αντίγραφο της βάσης IVDB που διαθέτει. Επίσης, στην περίπτωση όπου κάποιος εισβολέας αποκτήσει πρόσβαση σε κάποιο κόμβο επικεφαλή/IVS του δικτύου, όλες οι κρίσιμες πληροφορίες που αφορούν την αυθεντικοποίηση όλων των κόμβων του δικτύου θα είναι διαθέσιμες σε μη εξουσιοδοτημένους χρήστες.

5.6.2.2 Δομή Συστάδων – Κατανεμημένη έκδοση της βάσης IVDB

Η δομή του σχήματος περιγράφεται στην Εικόνα 27. Κάθε τοπικός επικεφαλής/IVS διαθέτει μόνο ένα κομμάτι της βάσης IVDB. Κατά την διάρκεια της αρχικοποίησης του δικτύου, η βάση IVDB διαιρείται σε N κομμάτια, όπου N είναι το πλήθος των συστάδων του δικτύου. Κάθε ένα από τα N κομμάτια μεταφέρεται σε έναν από τους N επικεφαλής/IVS κόμβους.



Εικόνα 32: Η δομή συστάδων όπου κάθε επικεφαλής κόμβος λειτουργεί και σαν τοπικός IVS. Κάθε τοπικός IVS έχει από μόνο ένα μέρος της IVDB βάσης.
Στην εικόνα, όπου 1, 2, …, n είναι το id της συστάδας και
X1, X2, …, Xn είναι το μέρος της IVDB βάσης του κάθε τοπικού IVS.

Ο ρόλος του κάθε επικεφαλή/IVS κόμβου είναι να ελέγχει την εγκυρότητα των κόμβων που βρίσκονται, κάθε στιγμή, στην συστάδα του. Η διαδικασία αυθεντικοποίησης κάποιου κόμβου από τον επικεφαλή/IVS μιας συστάδας είναι:

1. Ο κόμβος στέλνει στον επικεφαλή/IVS μια αίτηση αυθεντικοποίησής του.
2. Ο επικεφαλής/IVS ελέγχει το τοπικό κομμάτι της βάσης IVDB που έχει, ώστε να βρει τις απαιτούμενες πληροφορίες.
3. Στην περίπτωση όπου οι πληροφορίες βρίσκονται στο τοπικό κομμάτι της βάσης IVDB, η διαδικασία αυθεντικοποίησης συνεχίζεται κανονικά.
4. Στην περίπτωση όπου οι πληροφορίες δεν βρίσκονται στο τοπικό κομμάτι της IVDB, ο επικεφαλής/IVS στέλνει μια αίτηση αναζήτησης των πληροφοριών στους επικεφαλής/IVS των υπόλοιπων συστάδων.
5. Όταν κάποιος από τους υπόλοιπους επικεφαλής/IVS λάβει την αίτηση αναζήτησης των πληροφοριών, ψάχνει στο τοπικό κομμάτι της βάσης IVDB. Στην περίπτωση όπου εντοπίσει τις επιθυμητές πληροφορίες, τις διαγράφει από την τοπική του βάση και τις στέλνει στον επικεφαλή/IVS που τις ζήτησε.
6. Στην συνέχεια, η διαδικασία αυθεντικοποιήσης συνεχίζεται από τον επικεφαλή/IVS που είχε αρχίσει την διαδικασία. Στην περίπτωση όπου ο ελεγχόμενος κόμβος χαρακτηριστεί ως πιθανός εχθρός, τα αναγνωριστικά του αποθηκεύονται στο τοπικό κομμάτι της IVDB βάσης του επικεφαλή/IVS κόμβου, ενώ καμία επιπλέον ενέργεια δε εκτελείται ανάμεσα σε αυτόν και στους υπόλοιπους επικεφαλής/IVS κόμβους του δικτύου.

Κατά την αρχικοποίηση του δικτύου, η βάση IVDB διαιρείται τυχαία και μοιράζεται σε όλους τους επικεφαλής/IVS κόμβους του δικτύου. Με την πάροδο του χρόνου και την αυθεντικοποίηση ολοένα και περισσότερων κόμβων του δικτύου, οι πληροφορίες αυτές αναδιανέμονται σταδιακά ανάμεσα στου επικεφαλής/IVS κόμβους σύμφωνα με την διάταξη των ίδιων των κόμβων στις συστάδες τους. Η χειρότερη περίπτωση σε αυτή την διαδικασία ανακατανομής των πληροφοριών είναι όταν ένας κόμβος μετακινείται συνεχώς ανάμεσα σε διαφορετικές συστάδες. Σε αυτή την περίπτωση, οι αντίστοιχες

πληροφορίες θα πρέπει να μεταφέρονται συνεχώς ανάμεσα στους αντίστοιχους επικεφαλής/IVS κόμβους.

Η χρήση της συγκεκριμένης δομής αυξάνει την ικανότητα επεκτασιμότητας του δικτύου και εξαλείφει το πρόβλημα του συσσωρευμένου φόρτου σε συγκεκριμένα σημεία του δικτύου. Επιπλέον στην περίπτωση όπου κάποιος εισβολέας αποκτήσει πρόσβαση σε έναν επικεφαλή/IVS κόμβο του δικτύου, θα αποκτήσει πρόσβαση μόνο σε ένα μικρό μέρος των πληροφοριών αυθεντικοποίησης των κόμβων του δικτύου.

Από την άλλη, η χρήση της συγκεκριμένης δομής επιφέρει την αύξηση της επικοινωνίας ανάμεσα στους επικεφαλής/IVS κόμβους του δικτύου, ειδικά κατά τους πρώτους γύρους αυθεντικοποίησης των κόμβων. Τα μηνύματα που ανταλλάσσονται ανάμεσα στους επικεφαλής/IVS κόμβους περιέχουν κρίσιμες πληροφορίες για την αυθεντικοποίηση των κόμβων. Αυτός είναι και ο λόγος που η προφύλαξή τους με μια μέθοδο κρυπτογράφησης, όπως είναι ο XTEA αλγόριθμός, κρίνεται αναγκαία.

5.7 Υλοποίηση του Πλαισίου

Η υλοποίηση του πλαισίου λειτουργιών ασφάλειας έγινε για τους κόμβους Mica2 και για το λειτουργικό σύστημα Tinyos 2. Ακόμα, η υλοποίηση του πλαισίου που περιγράφεται παρακάτω, βασίζεται στην κεντρικοποιημένη αρχιτεκτονική όπως περιγράφεται στην παράγραφο 5.6.1.

Το πλαίσιο έχει υλοποιηθεί σε δύο μέρη: το πρώτο περιλαμβάνει την λειτουργικότητα του IVS και το δεύτερο την λειτουργικότητα του κόμβου. (Εικόνα 28)

IVS Code

```
on receive UserHashMsg:
        receive( idAddr , UserHashMsg );
        decrypt(UserHashMsg);
        if( check (UserHashMsg) == valid() ){
                VerifyMsg = Valid;
                encrypt(VerifyMsg);
                send( idAddr , VerifyMsg );
        }
        else{
                VerifyMsg = Invalid;
                encrypt(VerifyMsg);
                send( idAddr , VerifyMsg );
        }

on receive HashMsg:
        receive( idAddr , HashMsg );
        decrypt(HashMsg);
        if( IVDBcheck (HashMsg) == valid() ){
                VerifyMsg = Valid;
                encrypt(VerifyMsg);
                send( idAddr , VerifyMsg );
        }
        else{
                VerifyMsg = Invalid;
                encrypt(VerifyMsg);
                send( idAddr , VerifyMsg );
        }
```

Sensor Code

on boot:

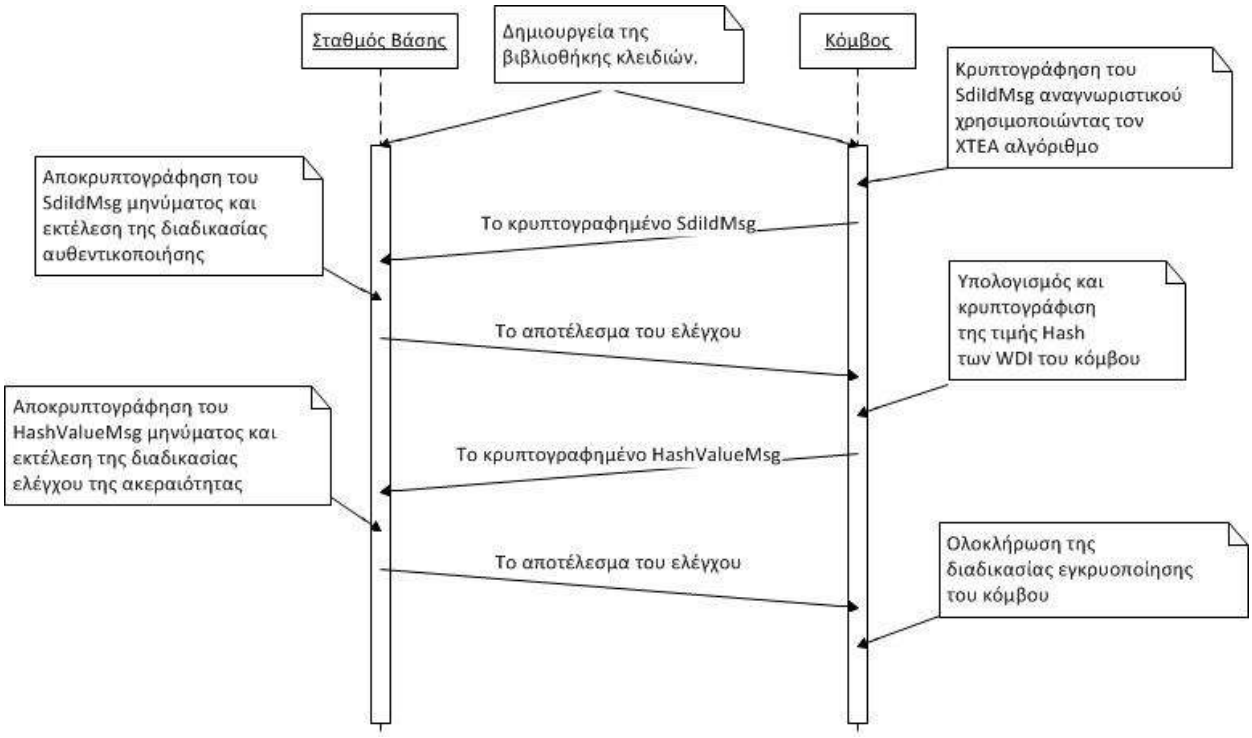
```
state = LOCKED;
encrypt(UserHashMsg);
send( broadcastAddr , UserHashMsg );
```

on receive VerifyMsg:

```
receive( idAddr , VerifyMsg );
decrypt(VerifyMsg);
if( VerifyMsg==Valid  && state==LOCKED){
        state = VERYFING;
        HashMsg = computeHashValue();
        encrypt(HashMsg);
        send( broadcastAddr , HashMsg  );
}
else if( VerifyMsg==Valid  && state==VERYFING){
        state = ACTIVATED;
        start  data  process();
}
else{
        state = LOCKED;
}
```

Εικόνα 33: Η υλοποίηση του πλαισίου.

Στην παρακάτω εικόνα φαίνεται το διάγραμμα ακολουθίας των μηνυμάτων του πλαισίου.



Εικόνα 34: Το διάγραμμα ακολουθίας των μηνυμάτων του πλαισίου.

1. Κατά την διάρκεια της 1^{ης} φάσης του πλαισίου κάθε κόμβος εφοδιάζεται με ένα σύνολο ασφαλών κλειδιών πλήθους 120 κλειδιών.

2. Ο κόμβος κρυπτογραφεί το SDI_ID αναγνωριστικό του χρησιμοποιώντας τον αλγόριθμο XTEA.
3. Ο κόμβος στέλνει το κρυπτογραφημένο μήνυμα, μεγέθους 80 bit, στον IVS.
4. Ο IVS αποκρυπτογραφεί το μήνυμα και ελέγχει το SDI_ID αναγνωριστικό.
5. Ο IVS στέλνει στον κόμβο το αποτέλεσμα του ελέγχου.
6. Ο κόμβος λαμβάνει το αποτέλεσμα. Στην περίπτωση όπου ο έλεγχος είναι επιτυχής, ο κόμβος αλλάζει κατάσταση από την LOCKED στην VERIFYING και ξεκινάει την εκτέλεση των διαδικασιών που απαιτούνται για την λήψη του αποτυπώματος την μνήμης και υπολογισμού του αριθμού hash. Ο αλγόριθμος που χρησιμοποιήθηκε για τον υπολογισμό του αριθμού hash είναι ο SHA-1, ο οποίος απαιτεί χρόνο ~13 ms για κάθε υπολογισμό hash [97]. Για την υλοποίηση του πλαισίου, χρησιμοποιείται ένα αποτύπωμα μεγέθους 512 bytes της μνήμης από τον οποίο υπολογίζεται ο αριθμός hash μεγέθους 160 bits.
7. Ο κόμβος κρυπτογραφεί την 160 bit hash τιμή και την στέλνει στον IVS. Το τελικό κρυπτογραφημένο μήνυμα έχει μέγεθος 208 bits.
8. Ο IVS αποκρυπτογραφεί το μήνυμα και ελέγχει την εγκυρότητα του αριθμού hash.
9. Ο IVS στέλνει το αποτέλεσμα του ελέγχου στον κόμβο.
10. Ο κόμβος, ανάλογα με τα αποτέλεσμα που έλαβε, αλλάζει την κατάσταση του σε ACTIVATED ή LOCKED και ενεργεί ανάλογα.

5.8 Ανάλυση Κατανάλωσης Ενέργειας του Πλαισίου

Στην επόμενη παράγραφο γίνεται μια ανάλυση της κατανάλωσης ενέργειας του πλαισίου. Για την προσομοίωση του πλαισίου και την μέτρηση της κατανάλωσης ενέργειας που απαιτεί, χρησιμοποιήθηκε ο προσομοιωτής AVRORA [95]. Πρόκειται για ένα σύνολο εργαλείων προσομοίωσης και ανάλυσης προγραμμάτων που έχουν υλοποιηθεί για εκτέλεση στους μικρο-ελεγκτές τύπου AVR. Οι συγκεκριμένοι μικρο-ελεγκτές κατασκευάζονται από την εταιρεία Atmel και χρησιμοποιούνται στους κόμβους Mica2. Ένα από τα εργαλεία ανάλυσης και προσομοίωσης που υπάρχουν στο AVRORA είναι το AOEN (Accurate Prediction of Power Consumption)[94]. Πρόκειται για ένα μοντέλο κατανάλωσης ενέργειας το οποίο χρησιμοποιεί επιμέρους εμπειρικές μετρήσεις (του υλικού του κόμβου, όπως είναι ο πομποδέκτης, ο μικρο-ελεγκτής, τα αισθητήρια όργανα) ώστε να υπολογίσει την συνολική κατανάλωση ενέργειας του κόμβου. Βασίζεται στην εκτέλεση του λειτουργικού συστήματος και του κώδικα του κόμβου, ώστε να υπολογίζει με όσο το δυνατόν μεγαλύτερη ακρίβεια την πραγματική κατανάλωση ενέργειάς του.

5.8.1 Κατανάλωση ενέργειας των λειτουργιών κρυπτογράφησης

Ο παρακάτω πίνακας συγκρίνει την ενέργεια που απαιτείται για την εκτέλεση των διάφορων αλγορίθμων κρυπτογράφησης της οικογενείας αλγορίθμων TEA. Πιο συγκεκριμένα, οι τιμές που παρουσιάζονται στον πίνακα αφορούν την ενέργεια που καταναλώνεται στον κόμβο για την εκτέλεση των λειτουργιών:

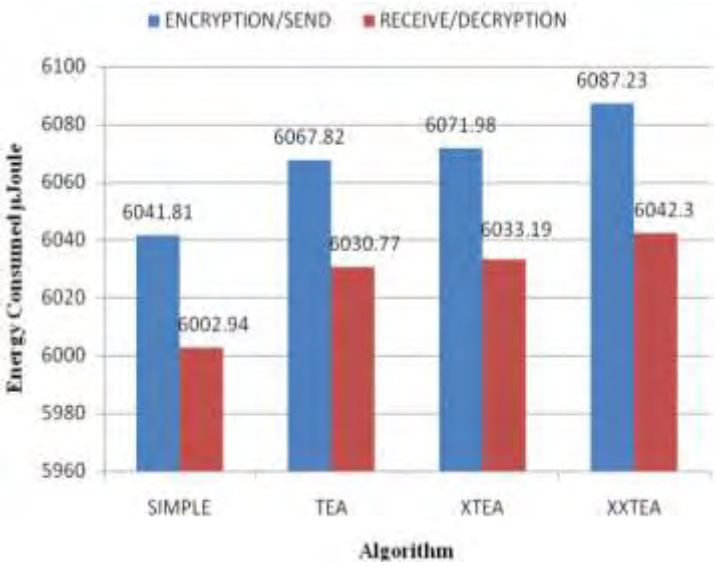
1. Κρυπτογράφηση και αποστολή ενός μηνύματος μεγέθους 64 bits
2. Λήψη και αποκρυπτογράφηση ενός μηνύματος μεγέθους 64 bits

Πίνακας 11: Ενεργειακό κόστος της χρήσης αλγορίθμων κρυπτογράφησης τύπου TEA. Οι τιμές είναι εκφρασμένες σε μJoule.

Αλγόριθμος	Ενεργειακό Κόστος	
	Κρυπτογράφηση - Αποστολή	Λήψη - Αποκρυπτογράφηση
ΑΠΛΟ	6041.81μJoule	6002.94 μJoule
TEA	6067.82 μJoule	6030.77 μJoule
XTEA	6071.98 μJoule	6033.19 μJoule
XXTEA	6087.23 μJoule	6042.30 μJoule

Στον παραπάνω πίνακα υπάρχει μια πλειάδα μετρήσεων για τον αλγόριθμο ΑΠΛΟ. Πρόκειται για την ενέργεια που απαιτείται από τον κόμβο μόνο για την αποστολή και την λήψη ενός πακέτου μεγέθους 64 bits. (χωρίς δηλαδή την εκτέλεση οποιαδήποτε κρυπτογραφικής λειτουργίας σε αυτό)

Δεν παρουσιάζεται το κόστος δημιουργίας των κλειδιών της κρυπτογράφησης. Γίνεται η θεώρηση ότι τα κλειδιά δημιουργήθηκαν κατά το 1^{ο} στάδιο εκτέλεσης του πλαισίου, όπως περιγράφεται στο κεφάλαιο 5.4.1 . Όπως φαίνεται και στην Εικόνα 30, το ενεργειακό κόστος της χρήσης των αλγορίθμων κρυπτογράφησης TEA είναι σχετικά χαμηλό και συγκρίσιμο με την χρήση επικοινωνίας χωρίς καμία λειτουργία κρυπτογράφησης.



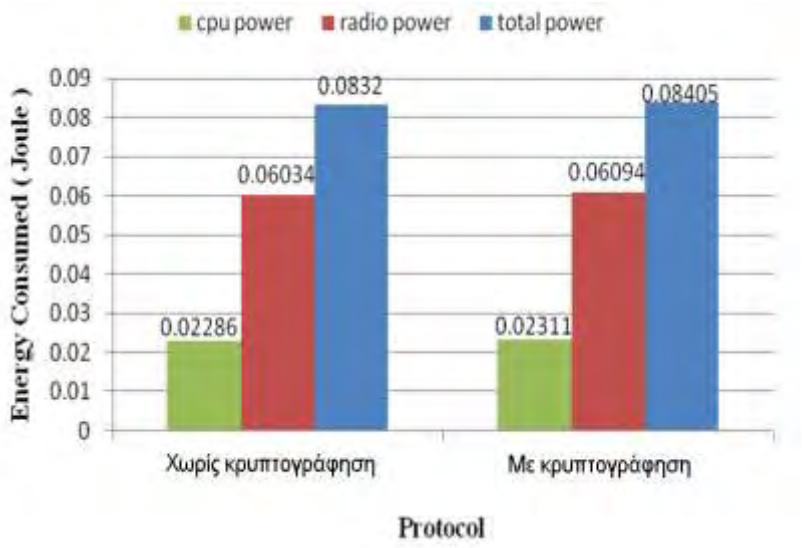
Εικόνα 35: Ενεργειακό κόστος της χρήσης αλγορίθμων κρυπτογράφησης τύπου TEA. Οι τιμές είναι εκφρασμένες σε μJoule.

5.8.2 Ενεργειακό κόστος του πλαισίου λειτουργιών ασφαλείας

Ο Πίνακας 9 συγκρίνει την κατανάλωσης ενέργειας δύο διαφορετικών εκδόσεων του πλαισίου. Οι μετρήσεις αφορούν τις ποσότητες ενέργειας που απαιτούνται για την ολοκλήρωση των λειτουργιών αυθεντικοποίησης και ελέγχου της ακεραιότητας ενός κόμβου. Η διαφορά ανάμεσα στις δύο εκδώσεις του πλαισίου έγκειται στην χρήση κρυπτογραφημένων ή όχι μηνυμάτων ανάμεσα στον κόμβο και στον IVS. Στην έκδοση του πρωτοκόλλου όπου γίνεται χρήση κρυπτογραφημένων μηνυμάτων χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης XTEA.

Πίνακας 12: Κατανάλωσης ενέργειας δύο διαφορετικών εκδόσεων του πλαισίου. Οι τιμές είναι εκφρασμένες σε Joule.

Έκδοση Πλαισίου	**Ενεργειακό Κόστος**		
	Ενέργεια μικρο-ελεγκτή	**Ενέργεια πομποδέκτη**	**Συνολική Ενέργεια**
Χωρίς χρήση κρυπτογραφίας	0.02286 Joule	0.06034 Joule	0.08321 Joule
Με χρήση κρυπτογραφίας	0.02311 Joule	0.06094 Joule	0.08406 Joule



Εικόνα 36: Κατανάλωσης ενέργειας δύο διαφορετικών εκδόσεων του πλαισίου. Οι τιμές είναι εκφρασμένες σε Joule.

5.9 Multihop πρωτόκολλο επικοινωνίας

Το κύριο πλήθος των εφαρμογών στον πραγματικό κόσμο που κάνουν χρήση των ασύρματων δικτύων αισθητήρων χρειάζονται επικοινωνία ανάμεσα στους κόμβους του δικτύου. Το εύρος της επικοινωνίας αυτής Ιανέ συνήθως παραπάνω από 1 hop, κάνοντας έτσι επιτακτική την χρήση multihop πρωτοκόλλων επικοινωνίας. Το πλαίσιο λειτουργιών ασφαλείας που περιγράφεται υποστηρίζει ασύρματη multihop επικοινωνία. Όπως έχει παρουσιαστεί παραπάνω στην Εικόνα 29, το πλαίσιο απαιτεί μια 2-μερή επικοινωνία. Η επικοινωνία η οποία έχει κατεύθυνση από τον σταθμό βάσης προς του κόμβους καλείται με τον όρο downlink. Αντίθετα η επικοινωνία με κατεύθυνση από του κόμβους του δικτύου προς τον σταθμό βάσης καλείται με τον όρο uplink. Κατά τη διάρκεια της φάσης αρχικοποίησης του πλαισίου, το uplink κανάλι επικοινωνίας μεταφέρει τα κρυπτογραφημένα SdiIdMsg και HashValueMsg πακέτα. Επιπλέον, κατά την φάση της κανονικής λειτουργίας του δικτύου, το uplink κανάλι επικοινωνίας μεταφέρει τα δεδομένα που έχον συλλέξει οι αισθητήρες σε κρυπτογραφημένη μορφή.

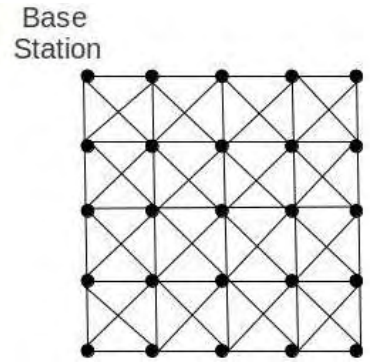
Για την υποστήριξη της multihop επικοινωνίας το πλαίσιο λειτουργιών ασφαλείας κάνει χρήση κάποιου multihop πρωτοκόλλου. Στα σενάρια εκτέλεσης που ακολουθούν χρησιμοποιείται ο αλγόριθμος πλημμύρας. Πρόκειται για την απλούστερη περίπτωση multihop πρωτοκόλλου, όπου ο κάθε κόμβος επανεκπέμπει τα πακέτα που δέχεται μέχρι αυτά να φτάσουν στον τελικό προορισμό τους. Για την αποφυγή ατέρμων κύκλων των πακέτων, κάθε κόμβος επανεκπέμπει το κάθε πακέτο μόνο την πρώτη φορά που το έλαβε. Είναι ένα πολύ απλό πρωτόκολλο το οποίο όμως έχει μειονεκτήματα, όπως είναι το πλήθος συγκρούσεων που προκαλεί στα πακέτα του δικτύου και το γεγονός ότι δεν λαμβάνεται καθόλου υπόψη η βέλτιστη διαχείριση και διαθεσιμότητα των πόρων των κόμβων. Για τα σενάρια που ακολουθούν επιλέχθηκε ο αλγόριθμος πλημύρας ως η πιο απλή αλλά και η χειρότερη, σε θέμα απόδοσης, λύση (worst case scenario).

5.9.1 Σενάρια εκτέλεσης

Η εκτέλεση των σεναρίων για την μέτρηση της αποδοτικότητας της multihop επικοινωνίας του πλαισίου χρησιμοποιήθηκε ο προσομοιωτής PowerTOSSIM. Πιο συγκεκριμένα το PowerTOSSIM είναι ένα περιβάλλον προσομοίωσης ασύρματων δικτύων αισθητήρων ειδικά σχεδιασμένο ώστε να παρέχει λεπτομερής πληροφορίες κατανάλωσης ενέργειας για κάθε κόμβο του δικτύου. Πρόκειται για μια επέκταση του εργαλείου προσομοίωσης TOSSIM, δηλαδή ενός προσομοιωτή ειδικά σχεδιασμένου να εκτελεί εφαρμογές που βασίζονται στο λειτουργικό TinyOS των ασύρματων δικτύων αισθητήρων. Το PowerTOSSIM χρησιμοποιεί λεπτομερή μοντέλα κατανάλωσης ενέργειας βασισμένα στο υλικό των κόμβων Mica2 [107].

5.9.1.1 Σενάριο 1

Το σενάριο περιλαμβάνει 25 κόμβους τύπου Mica2 οι οποίοι είναι τοποθετημένοι σε ένα πλέγμα μεγέθους 5x5. Η εμβέλεια ανάμεσα στους κόμβους είναι καθορισμένη, ώστε ο κάθε κόμβος να μπορεί να επικοινωνεί μόνο με τους άμεσους γείτονές του. Κάθε κόμβος έχει ένα μοναδικό αναγνωριστικό ID και επιπλέον ο κόμβος με το μικρότερο αναγνωριστικό (ID0) λειτουργεί σαν σταθμός βάσης του δικτύου και βρίσκεται στην πάνω αριστερή γωνία του πλέγματος (Εικόνα 32)



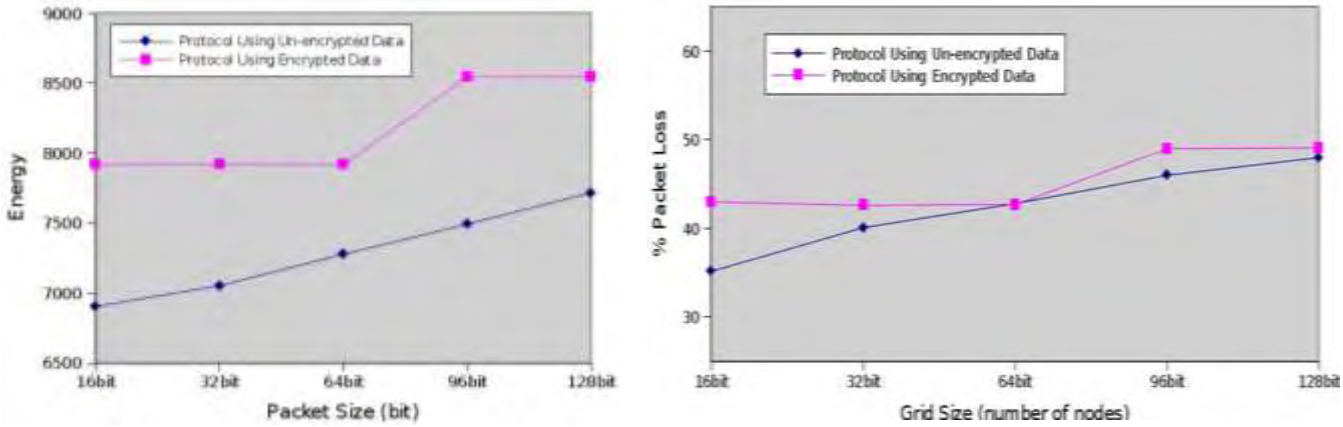
Εικόνα 37: Η τοποθέτηση των κόμβων του σεναρίου. Κάθε κόμβος μπορεί να επικοινωνεί μόνο με του άμεσους γείτονες του (το πολύ 8 κόμβους)

Κατά την διάρκεια εκτέλεσης του σεναρίου, οι κόμβοι, εκτός του σταθμού βάσης, βρίσκονται στην κατάσταση κανονικής λειτουργίας τους. Δηλαδή, περιοδικά δειγματοληπτούν και στέλνουν τα δεδομένα στον σταθμό βάσης. Για το σενάριο τις προσομοίωσης οι κόμβοι κάθε 5 δευτερόλεπτα στέλνουν ένα μήνυμα με τυχαία δεδομένα στον σταθμό βάσης.

Ο Πίνακας 10 συγκρίνει το ποσοστό χαμένων μηνυμάτων (% packet loss) και την συνολική ενέργεια που καταναλώθηκε από όλους τους κόμβους του δικτύου. Εκτελέστηκαν σενάρια προσομοίωσης με διακυμάνσεις στο μέγεθος των πακέτων που στέλνουν οι κόμβοι καθώς και στον τύπο τον πακέτων (κρυπτογραφημένα/μη-κρυπτογραφημένα).

Πίνακας 13: Κατανάλωση ενέργειας και ποσοστό χαμένων πακέτων κατά την multihop εκτέλεση του πλαισίου. Παρουσιάζονται τιμές για διαφορετικό μέγεθος και διαφορετικό τύπο πακέτων (κρυπτογραφημένα/μη-κρυπτογραφημένα)

Μέγεθος Πακέτου	**Ενεργειακό Κόστος**		**Ποσοστό Χαμένων Πακέτων**	
	Μη-κρυπτογραφημένα	**Κρυπτογραφημένα**	**Μη-κρυπτογραφημένα**	**Κρυπτογραφημένα**
16bit	6904 μJoule	7920 μJoule	35.15	43
32bit	7052 μJoule	7920 μJoule	40.09	42.6
64bit	7277 μJoule	7920 μJoule	42.8	42.7
96bit	7491 μJoule	8545 μJoule	46	49
128bit	7717 μJoule	8545 μJoule	48	49.1



Εικόνα 38: Κατανάλωση ενέργειας και ποσοστό χαμένων πακέτων κατά την multihop εκτέλεση του πλαισίου

Στις μετρήσεις δεν περιλαμβάνεται το κόστος δημιουργίας της αποθήκης κλειδιών που χρησιμοποιούνται στην κρυπτογράφηση των πακέτων, καθώς θεωρούμε ότι έχει δημιουργηθεί κατά την διάρκεια της 1ης φάσης του πλαισίου, όπως περιγράφεται στην ενότητα 5.4.1.

Στον Πίνακα 10 παρατηρούμε ότι στην περίπτωση χρήσης κρυπτογραφημένων πακέτων η κατανάλωση ενέργειας και τα ποσοστά χαμένων πακέτων παίρνουν παρόμοια τιμή για τα μεγέθη πακέτων 16, 32, και 64 bit και παρόμοια τιμή για τα μεγέθη πακέτων 96 και 128 bit. Αυτό οφείλεται στον γεγονός ότι ο αλγόριθμος κρυπτογράφησης XTEA χρησιμοποιεί/παράγει block μεγέθους 64 bits. Οπότε, ακόμα και στην περίπτωση όπου ο αλγόριθμος λάβει για κρυπτογράφηση ένα μήνυμα μεγέθους 16-βιτ, το κρυπτογραφημένο μήνυμα που θα παραχθεί θα έχει μέγεθος 64 bit.

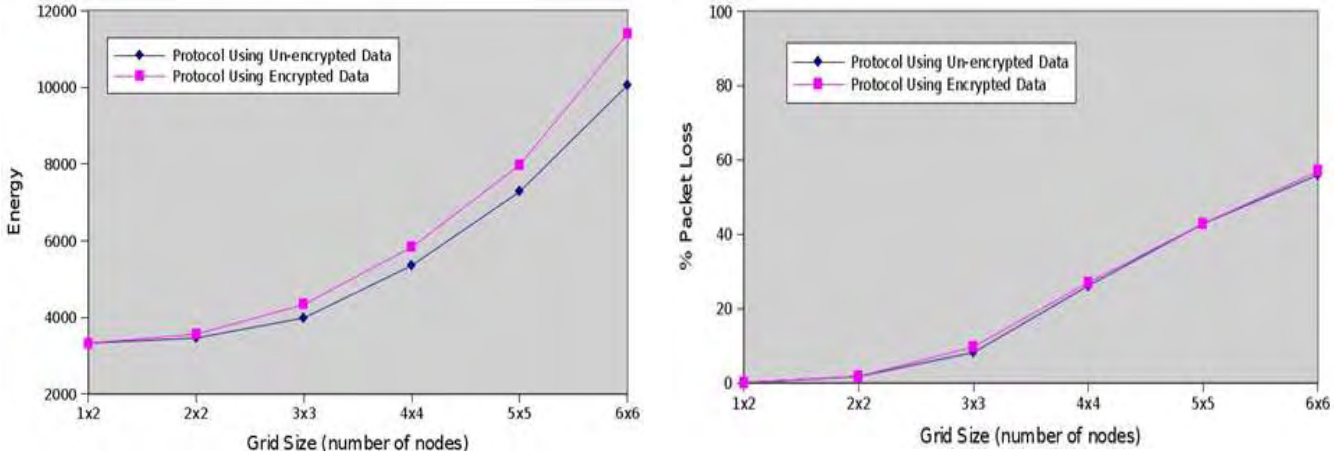
5.9.1.2 Σενάριο 2

Το σενάριο 2 περιλαμβάνει κόμβους Mica2 τοποθετημένους σε τοπολογία πλέγματος. Έγιναν διάφορες εκτελέσεις του σεναρίου 2, όπου η κάθε μια διαφέρει από τις υπόλοιπες ως προς το πλήθος των κόμβων άρα και το μέγεθος του πλέγματος που χρησιμοποιήθηκε. Οι τοπολογίες πλέγματος που χρησιμοποιήθηκαν είναι τετράγωνα μεγέθους από 1x2 έως 6x6. Ο κάθε κόμβος είχε το δικό του μοναδικό αναγνωριστικό ID και ο κόμβος με το μικρότερο αναγνωριστικό (ID0) βρίσκεται στην πάνω αριστερή γωνία του πλέγματος (Εικόνα 32) και λειτουργεί ως σταθμός βάσης. Κατά την διάρκεια εκτέλεσης των σεναρίων οι κόμβοι (εκτός του σταθμού βάσης) βρίσκονται σε κατάσταση κανονικής λειτουργίας και στέλνουν περιοδικά (κάθε 5 δευτερόλεπτα) πακέτα δεδομένων. Το μέγεθος των πακέτων αυτών είναι 64 bit.

Ο Πίνακας 11 συγκρίνει το ποσοστό χαμένων μηνυμάτων (% packet loss) και την συνολική ενέργεια που καταναλώθηκε από όλους τους κόμβους του δικτύου. Εκτελέστηκαν σενάρια προσομοίωσης με διακυμάνσεις στο πλήθος των κόμβων του δικτύου καθώς και στον τύπο τον πακέτων (κρυπτογραφημένα/μη-κρυπτογραφημένα).

Πίνακας 14 Κατανάλωση ενέργειας και ποσοστό χαμένων πακέτων κατά την multihop εκτέλεση του πλαισίου. Παρουσιάζονται τιμές για διαφορετικό πλήθος κόμβων και διαφορετικό τύπο πακέτων (κρυπτογραφημένα/μη-κρυπτογραφημένα)

Πλήθος Κόμβων	Ενεργειακό Κόστος		Ποσοστό Χαμένων Πακέτων	
	Μη-κρυπτογραφημένα	Κρυπτογραφημένα	Μη-κρυπτογραφημένα	Κρυπτογραφημένα
1x2	3330 μJoule	3330 μJoule	0	0
2x2	3464 μJoule	3561 μJoule	1.7	1.7
3x3	3988 μJoule	4338 μJoule	8.18	9.63
4x4	5354 μJoule	5833 μJoule	26.1	27
5x5	7277 μJoule	7922 μJoule	42.8	42.7



Εικόνα 39: Κατανάλωση ενέργειας και ποσοστό χαμένων πακέτων κατά την multihop εκτέλεση του πλαισίου για διαφορετικό πλήθος κόμβων.

5.9.2 Βελτίωση στο Multihop πρωτόκολλο

Μία επίθεση εμπόδισης της λειτουργικότητας (Denial-of-service attack – DoS attack) είναι μια προσπάθεια των επιτιθέμενων να εμποδίσουν την κανονική λειτουργία ενός συστήματος. Αν και τα μέσα, οι τρόποι, αλλά και οι στόχοι μια DoS επίθεσης ποικίλουν, πρόκειται για μία συντονισμένη προσπάθεια ενός ή και περισσοτέρων ατόμων να εμποδίσουν την κανονική λειτουργία συστήματος , ή κόμβου στην δική μας περίπτωση, προσωρινά ή και μόνιμα [107-108].

Πιο συγκεκριμένα μια συντονισμένη επίθεση πλημμύρας (DoS flooding attack) έχει στόχο να κατακλύσει τους περιορισμένους πόρους ενός κόμβου, όπως την μνήμη του, την επεξεργαστική ισχύ του μικρο-ελεγκτή του και το εύρος του πομποδέκτη του ώστε να εμποδίσει την κανονική λειτουργία του. Για παράδειγμα, στην περίπτωση όπου κάποιος επιτιθέμενος αποκτήσει πρόσβαση σε έναν κόμβο και τον προγραμματίσει έτσι ώστε να στέλνει συνεχώς πακέτα προς τους γείτονές του, θα καταφέρει να εξαντλήσει τα

αποθέματα ενέργειας του συγκεκριμένου κόμβου αλλά και των γειτονικών του κόμβων. Ακόμα, αν το δίκτυο λειτουργεί με κάποιο multihop πρωτόκολλο (όπως στην περίπτωση του πλαισίου που περιγράφουμε) τα συνεχή αυτά μηνύματα/σκουπίδια θα προωθούνται συνεχώς προς όλους τους κόμβους του δικτύου, εξαντλώντας σταδιακά τα αποθέματα ενέργειας όλων των κόμβων του δικτύου. Ένα multihop πρωτόκολλο το οποίο δεν θα προωθούσε όλα τα μηνύματα, αλλά θα περιόριζε την επανεκπομπή των κόμβων θα βελτίωνε σημαντικά τις επιπτώσεις της DoS επίθεσης στο σύνολο του δικτύου [109-110].

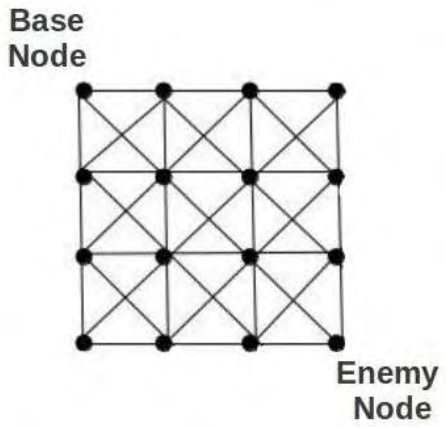
Στα πλαίσια του πλαισίου λειτουργιών ασφαλείας που περιγράφουμε, ο εντοπισμός και η μείωση των επιπτώσεων μιας DoS επίθεσης θα μπορούσε να γίνει με την εκτέλεση των παρακάτω λειτουργιών/βελτιώσεων.

1. Έτσι ότι κάποιος κόμβος αποτυγχάνει στην ολοκλήρωση των λειτουργιών αυθεντικοποίησης και ακεραιότητας, καθώς κάποιος κακόβουλος χρήστης έχει αποκτήσει πρόσβαση σε αυτόν.
2. Ο σταθμός βάσης αναλαμβάνει να ενημερώσει όλους του υπόλοιπους κόμβους του δικτύου για ύπαρξη πιθανής απειλής και τους στέλνει το αναγνωριστικό ID του κόμβου αυτού.
3. Οι κόμβοι που λειτουργούν κανονικά λαμβάνουν το αναγνωριστικό ID του εχθρικού κόμβου. Το αποθηκεύουν σε έναν πίνακα, ο οποίος λειτουργεί ως ένα είδος πίνακα μη-δρομολόγησης.
4. Πλέον όταν κάποιος από τους έγκυρους κόμβος λάβει μήνυμα από κόμβο. Ελέγχει το αναγνωριστικό του κόβου.
5. Αν το αναγνωριστικό υπάρχει μέσα στον πίνακα, το μήνυμα δεν προωθείται αλλά διαγράφεται. Αντίθετα, στην περίπτωση όπου το αναγνωριστικό δεν υπάρχει στον πίνακα, το αντίστοιχο μήνυμα προωθείται χωρίς κανένα πρόβλημα στους υπόλοιπους κόμβους του δικτύου.

Χρησιμοποιώντας τα παραπάνω βήματα/βελτιώσεις, τα μηνύματα που στέλνονται από τον εχθρικό κόμβο λαμβάνονται μόνο από τους γειτονικούς του κόμβου. Αυτό έχει σαν αποτέλεσμα, η συγκεκριμένη επίθεση να έχει επιπτώσεις μόνο στους γειτονικούς κόμβους και όχι σε όλο το σύνολο του δικτύου, βελτιώνοντας έτσι κατά πολύ την διάρκεια ζωής του.

5.9.2.1 Κατανάλωση ενέργειας της βελτιωμένης multihop επικοινωνίας

Το σενάριο περιλαμβάνει 16 κόμβους Mica2 τοποθετημένους σε τοπολογία πλέγματος μεγέθους 4x4. Η εμβέλεια ανάμεσα στους κόμβους είναι καθορισμένη, ώστε ο κάθε κόμβος να μπορεί να επικοινωνεί μόνο με τους άμεσους γείτονές του. Ο κάθε κόμβος είχε το δικό του μοναδικό αναγνωριστικό ID και ο κόμβος με το μικρότερο αναγνωριστικό (ID0) βρίσκεται στην πάνω αριστερή γωνία του πλέγματος και λειτουργεί ως σταθμός βάσης. Ο κόμβος με το μεγαλύτερο αναγνωριστικό ID βρίσκεται στο κάτω αριστερό μέρος του πλέγματος και λειτουργεί ο εχθρικός κόμβος. (Εικόνα 35)



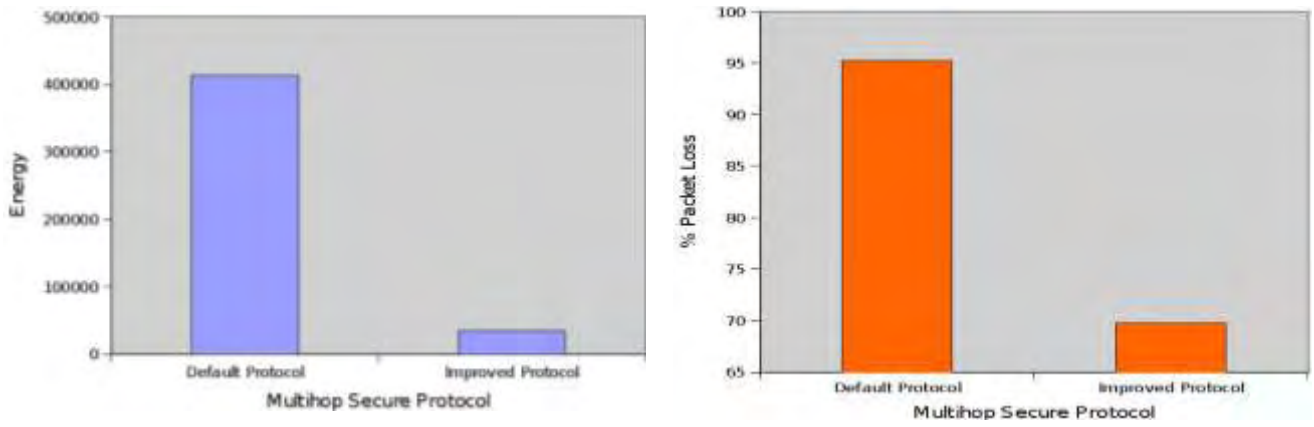
Εικόνα 40: Η τοποθέτηση των κόμβων του σεναρίου. Κάθε κόμβος μπορεί να επικοινωνεί μόνο με του άμεσους γείτονες του (το πολύ 8 κόμβους).

Κατά την διάρκεια εκτέλεσης του σεναρίου οι κόμβοι (εκτός του σταθμού βάσης) βρίσκονται σε κατάσταση κανονικής λειτουργίας και στέλνουν περιοδικά (κάθε 5 δευτερόλεπτα) πακέτα δεδομένων. Αντίθετα ο εχθρικός κόμβος στέλνει μήνυμα/σκουπίδι κάθε 0.5 δευτερόλεπτο. Το μέγεθος των πακέτων αυτών είναι 64 bit.

Ο Πίνακας 12 συγκρίνει το ποσοστό χαμένων μηνυμάτων (% packet loss) και την συνολική ενέργεια που καταναλώθηκε από όλους τους κόμβους του δικτύου. Εκτελέστηκαν σενάρια προσομοίωσης με και χωρίς την χρήση των βελτιώσεων επικοινωνίας που περιγράφηκαν παραπάνω.

Πίνακας 15 Κατανάλωση ενέργειας και ποσοστό χαμένων πακέτων κατά την multihop εκτέλεση του πλαισίου. Παρουσιάζονται τιμές για την χρήση και μη των διαφορετικό εκδόσεων του πρωτοκόλλου επικοινωνίας

Τύπος επικοινωνίας	Ενεργειακό Κόστος	Ποσοστό Χαμένων Πακέτων
Κανονικός	412908 μJoule	95.28
Βελτιωμένος	34348 μJoule	69.8



Εικόνα 41: Κατανάλωση ενέργειας και ποσοστό χαμένων πακέτων κατά την multihop εκτέλεση του πλαισίου για διαφορετικό τύπο επικοινωνίας.

6 *Μέθοδος Ανίχνευσης Απειλών*

Η ανίχνευση απειλών αποτελεί ένα από τα κύρια θέματα έρευνας για τις εφαρμογές των ασύρματων δικτύων αισθητήρων. Για την επιτυχή ανίχνευση μιας απειλής, ένα δίκτυο αισθητήρων καλείται να αναγνωρίσει το είδος και το σημείο που συνέβη κάποιο συγκεκριμένο γεγονός μέσα στην περιοχής κάλυψης και επίβλεψης του δικτύου. Αυτή η ανίχνευση και αναγνώριση του γεγονότος από το δίκτυο βασίζεται κυρίως σε ακατέργαστα δεδομένα που συλλέγονται από του κόμβους του. Το κύριο ζητούμενο είναι η αναγνώριση και η ανίχνευση του γεγονότος να γίνεται με μεγάλη ακρίβεια αλλά και με το ελάχιστο ενεργειακό κόστος για το σύνολο των κόμβων του δικτύου, ώστε να μεγιστοποιείται η διάρκεια λειτουργίας του.

Τα ασύρματα δίκτυα αισθητήρων βρίσκουν εφαρμογή σε ιδιαίτερα πολύπλοκες εφαρμογές όπως είναι η παρακολούθηση οχημάτων [96], η καταγραφή της υποθαλάσσιας ζωής [114] και η παρακολούθηση και ο χαρακτηρισμός της κίνησης των ανθρώπων [115]. Σε όλες αυτές τις περιπτώσεις, η ανίχνευση των γεγονότων επιτυγχάνεται με την χρήση ενός δικτύου αισθητήρων που εξάγει συμπεράσματα σύμφωνα με τα δεδομένα που καταγράφονται από τα διάφορα αισθητήρια όργανα των κόμβων. Υπάρχουν δύο κυρίαρχες προσεγγίσεις σχετικά με την αντιμετώπιση του προβλήματος της ανίχνευσης απειλών από τα ασύρματα δίκτυα αισθητήρων:

1. Η πρώτη προσέγγιση περιλαμβάνει την απευθείας αποστολή των ακατέργαστων δεδομένων από τους κόμβους του δικτύου στον σταθμό βάσης του. Στο σταθμό βάσης γίνεται μια κεντρικοποιημένη και σύγχρονη αξιολόγηση, ανάλυση και συσχέτιση των δεδομένων όλων των κόμβων του δικτύου. Το κύριο μειονέκτημα αυτής της προσέγγισης είναι η γρήγορη σπατάλη των ενεργειακών πόρων του δικτύου λόγω της συνεχόμενης αποστολής δε3δομένων μειώνοντας έτσι δραστικά την συνολική διάρκεια λειτουργίας του. Επιπλέον, η συνεχής αποστολή δεδομένων ανάμεσα στους κόμβους προκαλεί προβλήματα στην αποδοτική ασύρματη επικοινωνία τους λόγω της εμφάνισης διάφορων φαινομένων όπως είναι η συνεχής εμφάνιση συγκρούσεων των πακέτων (packet collisions) και η γρήγορη κάλυψη όλου του εύρους ασύρματης επικοινωνίας τους (bandwidth).
2. Στην δεύτερη περίπτωση, ο κάθε κόμβος αναλαμβάνει την τοπική αξιολόγηση των δεδομένων του και στην συνέχεια την αποστολή μόνο του αποτελέσματος στον σταθμό βάσης. Ο σταθμός βάσης εκτελεί μια στατιστική αξιολόγηση και συσχέτιση των επιμέρους αποτελεσμάτων ώστε να εξάγει ένα τελικό συμπέρασμα για το σύνολο του δικτύου. Σε αυτή την περίπτωση, η ακρίβεια του τελικού αποτελέσματος υποφέρει από το γεγονός ότι εξαρτάται αποκλειστικά από τα επιμέρους ανεξάρτητα αποτελέσματα των κόμβων. Επιπλέον, η εκτέλεση των διαδικασιών αξιολόγησης των δεδομένων τοπικά

από τους κόμβους επιφέρει κάποια σχετική καθυστέρηση στην έκδοση του αποτελέσματος. Αυτή η καθυστέρηση μπορεί να είναι τόσο μεγάλη ώστε η τελική αναφορά του γεγονότος από τον σταθμό βάσης να γίνεται εκτός των χρονικά αποδεκτών (από την εκάστοτε εφαρμογή) ορίων [116].

Στις παρακάτω ενότητες παρουσιάζεται αναλυτικά μια μέθοδος ανίχνευσης απειλών σε ένα χώρο με την χρήση ασύρματων δικτύων αισθητήρων. Πιο συγκεκριμένα, πρόκειται για μέθοδο η οποία χρησιμοποιεί δεδομένα από ακουστικούς αισθητήρες ώστε να παρέχει την ικανότητα εντοπισμού και έγκαιρης ειδοποίησης στην περίπτωση παρουσίας ενός γεγονότος ενδιαφέροντος μέσα στον επιβλέποντα χώρο. Ως γεγονότα ενδιαφέροντος θεωρούμαι την ύπαρξη και κίνηση ανθρώπων και οχημάτων μέσα στον χώρο. Ο επιτυχής εντοπισμός ενός από τα παραπάνω γεγονότα προϋποθέτει τη εύρεση της θέσης του μέσα στον χώρο με όσο το δυνατόν μεγαλύτερη ακρίβεια και μικτότερη καθυστέρηση από την στιγμή εμφάνισης του. Επιπλέον, η συγκεκριμένη μέθοδος ικανοποιεί της παρακάτω απαιτήσεις, κάνοντας την έτσι εφαρμόσιμη και χρήσιμη σε πραγματικά συστήματα. Οι απαιτήσεις αυτές είναι:

1. **Μακροβιότητα:** Η λειτουργία μιας τυπικής εφαρμογής επιτήρησης διαρκεί από μερικές ημέρες μέχρι μερικούς μήνες. Πολλές φορές οι συσκευές που την απαρτίζουν βρίσκονται κρυμμένες στο χώρο, ώστε να μην είναι εύκολα εντοπίσιμες και προσπελάσιμες από τους κακόβουλους χρήστες. Αυτό το γεγονός δημιουργεί την απαίτηση οι συσκευές να είναι ενεργειακά αυτάρκης καθόλη την διάρκεια λειτουργίας τη εφαρμογής. Έτσι, η μέθοδος που παρουσιάζεται παρακάτω χρησιμοποιεί ένα σχήμα χαμηλής κατανάλωσης, το οποίο μπορεί να επεκτείνει την διάρκεια λειτουργίας των κόμβων αλλά και συνολικά του δικτύου ώστε να είναι διαθέσιμο καθόλη την απαιτούμενη διάρκεια λειτουργίας της εκάστοτε εφαρμογής επιτήρησης.
2. **Προσαρμοστικότητα:** Η μέθοδος θα πρέπει να προσαρμόζεται στο περιβάλλον που θα λειτουργεί και να ρυθμίζει την ευαισθησία της ανάλογα με τις απαιτήσεις της εφαρμογής. Ένα σύστημα ανίχνευσης απειλών εφαρμόζεται κυρίως σε εξωτερικούς χώρους. Αυτό έχει σαν αποτέλεσμα η καταγραφή των ακουστικών κυμάτων και η ανάλυση τους από τους κόμβους να επηρεάζεται σε μεγάλο βαθμό από τις συνθήκες του περιβάλλοντος αλλά και τον θόρυβο που επικρατεί (π.χ. άνεμος). Ακόμα, ανάλογα το είδος και την κρισιμότητα της εφαρμογής επιτήρησης, πολλές φορές είναι αναγκαία η αυξομείωση της ευαισθησίας της μεθόδου και των ακουστικών αισθητήρων. Για παράδειγμα, σε μια κρίσιμη εφαρμογή επιτήρησης είναι αναγκαία η αύξηση της ευαισθησίας ώστε να εντοπισθούν όλες οι πιθανές απειλές, έστω και αν έχουμε σαν αποτέλεσμα μεγάλο αριθμό λανθασμένων εντοπισμών (false alarms). Από την άλλη, στην περίπτωση μιας μη-κρίσιμης εφαρμογής, η χρήση μέτριας ευαισθησίας είναι αρκετή ώστε να έχουμε εντοπισμό του μεγαλύτερου πλήθους των απειλών χωρίς την παραγωγή μεγάλων λανθασμένων εντοπισμών και με αρκετή εξοικονόμηση ενέργειας για τους κόμβους του δικτύου.
3. **Απόκρυψη Ύπαρξης:** Πολλές φορές τα συστήματα επιτήρησης που χρησιμοποιούνται σε κρίσιμες εφαρμογές (όπως είναι οι στρατιωτικές) έχουν την απαίτηση να έχουν μικρή πιθανότητα εντοπισμού και υποκλοπής τους. Το μικρό μέγεθος των κόμβων και η χρήση πλαισίων ασφαλείας (όπως αυτό που

περιγράφτηκε στην προηγούμενη ενότητα) κάνουν την εφαρμογή δύσκολη στην υποκλοπή. Παρόλα αυτά, τα μηνύματα που ανταλλάσσονται ασύρματα ανάμεσα στους κόμβους αποτελούν μια ένδειξη ύπαρξης κάποιου συστήματος. Στην συγκεκριμένη περίπτωση η μέθοδος χρησιμοποιεί όσο το δυνατόν μικρότερο αριθμό μηνυμάτων, ώστε να είναι δύσκολος ο εντοπισμός της.

4. **Αποτελεσματικότητα:** Η αποτελεσματικότητα μιας μεθόδου επιτήρησης εξαρτάται από την ακρίβεια του σημείου εντοπισμού ενός γεγονότος αλλά και το χρόνο που απαιτεί για να το εντοπίσει. Η πλειοψηφία των εφαρμογών έχουν χαλαρές απαιτήσεις για τις παραπάνω δύο τιμές. Έτσι μια μέθοδος με ακρίβεια εντοπισμού μερικά μέτρα και χρόνο καθυστέρησης μερικά δευτερόλεπτα καλύπτει πλήρως τις ανάγκες της πλειοψηφίας των εφαρμογών επιτήρησης [117-118].

6.1 Υφιστάμενες Μέθοδοι

Με την ανάπτυξη των ασύρματων δικτύων αισθητήρων η καταγραφή δεδομένων για την ανίχνευση και παρακολούθηση γεγονότων δημιούργησε πρόσφορο έδαφος για την ανάπτυξη πλήθους ερευνητικών εφαρμογών. Οι εφαρμογές που αναπτύχθηκαν βασίζουν την λειτουργία τους στην χρήση μεμονωμένων ή και συνδυασμού διαφορετικών τύπων αισθητήρων.

Ο πιο συνηθισμένος τύπος αισθητήρα που χρησιμοποιείται στις εφαρμογές είναι ο ακουστικός. Έτσι πλήθος εμπορικών [23-27] και ερευνητικών εφαρμογών [33, 119, 120, 132] βασίζονται στην χρήση των ακουστικών αισθητήρων. Πιο συγκεκριμένα, κάθε εφαρμογή χρησιμοποιεί έναν ή περισσότερους ακουστικούς αισθητήρες οι οποίοι είναι συγχρονισμένοι και καταγράφουν ταυτόχρονα οποιοδήποτε ακουστικό φαινόμενο συμβεί στον χώρο [121]. Πολλές από αυτές τις εφαρμογές είναι φορητές, ενώ υπάρχουν και περιγραφές ενσωμάτωσης των ακουστικών αισθητήρων στα κράνη των στρατιωτών για την χρήση τους στο πεδίο της μάχης [32].

Πολλές αναφορές υπάρχουν για ανάπτυξη συστημάτων επιτήρησης που κάνουν χρήση ακουστικών αισθητήρων και έχουν τοποθετηθεί σε εφαρμογές του πραγματικού κόσμου. Πιο συγκεκριμένα, οι Szewczyk et al. [122] περιγράφουν την ανάπτυξη ενός συστήματος παρακολούθησης ζώων στην περιοχή Great Duck Island με διάρκεια συνεχούς λειτουργίας αρκετούς μήνες. Οι Zhang et al. [123] περιγράφουν ένα σύστημα καταγραφής της άγριας ζωής το οποίο βασίζεται σε ασύρματα δίκτυα αισθητήρων.

Ένα παράδειγμα εφαρμογής που κάνει χρήση συνδυασμού αισθητήρων είναι η εργασία [117]. Οι συγγραφείς περιγράφουν ένα δίκτυο επιτήρησης το οποίο ανιχνεύει κινούμενους στόχους. Το σύστημα χρησιμοποιεί κόμβου Mica2, εφοδιασμένους με μαγνητόμετρα, ακουστικούς αισθητήρες και αισθητήρες κίνησης. Το σύστημα έχει την ικανότητα να αναφέρει έναν στόχο ως κινούμενο άνθρωπο ή όχημα, προσφέροντας έτσι μια λειτουργία αναγνώρισης του στόχου. Παρόλα αυτά η ανάλυση και συσχέτιση τόσων δεδομένων από διαφορετικούς αισθητήρες απαιτεί μεγάλη επεξεργαστική ισχύ και μεγάλη χωρητικότητα μνήμης από τους κόμβους, κάνοντας έτσι την εφαρμογή αναποτελεσματική. Επιπλέον, ο κάθε αισθητήρας κίνησης που χρησιμοποιείται κοστίζει περισσότερο από 400 δολάρια, κάτι που δεν αποτελεί και την καλύτερη λύση για την δημιουργία ενός αποτελεσματικού και οικονομικού συστήματος.

Γενικά, πλήθος εφαρμογών επιτήρησης βασίζονται σε κατανεμημένους ανεξαρτήτους ακουστικούς αισθητήρες. Όπως είναι προφανές, το κύριο πρόβλημα που καλούνται να λύσουν αυτές οι εφαρμογές είναι ο συγχρονισμός των κόμβων. Η πλειοψηφία των αλγορίθμων υπολογισμού της θέσης μιας απειλής βασίζονται στην διαφορά του χρόνου άφιξης ρου ακουστικού φαινομένου στους κόμβους ώστε να υπολογίσουν το σημείο που βρίσκεται η πηγή του. Έτσι, ο λάθος συγχρονισμός των κόμβων έχει σαν αποτέλεσμα την λήψη λάθος παραμέτρων από τον αλγόριθμο εντοπισμού, οπότε και τον λανθασμένο υπολογισμό της θέσης της απειλής. Υπάρχουν εργασίες που προτείνουν διάφορες τεχνικές συγχρονισμού των κόμβων [124-126], οι οποίες όμως απαιτούν την ανταλλαγή αρκετών μηνυμάτων σπαταλώντας έτσι μεγάλες ποσότητες της ενέργειας των κόμβων.

Στις εργασίες [33,127,128] μελετώνται το μέγεθος της επίδρασης του λανθασμένου συγχρονισμού ανάμεσα στους κόμβους στην ικανότητα του συστήματος για τον ακριβή εντοπισμό της απειλής. Η μελέτη βασίζεται στην διενέργεια προσομοιώσεων τύπου Monte Carlo. Ένα από τα αποτελέσματα της μελέτης είναι το γεγονός ότι η ανακρίβεια του συστήματος εντοπισμού αυξάνεται σημαντικά (>2μ) όταν το λάθος συγχρονισμού ανάμεσα στους κόμβους ξεπερνάει τα 4ms.

Γενικά οι μέθοδοι υπολογισμού της θέσης της πηγής ενός ακουστικού φαινομένου βασίζονται στην διαφοροποίηση διάφορων ιδιοτήτων του φαινομένου που παρατηρούνται από κόμβο σε κόμβο. Αυτές οι ιδιότητες μπορεί να είναι: η γωνία άφιξης του ακουστικού κύματος (angle of arrival - AOA), ο χρόνος άφιξης του (time of arrival - TOA), η χρονική διαφορά άφιξης του ίδιου κύματος σε διαφορετικούς κόμβους (time difference of arrival - TDOA), η ισχύς του κύματος (received signal strength - RSS), και η απόκριση κατευθυνόμενης ισχύος γνωστή και ως beamforming (steered response power - SRP). Η χρήση των παραπάνω ιδιοτήτων του ακουστικού κύματος βοηθάνε στο προσδιορισμό της κατεύθυνσης του αλλά και στον προσδιορισμό της θέσης της ηχητικής πηγής του. Το μεγαλύτερο πλήθος των μεθόδων εντοπισμού ενός ακουστικού φαινομένου κάνουν χρήση των TDOA και SRP.

Μια πολύ γνωστή μέθοδος που βασίζεται στην χρήση του SRP είναι η Steered Response Power – Phase Transform (SRP-PHAT)[129]. Η συγκεκριμένη μέθοδος υπολογίζει με ακρίβεια την πηγή ενός ακουστικού κύματος και δεν επηρεάζεται από την ύπαρξη αντηχήσεων του, κάνοντας την έτσι αποτελεσματική για χρήση σε εξωτερικούς αστικούς χώρους. Παρόλα αυτά η χρήση της σε εφαρμογές ασύρματων δικτύων αισθητήρων είναι απαγορευτική καθώς απαιτεί πολύπλοκες, χρονοβόρες και ενεργοβόρες υπολογιστικές διαδικασίες για τον εντοπισμό της ακουστικής πηγής.

Εναλλακτικά, το πρόβλημα μπορεί να λυθεί χρησιμοποιώντας μια μέθοδο δύο σταδίων [130]. Το πρώτο στάδιο της μεθόδου βασίζεται στην διαφορά άφιξης των κυμάτων στους κόμβους (TDOA) ώστε να κάνει μια πρώτη συσχέτιση ανάμεσα στα αφιχθέντα, από τους κόμβους, σήματα [131]. Στην συνέχεια οι TDOA τιμές που παράγονται συνδυάζονται ώστε να υπολογιστεί το σημείο της ακουστικής πηγής.

Υπάρχουν τρείς διαφορετικές προσεγγίσεις για την εκτίμηση των TDOA τιμών [131]. Αυτές είναι: η προσέγγιση συσχέτισης (general cross-correlation - GCC), η προσέγγιση μέγιστης ομοιότητας (maximum likelihood - ML) και η προσέγγιση μετασχηματισμού της φάσης (phase transform - PHAT). Όλες οι παραπάνω προσεγγίσεις υπολογίζουν την συσχέτιση των κυμάτων με έναν βέλτιστο ή ημι-βέλτιστο τρόπο και επιλέγουν μια συγκεκριμένη στιγμή όλων των κύματα να είναι η συνολική TDOA τιμή.

Οι μέθοδοι εντοπισμού δύο σταδίων διακρίνονται για την ταχύτητα τους αλλά πολλές φορές εμφανίζουν πρόβλημα προσαρμοστικότητας [131]. Για παράδειγμα, πολλές φορές γίνεται λάθος υπολογισμός της χρονικής καθυστέρησης του κύματος εξαιτίας της ύπαρξης αντηχήσεων. Οι οποίες μερικές φορές έχουν μεγαλύτερη ενέργεια ακόμα και από το ίδιο κύμα που προέρχεται απευθείας από την πηγή.

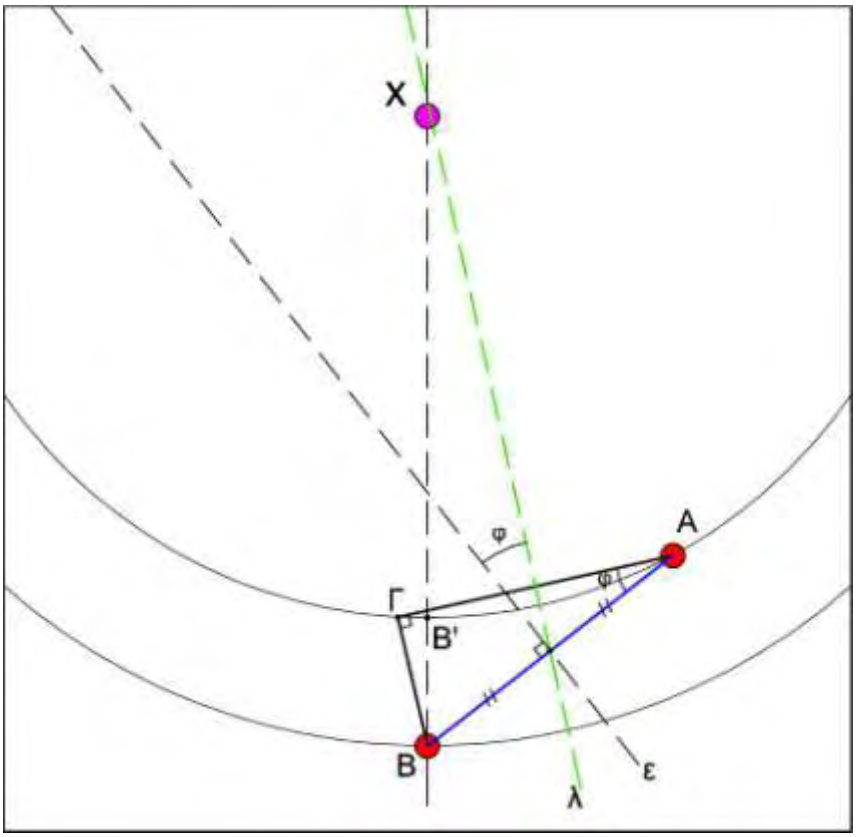
Παρόλα αυτά, η μέθοδος που παρουσιάζεται παρακάτω κάνει χρήση της προσέγγισης δύο σταδίων υπολογισμού, λόγω της ταχύτητας υπολογισμού και των χαμηλών υπολογιστικών απαιτήσεων που έχει.

6.2 Βασική αρχή προσδιορισμού της θέσης μιας ηχητικής πηγής

Όπως περιγράφηκε αναλυτικά στο Κεφάλαιο 2, τα ακουστικά κύματα που παράγονται από μια ηχητική πηγή διαδίδονται στον αέρα με συγκεκριμένο τρόπο και ταχύτητα. Η διάδοση των κυμάτων εξαρτάται σε μεγάλο βαθμό από τις περιβαλλοντικές συνθήκες του μέσου στο οποίο διαδίδεται. Η μέθοδος που αναλύεται λαμβάνει υπόψη τον τρόπο διάδοσης αυτών των ακουστικών κυμάτων προκειμένου να εντοπίσει την θέση της πηγής τους. Βασικό συστατικό της είναι ένα σύνολο ασύρματων κόμβων κατανεμημένων στην περιοχή διάδοσης των κυμάτων.

Οι ασύρματοι αυτοί κόμβοι φέρουν ακουστικούς αισθητήρες (μικρόφωνα). Αυτοί οι ακουστικοί αισθητήρες καταγράφουν συνεχώς τα ακουστικά κύματα τα επεξεργάζονται και εξάγουν συμπεράσματα τα οποία στέλνονται ασύρματα στο σταθμό βάσης του δικτύου. Στη συγκεκριμένη περίπτωση, οι κόμβοι στέλνουν στον σταθμό βάσης την στιγμή όπου έγινε η άφιξη του ακουστικού κύματος σε κάθε έναν από αυτούς. Στην συνέχεια ο σταθμός βάσης χρησιμοποιεί τα αποτελέσματα του κάθε κόμβου και υπολογίζει την χρονική διαφορά μεταξύ των αφίξεων του ακουστικού κύματος από κόμβο σε κόμβο. Ο σταθμός βάσης συνδυάζει αυτή την χρονική διαφορά αφίξεων του κύματος με την απόσταση ανάμεσα στους κόμβους και τις περιβαλλοντικές συνθήκες που επικρατούν τη συγκεκριμένη στιγμή ώστε να υπολογίσει την θέση της πηγής του κύματος. Ουσιαστικά η παραπάνω διαδικασία αποτελεί μια μέθοδο εντοπισμού δύο σταδίων. Το $1^{ο}$ στάδιο είναι ο υπολογισμός του χρόνου άφιξης του κύματος από του κόμβους και το $2^{ο}$ στάδιο αποτελείται από το συνδυασμό των χρόνων άφιξης του κύματος στους κόμβους με επιπλέον χρήσιμες πληροφορίες (απόσταση κόμβων και περιβαλλοντικέ συνθήκες).

Η Εικόνα 37 παρουσιάζει τον τρόπο συσχέτισης της χρονικής διαφοράς αφίξεων με τη απόσταση ανάμεσα στους κόμβους ώστε να υπολογίσει την θέση της πηγής. Για λόγους απλότητας παρουσιάζεται η συσχέτιση δυο μόνο κόμβων.



Εικόνα 42: Ο υπολογισμός της πηγής του ακουστικού κύματος μέσω της διαφοράς άφιξης του κύματος σε δύο κόμβους.

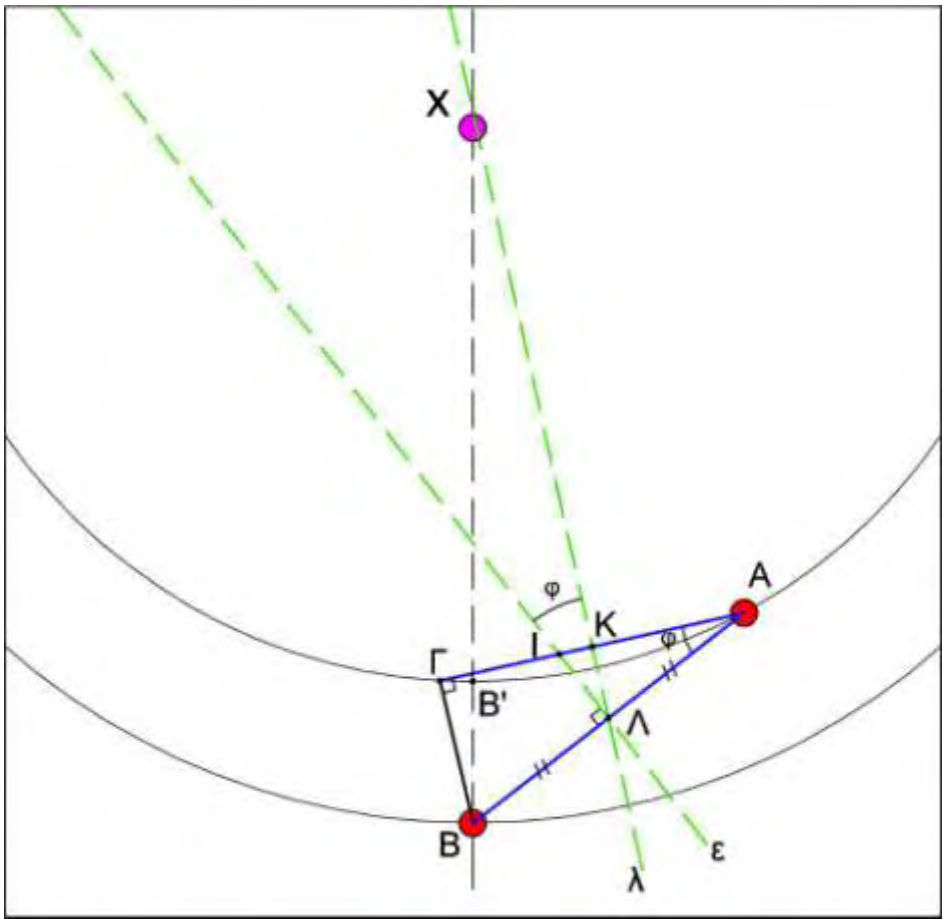
Έστω, στο παραπάνω σχήμα, Χ η θέση της ηχητικής πηγής, Α και Β οι θέσεις των δύο κόμβων με γνωστή την μεταξύ τους απόσταση. Σύμφωνα με το σχήμα, όταν ένα ακουστικό κύμα δημιουργηθεί στην πηγή Χ, θα φτάσει πρώτα στον κόμβο Α και έπειτα στον κόμβο Β. Αυτό οφείλεται στις θέσεων των κόμβων και στον τρόπο διάδοσης των κυμάτων. Α η χρονική διαφορά άφιξης του κύματος στους κόμβους είναι η τιμή t, τότε το t * (ταχύτητα του ήχου) ισοδυναμεί με την απόσταση ΒΒ΄. Στην περίπτωση όπου η απόσταση της ηχητικής πηγής από τους κόμβους είναι αρκετά μεγάλη σε σχέση με την απόσταση ανάμεσα στους κόμβους ΑΒ, μπορεί με ασφάλεια να γίνει η προσέγγιση ότι ο ΒΓ==ΒΒ΄. Όπου Γ θεωρείται το σημείο πάνω στον ομόκεντρο κύκλο (ηχητικό κύμα) που ανήκει το σημείο Α και ισχύει ότι η γωνία ΑΓΒ = 90^{o}. Στο ορθογώνιο τρίγωνο ΑΒΓ που δημιουργείται, έστω η γωνία ΒΑΓ = φ . Η γωνία φ μπορεί να υπολογιστεί εύκολα αφού ισχύει ημ(φ) = ΓΒ/ΑΒ . Στην συνέχεια στην μεσοκάθετο του ευθυγράμμου τμήματος ΑΒ φέρεται ευθεία σε γωνία φ. Η ευθεία αυτή που δημιουργήθηκε (έστω ε) διέρχεται πάνω από το σημείο της ηχητικής πηγής.

6.2.1 Απόδειξη μεθόδου υπολογισμού θέσης της πηγής

Σύμφωνα με την Εικόνα 42, το σημείο Χ της ηχητικής πηγής αποτελεί το κέντρο ομόκεντρων κύκλων. Αυτοί οι ομόκεντροι κύκλοι είναι τα ηχητικά κύματα της πηγής τα οποία θεωρητικά διαδίδονται προς όλες τις κατεύθυνσης με τον ίδιο τρόπο. Για να γίνει η απόδειξη ότι η τελική ευθεία ε που σχηματίζεται διέρχεται από το σημείο Χ αρκεί η

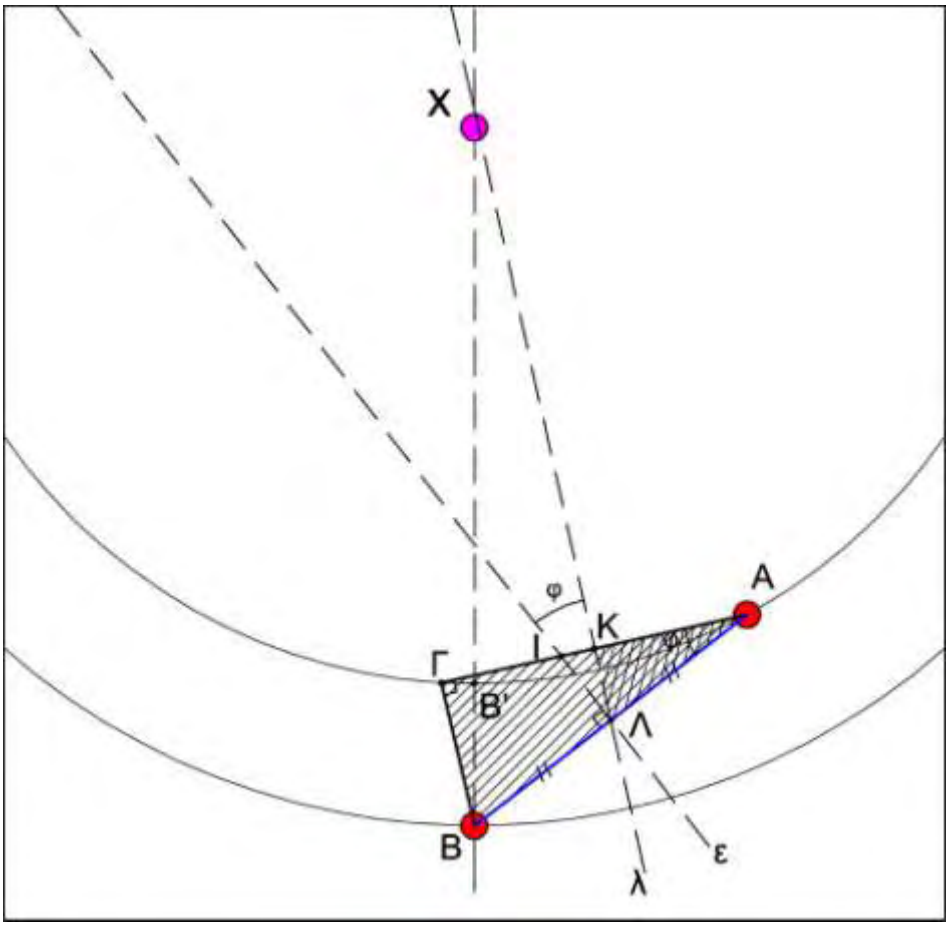
ευθεία αυτή να αποτελεί και μεσοκάθετο του ευθύγραμμου τμήματος ΑΓ. Εφόσον οι άκρες του ΑΓ ανήκουν στον ίδιο κύκλο, η μεσοκάθετος του θα περνάει από το κέντρο Χ του κύκλου (θέση ηχητικής πηγής).

Εξ'ορισμού, η οξεία γωνία που δημιουργείται από τις ευθείς ε και λ (έστω ΙΛΚ η γωνία) είναι φ και ίση με την γωνία ΒΑΓ. Ακόμα είναι γνωστό ότι η ευθεία λ είναι μεσοκάθετος του ευθύγραμμου τμήματος ΑΒ. Οπότε εφόσον οι 2 γωνίες ΙΛΚ και ΓΑΒ είναι ίσες και η μια πλευρά της μιας γωνίας τέμνεται κάθετα με την μια πλευρά της άλλης, τότε και οι δύο άλλες πλευρές των γωνιών θα τέμνονται κάθετα. Οπότε η ευθεία ε τέμνει κάθετα το τμήμα ΑΓ.



Εικόνα 43: Με έντονα χρώματα φαίνονται οι 2 ίσες γωνίες.

Για να αποδεχτεί το γεγονός ότι η ευθεία ε τέμνει το τμήμα ΑΓ στο μέσο του θα χρησιμοποιηθούν κριτήρια ομοιότητας τριγώνων. Έτσι τα τρίγωνα ΑΒΓ και ΑΛΚ είναι όμοια επειδή έχουν όλες τις γωνίας τους ίσες. Άρα εφόσον το ΑΒ = 2*ΑΛ θα ισχύει και ΑΓ = 2 * ΑΚ.



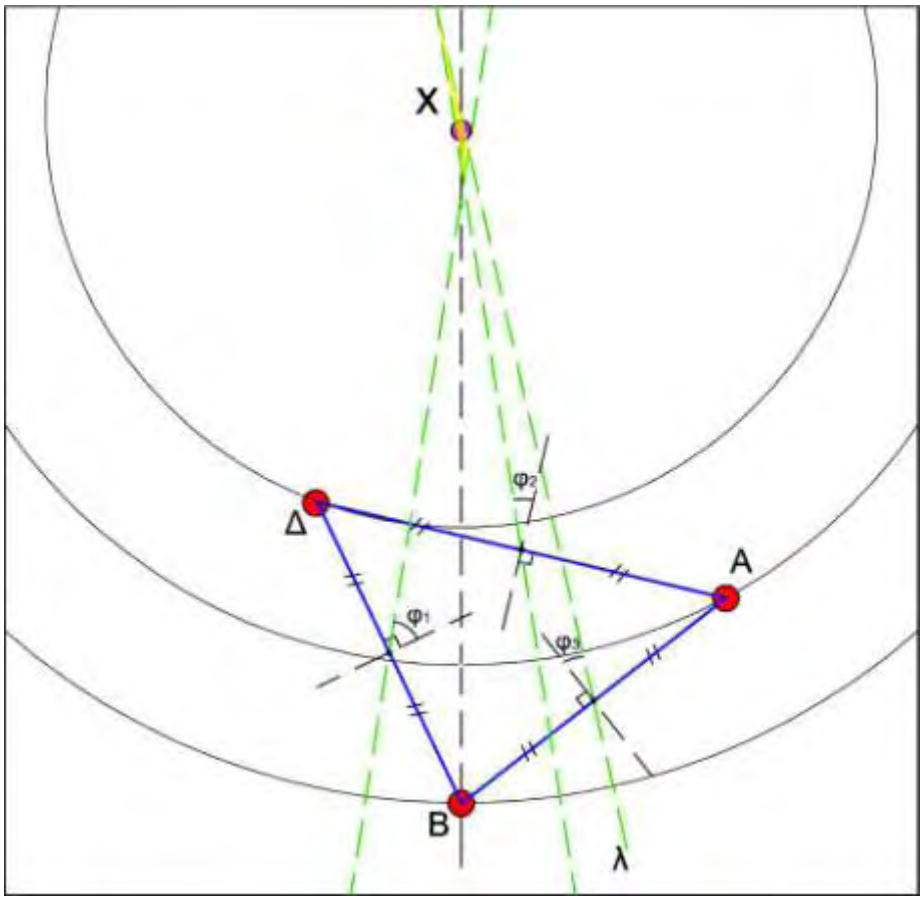
Εικόνα 44: Με έντονη σκίαση φαίνονται τα δύο όμοια τρίγωνα.

Οι παραπάνω συλλογισμοί απέδειξαν ότι η ευθεία ε αποτελεί μεσοκάθετο του ευθύγραμμου τμήματος ΑΓ, οπότε και διέρχεται από το σημείο Χ της ηχητικής πηγής.

6.2.2 Μέθοδος εντοπισμού με πλήθος ακουστικών κόμβων (>2)

Το αποτέλεσμα της μεθόδου εντοπισμού της ηχητικής πηγής στην περίπτωση όπου χρησιμοποιούνται δύο ακουστικοί αισθητήρες είναι μια ευθεία γραμμή. Η ευθεία αυτή έχει την ιδιότητα να διέρχεται από την θέση της ηχητικής πηγής.

Η αύξηση της ακρίβειας της μεθόδου εντοπισμού απαιτεί την χρήση περισσότερων αισθητήρων. Η εισαγωγή ενός επιπλέον ακουστικού αισθητήρα (Εικόνα 45, έστω τα Α, Β, Δ αισθητήρες) αυξάνει τον συνολικό αριθμό αισθητήρων στους 3. Έτσι, η μέθοδος εντοπισμού μπορεί να εκτελεστεί τρείς φορές παίρνοντας κάθε φορά σαν παράμετρο τα τρία διαφορετικά ζευγάρια των αισθητήρων (ΑΒ, ΑΔ, ΒΔ). Κάθε εκτέλεση της μεθόδου δημιουργεί και μια νέα ευθεία η οποία διέρχεται από την θέση της ηχητικής πηγής. Κατόπιν, τα σημεία τομής τω ευθειών αυτών βρίσκονται ιδανικά ακριβώς πάνω από την θέση της ηχητικής πηγής.



Εικόνα 45: Ο υπολογισμός της περιοχής όπου βρίσκεται η πηγή του ακουστικού κύματος χρησιμοποιώντας την διαφορά άφιξης του ακουστικού κύματος τριών σημείων.

Στην πραγματικότητα, λόγω διάφορων προσεγγίσεων που έγιναν κατά την εκτέλεση της μεθόδου (π.χ. στη Εικόνα 42 τα ΒΓ==ΒΒ΄), οι ευθείες που δημιουργούνται δεν διέρχονται ακριβώς πάνω από την θέση της πηγής, αλλά διέρχονται πολύ κοντά από αυτή. Έτσι, τα σημεία τομής τω τριών ευθειών δεν βρίσκονται ακριβώς στην θέση της πηγής, αλλά σχηματίζουν μια τρίγωνη περιοχή πρόβλεψης μέσα στην οποία βρίσκεται η θέση της ηχητικής πηγής. Ουσιαστικά, το μέγεθος αυτής της περιοχής πρόβλεψης ορίζει την ακρίβεια της μεθόδου. Αύξηση της ακρίβειας εντοπισμού προϋποθέτει την χρήση περισσότερων ακουστικών αισθητήρων, τοποθετημένων σε μεγάλες αποστάσεις μεταξύ τους.

6.3 Βασικά συστατικά της μεθόδου εντοπισμού

Η μέθοδος εντοπισμού της ηχητικής πηγής αποτελείται από ένα σύνολο επιμέρους διαδικασιών, από τις οποίες μερικές είναι διακριτές (όπως περιέχονται στην παραπάνω περιγραφή της μεθόδου) και άλλες όχι. Οι συγκεκριμένες διαδικασίες εκτελούνται παράλληλα, παρέχοντας στην μέθοδο εντοπισμού τις πληροφορίες και λειτουργίες που είναι απαραίτητες για την ορθότερη και βέλτιστη εκτέλεση των υπολογισμών της. Στην πραγματικότητα, αυτές οι διαδικασίες αναλαμβάνουν τον χειρισμό των ασύρματων κόμβων, την επεξεργασία των δεδομένων τους και την καταγραφή των περιβαλλοντικών

συνθηκών. Επομένως, η ορθότητα και η ακρίβεια της μεθόδου εντοπισμού εξαρτάται σε μεγάλο βαθμό από την αποτελεσματικότητα των επιμέρους αυτών διαδικασιών αλλά και της συνεργασίας τους, Ειδικότερα, οι εν λόγω διαδικασίες αναλαμβάνουν:

1. Τον υπολογισμό της χρονικής διαφοράς της άφιξης του κύματος στους κόμβους.
2. Τον συγχρονισμό των ασύρματων κόμβων
3. Τον υπολογισμό ενός κατωφλίου
4. Τη καταγραφή των περιβαλλοντικών συνθηκών και υπολογισμού της ταχύτητας διάδοσης του ακουστικού κύματος.
5. Τη καταγραφή της θέσης των κόμβων.

6.3.1 Υπολογισμός της χρονικής διαφοράς άφιξης του κύματος.

Βασική αρχή στον υπολογισμό της θέσης της ηχητικής πηγής αποτελεί η καταγραφή του ακουστικού κύματος και ο υπολογισμός της χρονικής διαφοράς άφιξης του από όλους τους ακουστικούς κόμβους του δικτύου. Ο υπολογισμός αυτής της χρονικής διαφοράς μπορεί να πραγματοποιεί με δύο τρόπους:

1. Με την χρήση μεθόδων ψηφιακής επεξεργασίας σήματος
2. Με την χρήση ενός χαρακτηριστικού σημείου των κυματομορφών παρατηρώντας έτσι την χρονική καθυστέρηση εμφάνισης του σήματος στον κάθε αισθητήρα.

6.3.1.1 Χρήση μεθόδων ψηφιακής επεξεργασίας σημάτων για τον προσδιορισμό ηχητικής πηγής

Στην βιβλιογραφία υπάρχει πλήθος μελετών [133-136] που προτείνουν την χρήση μεθόδων ψηφιακής επεξεργασίας ενός ακουστικού κύματος με σκοπό τον εντοπισμό της ηχητικής πηγής του. Συγκεκριμένα, στην περίπτωση ύπαρξης ενός ακουστικού κύματος που καταγράφεται από 2 αισθητήρες, γίνεται η θεώρηση ότι το κύμα και μια "καθυστερημένη έκδοση" του κύματος στα οποία έχει προστεθεί θόρυβος, λαμβάνονται από το ζευγάρι των αισθητήρων. Η καθυστέρηση άφιξης του ακουστικού κύματος ανάμεσα στους δύο αισθητήρες μπορεί να υπολογισθεί με την χρήση μιας συνάρτησης συσχέτισης.

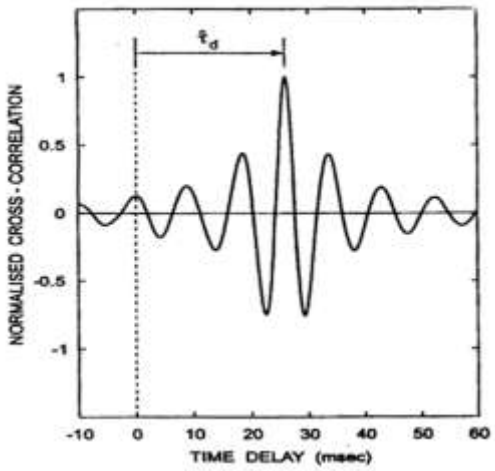
Η μορφή κάθε ακουστικού κύματος που διαδίδεται στον χώρο εξαρτάται από 2 συνιστώσες, την συνιστώσα του κύματος που παράγεται από την ηχητική πηγή και την συνιστώσα του θορύβου του περιβάλλοντος όπου διαδίδεται αυτό. Λαμβάνοντας υπόψη τις δύο αυτές συνιστώσες, τα ακουστικά κύματα που καταγράφηκαν από τους παραπάνω δύο αισθητήρες μπορούν να μοντελοποιηθούν με τις παρακάτω μαθηματικές σχέσεις:

$$\begin{aligned} x(t) &= s(t) + n_x(t) \\ y(t) &= s(t-\tau_d) + n_y(t), \quad 0 \le t \le T, \end{aligned} \tag{1}$$

όπου x(t) και y(t) τα δύο ακουστικά κύματα που καταγράφηκαν, s(t) η συνιστώσα του κύματος στον πλησιέστερο στην πηγή αισθητήρα, $s(t-\tau_d)$ η συνιστώσα του κύματος στον πιο απομακρυσμένο αισθητήρα που έχει καθυστέρηση κατά τ_d. Στην κάθε συνιστώσα του κύματος έχει προστεθεί θόρυβος με μηδενική μέση τιμή, κατανομής Gauss, ασυσχέτιστος για τις δύο θέσεις x και y των αισθητήρων και επιπλέον ασυσχέτιστος με το σήμα. Το

χρονικό διάστημα παρατήρησης T, θεωρείται πολύ μεγαλύτερο από την καθυστέρηση τ_d. Το μοντέλο υποθέτει σταθερή καθυστέρηση τ_d που απαιτεί πηγή σταθερή σε σχέση με την θέση των δύο αισθητήρων καθ' όλη την διάρκεια παρατήρησης T. Τέλος η εξασθένιση της έντασης του σήματος λόγω της διαφοράς δρόμων ανάμεσα στην πηγή και τους αισθητήρες θεωρείται μοναδιαία.

Η πρόβλεψη της χρονικής καθυστέρησης στην άφιξη του μετώπου του ακουστικού σήματος ανάμεσα στους δύο αισθητήρες μπορεί να επιτευχθεί με τον υπολογισμό της συνάρτησης συσχέτισης $R_{xy}(\tau)$, ανάμεσα στο σήμα και την "καθυστερημένη έκδοσή" του, οπότε η τιμή του χρόνου για την οποία η συνάρτηση συσχέτισης παίρνει την μέγιστη τιμής της αντιστοιχεί στην προβλεπόμενη χρονική καθυστέρηση $\hat{\tau}_d$ (Εικόνα 46).



Εικόνα 46: Η χρονική διάρκεια $\hat{\tau}_d$ όπου η συνάρτηση συσχέτισης παίρνει την μέγιστη τιμή της.

Για την απλή περίπτωση που οι όροι του θορύβου είναι στατιστικά ανεξάρτητες μεταξύ τους, η συνάρτηση συσχέτισης $R_{xy}(\tau)$, για τα λαμβανόμενα σήματα, x(t) και y(t), δίνεται από την σχέση:

$$R_{xy}(\tau) = E[x(t)y(t+\tau)] = R_{ss}(\tau-\tau_d) \qquad (2)$$

όπου E[.] ο τελεστής πρόβλεψης και $R_{ss}(\tau)$ η συνάρτηση αυτοσυσχέτισης του σήματος s(t), έχοντας μετατραπεί ώστε να παίρνει την μέγιστη τιμή της στο σημείο $\tau=\tau_d$. Προφανώς η συνάρτηση συσχέτισης παίρνει την μέγιστη τιμή της για την χρονική καθυστέρηση $\tau_d=(\Delta d)/c$, όπου Δd η διαφορά δρόμων και c είναι η (υποθέτοντας την σταθερή) η ταχύτητα του ήχου στο ακουστικό μέσο.

Εναλλακτικά, η συνάρτηση συσχέτισης μπορεί να υπολογιστεί από την συνάρτηση πυκνότητας φάσματος $G_{xy}(f)$, των λαμβανομένων σημάτων χρησιμοποιώντας τον μετασχηματισμό Fourier:

$$R_{xy}(\tau) = \int G_{xy}(f) \exp(j2\pi f\tau)df, \qquad (3)$$

όπου:

$$G_{xy}(f) = G_{ss}(f)\exp(-j2\pi f\tau_d). \quad (4)$$

Στην τελευταία σχέση η χρονική καθυστέρηση τ_d εμφανίζεται στην πυκνότητα φάσματος ως συνάρτηση φάσης η οποία δίνεται από την σχέση:

$$\varphi_{xy}(f) = 2\pi f\tau_d. \quad (5)$$

Είναι φανερό ότι είτε με την ανάλυση στο πεδίο του χρόνου είτε με αυτήν στο πεδίο της συχνότητας η $R_{xy}(\tau)$ παίρνει την μέγιστη τιμή της για $\tau=\tau_d$.

Εφόσον ο πολλαπλασιασμός στο πεδίο της συχνότητας είναι συνέλιξη στο πεδίο του χρόνου και αντίστροφα συνεπάγεται ότι:

$$R_{xy}(\tau) = R_{ss}(\tau) * \delta(\tau-\tau_\delta), \quad (6)$$

όπου $*$ η συνέλιξη και δ η συνάρτηση δέλτα Dirac. Από την σχέση αυτή φαίνεται ότι η συνάρτηση δέλτα διαπλατύνεται από τον μετασχηματισμό Fourier του φάσματος του σήματος. Υποθέτοντας λευκό θόρυβο, ο μετασχηματισμός Fourier του φάσματος του σήματος είναι μια συνάρτηση δέλτα οπότε δεν έχουμε καμία διαπλάτυνση. Για ζωνοπερατό λευκό θόρυβο, ο μετασχηματισμός Fourier του φάσματος του σήματος είναι συνιμητονοειδής συνάρτηση διαμορφωμένη από μία συνάρτηση sinc, έτσι ώστε η διαπλάτυνση να μεγαλώνει καθώς μειώνεται το εύρος ζώνης όπως φαίνεται από την:

$$R_{ss} = P_s \frac{\sin(\pi B\tau)}{\pi B\tau} \cos 2\pi f_o\tau, \quad (7)$$

όπου P_s η ισχύς του σήματος, B το εύρος ζώνης, και f_o η κεντρική συχνότητα. Καθώς το εύρος ζώνης του σήματος γίνεται πολύ μικρό σε σχέση με την κεντρική συχνότητα τα μέγιστα στην συνάρτηση συσχέτισης τείνουν να έχουν το ίδιο πλάτος με αποτέλεσμα η αναγνώριση του μεγίστου που δίνει την ζητούμενη διαφορά χρόνου γίνεται ιδιαίτερα δύσκολη.

Η τυπική απόκλιση της εκτιμούμενης χρονικής καθυστέρησης γύρω από την πραγματική τιμής της χρονικής καθυστέρησης είναι μεγαλύτερη ή ίση από την τιμή (κάτω φράγμα Cramer-Rao):

$$\sigma_{CR}^2 = \left\{ 2T \int_0^\infty (2\pi f)^2 \frac{|\gamma(f)|^2}{1-|\gamma(f)|^2} df \right\}^{-1}, \quad (8)$$

όπου γ η συνάρτηση:

$$|\gamma(f)|^2 = \frac{G_{ss}^2(f)}{[G_{ss}(f)+G_{nn}(f)]^2} \quad (9)$$

όπου $G_{ss}(f)$ η συνάρτηση φάσματος του σήματος και $G_{nn}(f)$ η συνάρτηση φάσματος του θορύβου.

Υποθέτοντας ότι το σήμα και ο θόρυβος είναι ασυσχέτιστες και στατικές διαδικασίες μπορεί να αποδειχτεί ότι το κάτω φράγμα Cramer-Rao δίνεται από την[6]:

$$\sigma_{CR}^2 \approx \frac{3}{4\pi^2 T} \cdot \frac{1}{SNR} \cdot \frac{1}{f_2^3 - f_1^3} \quad \text{για SNR >> 1,} \qquad (10)$$

όπου T το χρονικό διάστημα παρατήρησης και οι τιμές του φάσματος του σήματος και του θορύβου θεωρούνται σταθερές (S_o και N_o W/Hz, αντίστοιχα) στην ζώνη συχνοτήτων f_1 έως f_2 Hz. Σε αυτή την περίπτωση η ισχύς του σήματος $S = S_o(f_2 - f_1)$ και του θορύβου $N = N_o(f_2 - f_1)$ και άρα ο σηματοθορυβικός λόγος, SNR, είναι ίσος με S_o / N_o. Έτσι αυξάνοντας τον χρόνο παρατήρησης, το εύρος συχνοτήτων, ή τον σηματοθορυβικό λόγο μειώνεται η τυπική απόκλιση της εκτιμούμενης καθυστέρησης.

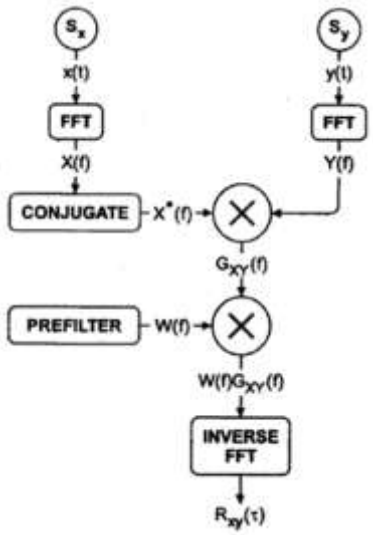
Στην πράξη η συνάρτηση συσχέτισης υπολογίζεται από δεδομένα που συλλέγονται σε ένα πεπερασμένο χρονικό διάστημα T. Πριν τον υπολογισμό της συνάρτησης συσχέτισης, ένας γενικευμένος συσχετιστής φιλτράρει τα λαμβανόμενα σήματα για να βελτιωθεί η ακρίβεια στην εκτίμηση της χρονικής καθυστέρησης $\hat{\tau}_d$.

Η γενικευμένη συνάρτηση συσχέτισης $R_{xy}^{(G)}(\tau_d)$, δίνεται από την σχέση:

$$R_{xy}^{(G)}(\tau_d) = \int_{-\infty}^{\infty} W(f)G_{xy}(f)\exp(j2\pi f\tau)df, \qquad (11)$$

όπου $W(f) = H_x(f)H_y^*(f)$, με $H_x(f)$ και $H_y(f)$ τις συναρτήσεις μεταφοράς του φίλτρου οι οποίες πρέπει να έχουν όμοιες χαρακτηριστικές φάσεις, ή ισοδύναμα η W(f) να είναι πραγματική (W(f)=1 για την κλασσική διαδικασία αυτοσυσχέτισης). Στην Εικόνα 47 φαίνεται ένα μπλοκ διάγραμμα με την υλοποίηση του γενικευμένου συσχετιστή στο πεδίο της συχνότητας.

Ο σηματοθορυβικός λόγος και κατά συνέπεια η πρόβλεψη της χρονικής καθυστέρησης της άφιξη του μετώπου του ηχητικού κύματος από τον πρώτο στον δεύτερο ακουστικό αισθητήρα μπορεί να βελτιωθεί αντικαθιστώντας κάθε έναν από τους ακουστικούς αισθητήρες με μια σειρά από αισθητήρες.



Εικόνα 47: Η υλοποίηση του γενικευμένου συσχετιστή στο πεδίο της συχνότητας.

6.3.1.2 *Χρήση ενός χαρακτηριστικού σημείου των κυματομορφών.*

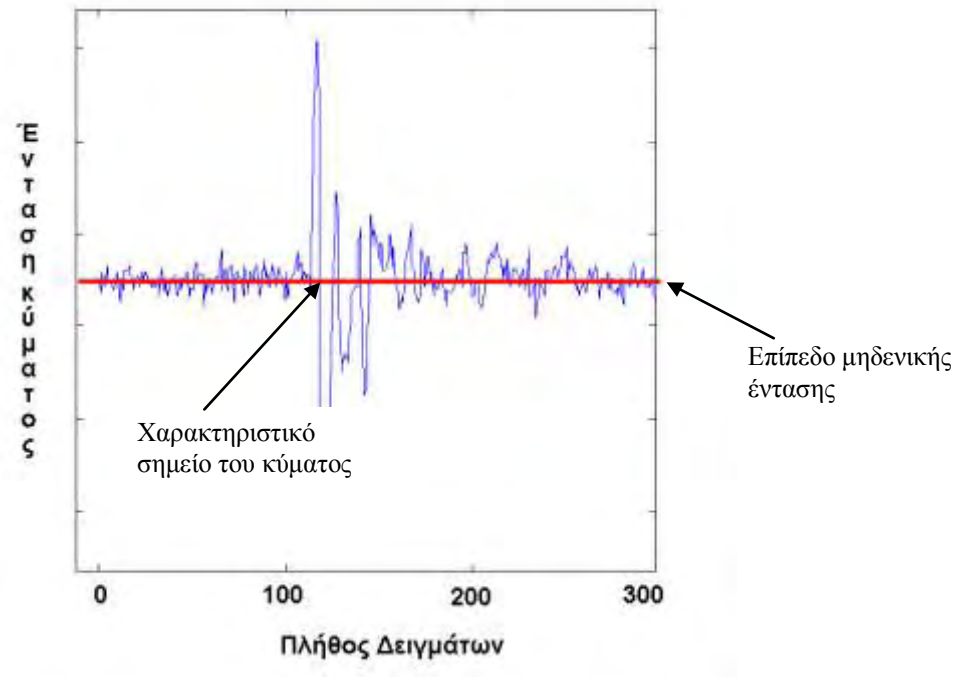
Εναλλακτικά της χρήσης μεθόδων ψηφιακής επεξεργασίας του κύματος για τον εντοπισμό της θέσης της ηχητικής πηγής, μπορεί να χρησιμοποιηθεί ο εντοπισμός ενός κοινού χαρακτηριστικού σημείου του κύματος. Ουσιαστικά, ο υπολογισμός της χρονικής διαφοράς άφιξης ενός κύματος στους αισθητήρες επαφίεται στην χρονική διαφορά της καταγραφής του συγκεκριμένου κοινού σημείου του κύματος από κάθε κόμβο.

Υπάρχει πλήθος προτάσεων για την μέθοδο ορισμού ενός χαρακτηριστικού σημείου ενός κύματος (όπως ο ορισμός του σημείου στην μέγιστη ένταση του κύματος ή στην στιγμή όπου η ένταση του βρίσκεται πάνω από ένα προκαθορισμένο όριο). Οι περισσότερες από αυτές τις μεθόδους υποφέρουν από τα ιδιαίτερα χαρακτηριστικά των ακουστικών αισθητήρων που χρησιμοποιούνται αλλά και του τρόπου καταγραφής του κύματος. Για παράδειγμα, η χρήση ακουστικών αισθητήρων με διαφορετική ευαισθησία θα προκαλέσει την καταγραφή διαφορετικών εντάσεων του ίδιου σήματος. Έτσι ανάλογα την θέση των αισθητήρων σε σχέση με την ακουστική πηγή αλλά και την ευαισθησία τους μπορούν να προκληθούν

- **φαινόμενα ψαλιδισμού** του κύματος λόγω της πολύ απότομης και υψηλής μεταβολής του κύματος (π.χ. έκρηξη)
- **μη καταγραφή των τιμών** που είναι μικρότερες από το επίπεδο θορύβου
- **καταγραφή του κύματος στον κόρο** λόγω την πολύ μεγάλης ευαισθησίας των αισθητήρων αλλά και της πολύ μικρής απόσταση από την ηχητική πηγή.
- Για τους ίδιους λόγους παρουσιάζονται **φαινόμενα μη ελεύθερης ταλάντωσης (μπούκωμα)** των μικροφώνων με αποτέλεσμα να μην είναι η καταγραφή του κύματος όμοια σε όλους του αισθητήρες.

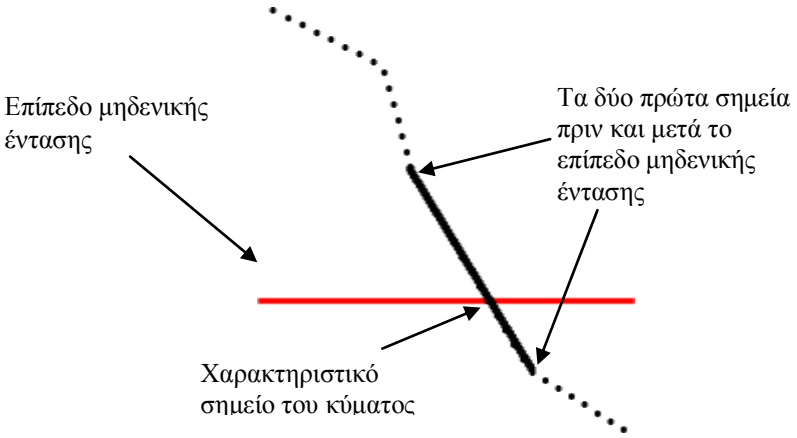
Η αποφυγή των παραπάνω φαινομένων οδηγεί στην επιλογή ενός σημείου μακριά από τις περιοχές του κόρου το οποίο να εξαρτάται όσο το δυνατόν λιγότερο από την ένταση του κύματος. Έτσι το χαρακτηριστικό σημείο του κύματος ορίζεται ως το σημείο

όπου μηδενίζεται για πρώτη φορά (αμέσως μετά από την υπέρβαση ενός καθορισμένου ορίου έντασης) η ένταση του κύματος.



Εικόνα 48: Ορισμός του χαρακτηριστικού σημείου ενός κύματος

Η ανίχνευση αυτού του σημείου είναι μια πολύ απλή διαδικασία για τον αισθητήρα. Δεν απαιτεί την εκτέλεση ιδιαίτερα πολύπλοκων πράξεων και έχει χαμηλές ενεργειακές απαιτήσεις. Η διαδικασία εντοπισμού του σημείου αρχικά ελέγχει την ενέργεια του κύματος προκειμένου να εντοπίσει κάποιο ενεργειακό μέγιστο το οποίο είναι πάνω από κάποιο καθορισμένο όριο. Αφού εντοπιστεί κάποιο τέτοιο μέγιστο (εντοπισμός συμβάντος) ξεκινάει η αναζήτηση του πρώτου σημείου του κύματος το οποίο θα έχει τιμή έντασης είτε ίση είτε μικρότερη από το **επίπεδο μηδενικής έντασης** (επίπεδο αναφοράς) του κύματος. Συγκεκριμένα, στην περίπτωση όπου τα σημεία του κύματος δεν συμπίπτουν ακριβώς πάνω στο επίπεδο μηδενικής έντασης (λόγω της δειγματοληψίας του κύματος) παίρνουμε τα 2 πρώτα σημεία πριν και μετά τον μηδενισμό του κύματος και υπολογίζουμε την ευθεία που διέρχεται από αυτά. Θεωρώντας την καμπύλη του σήματος γραμμική στην περιοχή ανάμεσα σε αυτά τα σημεία, η τομή της ευθείας που διέρχεται από αυτά τα δύο σημεία με το επίπεδο μηδενικής έντασης αποτελεί το χαρακτηριστικό σημείου του κύματος.



Εικόνα 49: Υπολογισμός του χαρακτηριστικού σημείου του κύματος

6.3.2 Συγχρονισμός των ασύρματων κόμβων

Η ακριβής μέτρηση του χρόνου από τους κόμβους αποτελεί σημαντική απαίτηση για την επιτυχή και ακριβής καταγραφή των ακουστικών κυμάτων και των χρόνων άφιξης τους. Οι ασύρματοι κόμβοι που χρησιμοποιούνται μετράνε τον χρόνο μέσω ενός ρολογιού που διαθέτουν. Αυτό το ρολόι είναι και η μοναδική τους αίσθηση με τον χρόνο και είναι ουσιαστικά ένα χρονόμετρο που μετράει τις ταλαντώσεις ενός κρυστάλλου χαλαζία σε μια συγκεκριμένη συχνότητα. Η δημιουργία ενός ρολογιού που προσφέρει μεγάλη ακρίβεια και σταθερότητα στην μέτρηση του χρόνου απαιτεί την χρήση χώρου, ενέργειας και επεξεργαστικής ισχύς τα οποία δεν είναι διαθέσιμα στους ασύρματους κόμβους. Έτσι οι κόμβοι καλούνται να αντιμετωπίσουν συχνά το σφάλμα των ρολογιών που διαθέτουν με την χρήση κατάλληλων πρωτοκόλλων συγχρονισμού. Οι κυριότεροι λόγοι για τους οποίους τα ρολόγια αυτά παρουσιάζουν χρονική ανακρίβεια είναι:

1. Η εκκίνηση των κόμβων και των ρολογιών τους σε διαφορετικές χρονικές στιγμές
2. Η συχνότητα ταλάντωσης του κρυστάλλου χαλαζία μπορεί να διαφέρει από κόμβο σε κόμβο. Αυτό προκαλεί την σταδιακή απόκλιση των ρολογιών των κόμβων.
3. Η συχνότητα ταλάντωσης του κρυστάλλου χαλαζία μπορεί να μεταβάλλεται με την πάροδο του χρόνου καθώς εξαρτάται σε μεγάλο βαθμό από την θερμοκρασία του περιβάλλοντος. [137-138]

Ο συγχρονισμός των ασύρματων κόμβων αποτελεί ένα σημαντικό ζήτημα στην σωστή λειτουργία των δικτύων αισθητήρων. Πρώτον, είναι ζωτικής σημασίας για την λειτουργία του δικτύου τα ρολόγια των κόμβων να είναι συγχρονισμένα με βάση κάποιο γενικό ρολόι. Με αυτό τον τρόπο επιτυγχάνεται η σωστή χρονολόγηση των δεδομένων που καταγράφονται από τους διάφορους κόμβους του δικτύου. Σε διαφορετική περίπτωση, τα δεδομένα θα έχω ανακριβή χρονοσφραγίδα με αποτέλεσμα να είναι πιθανή η λάθος χρονολογική ταξινόμησή τους οπότε και η εξαγωγή λανθασμένων συμπερασμάτων που βασίζονται σε αυτά. Δεύτερον, ο συγχρονισμός των ασύρματων κόμβων είναι σημαντικός για την εύρυθμη και αποδοτική λειτουργία πρωτοκόλλων χαμηλής κατανάλωσης ενέργειας σε αυτά [140]. Ένα ασύρματο δίκτυο αισθητήρων,

κατά την διάρκεια λειτουργίας του, βρίσκεται την περισσότερα ώρα σε κατάσταση «ύπνου» ώστε να μειώσει όσο το δυνατόν περισσότερο την κατανάλωση ενέργειάς του. Στην περίπτωση χρήσης πρωτοκόλλων δρομολόγησης χαμηλής κατανάλωσης ενέργειας, οι ασύρματοι κόμβοι εναλλάσσουν την κατάσταση λειτουργίας τους από σε «πλήρη» σε «ύπνου» και αντίστροφα, κυρίως για δύο λόγους: για την καταγραφή μετρήσεων και για την προώθηση μηνυμάτων των γειτονικών κόμβων. Το τελευταίο προϋποθέτει ότι τουλάχιστον οι γειτονικοί κόμβοι θα πρέπει να είναι συγχρονισμένοι μεταξύ τους έτσι ώστε να συμπίπτουν οι εναλλαγές των καταστάσεων λειτουργίας τους. Θα πρέπει δηλαδή οι κόμβοι να είναι όλοι ταυτόχρονα σε κατάσταση πλήρους λειτουργίας ώστε να μπορέσουν να λάβουν τα μηνύματα και να τα προωθήσουν κατάλληλα. Σε διαφορετική περίπτωση, η διάδοση ενός πακέτου μέσα στο δίκτυο θα μπορούσε να είναι πολύ αργή έως και ανεπιτυχής [139].

Παρακάτω ακολουθεί μια ανασκόπηση των υφιστάμενων πρωτοκόλλων συγχρονισμού των ασύρματων κόμβων αισθητήρων. Τονίζονται οι ιδιαιτερότητες του κάθε πρωτοκόλλου καθώς και οι περιορισμοί που εισάγουν στην περίπτωση της χρήσης τους σε ένα σύστημα επιτήρησης χώρων. Τέλος παρουσιάζεται το πρωτόκολλο το οποίο αναπτύχθηκε με σκοπό την βέλτιστη ικανοποίηση των απαιτήσεων των μεθόδων ανίχνευσης απειλών που περιγράφονται.

6.3.2.1 Υφιστάμενα πρωτόκολλα συγχρονισμού

Η εφαρμογή πρωτοκόλλων συγχρονισμού στα ασύρματα δίκτυα αισθητήρων προϋποθέτει την αντιμετώπιση πολλών περιορισμών και προκλήσεων. Πρώτων, το περιορισμένο πλήθος πόρων που διατίθεται από τους ασύρματους κόμβους αναγκάζει τα πρωτόκολλα να επιτυγχάνουν συγχρονισμό με όσο το δυνατό μικρότερη χρήση τους (για παράδειγμα, η αποστολή όσο το δυνατόν λιγότερο πακέτων συγχρονισμού έτσι ώστε η κεραία να μην καταναλώνει μεγάλα ποσά ενέργειας για την αποστολή τους). Δεύτερων, η κοινή χρήση του ασύρματου μέσου μετάδοσης από τους κόμβους έχει ως αποτέλεσμα την εμφάνιση συγκρούσεων ανάμεσα στα πακέτα, ακόμα και την καταστροφή τους. Αυτό αυξάνει την καθυστέρηση μετάδοσης ενός πακέτου στο εσωτερικού ενός δικτύου, ενώ πολλές φορές απαιτείται ακόμα και η επανεκλογή του αυξάνοντας έτσι την κατανάλωση ενέργειας. Τρίτων, τα δίκτυα αισθητήρων αποτελούνται συνήθως από φτηνούς κόμβους οι οποίοι χρησιμοποιούν κρυστάλλους χαμηλού κόστους για τις λειτουργίες του ρολογιού τους. Το μειονέκτημα αυτών των ρολογιών είναι η μεγαλύτερη ευπάθειά τους στη παρουσίαση αλμάτων (clock drifts) σε σχέση με τα παραδοσιακούς μηχανισμούς ρολογιών που χρησιμοποιούνται σε συσκευές με αρκετούς πόρους, όπως είναι οι φορητοί υπολογιστές και οι servers. Τέλος, διαφορετικές εφαρμογές παρουσιάζουν διαφορετικές απαιτήσεις σε ακρίβεια συγχρονισμού. Έτσι μερικές εφαρμογές απαιτούν απλά έναν χαλαρό συγχρονισμό, όπου αρκεί απλά η εύρεση της σειράς των γεγονότων. Από την άλλη, εφαρμογές, όπως αυτές εντοπισμού της θέσης διάφορων φαινομένων, απαιτούν συγχρονισμό μεγάλης ακρίβειας που μπορεί να φτάνει ακόμα και σε ακρίβεια μερικών milliseconds [139].

Υπάρχει πλήθος ερευνών που μελετούν την υλοποίηση πρωτοκόλλων συγχρονισμού ειδικά σχεδιασμένα για τα ασύρματα δίκτυα αισθητήρων (όπως είναι AD [141], TSS [142], TPSN [143], FTSP [138], VHT [144], ODS[151] κλπ). Στην μελέτη τους [145-146] οι ερευνητές παρουσιάζουν το πρωτόκολλο Reference Broadcast Synchronization

(RBS). Στο πρωτόκολλο αυτό ο κάθε κόμβος περιοδικά εκπέμπει ένα μήνυμα αναφοράς (beacon message) στους γείτονές του. Οι γειτονικοί κόμβοι χρησιμοποιούν τις στιγμές άφιξης των μηνυμάτων αναφοράς σαν σημεία αναφοράς ώστε να συγκρίνουν τα ρολόγια τους. Οι τοπικές αυτές χρονοσφραγίδες ανταλλάσσονται ανάμεσα στους γειτονικούς κόμβους ώστε να γίνει υπολογισμός της ολίσθησης των ρολογιών τους με σκοπό να τα συγχρονίσουν. Το πρωτόκολλο RBS επιτυγχάνει ακρίβεια της τάξης του 1 μsec. Ένα μειονέκτημα που παρουσιάζει η συγκεκριμένη προσέγγιση είναι ο φόρτος που προκαλείται εξαιτίας της συνεχόμενης ανταλλαγής μηνυμάτων ανάμεσα στους γειτονικούς κόμβους, ο οποίος αυξάνεται δραματικά στην περίπτωση πυκνών ασύρματων δικτύων [147].

Στην εργασία [138] προτείνουν το flooding time synchronization protocol (FTSP) πρωτόκολλο συγχρονισμού. Το FTSP επιτυγχάνει μεγάλη ακρίβεια συγχρονισμού χρησιμοποιώντας χρονοσφραγίδες στο MAC επίπεδο επικοινωνίας και γραμμικό αλγόριθμό παλινδρόμησης για την διόρθωση της ολίσθησης των ρολογιών των κόμβων. Κάθε κόμβος του δικτύου εκπέμπει ένα μήνυμα συγχρονισμού. Λόγω της κοινής φύσης της ασύρματης επικοινωνίας, παραλήπτες του μηνύματος θα είναι όλοι οι κόμβοι που βρίσκονται μέσα στην εμβέλεια εκπομπής του αποστολέα. Για το μήνυμα αυτό υπολογίζεται η χρονοσφραγίδα της αποστολής και της λήψης του στα MAC επίπεδα των αντίστοιχων κόμβων. Προτιμάται η λήψη των χρονοσφραγίδων στο MAC επίπεδο αποστολής του μηνύματος, καθώς με αυτό τον τρόπο εξαλείφεται μεγάλο μέρος των καθυστερήσεων στο εσωτερικό του κόμβου. Στην συνέχεια ο κάθε κόμβος χρησιμοποιεί τις χρονοσφραγίδες σε μια γραμμική συνάρτηση παλινδρόμησης με σκοπό να διορθώσει την ακρίβεια του ρολογιού του. Το πρωτόκολλο συγχρονισμού FTSP πετυχαίνει μεγάλη ακρίβεια και είναι εύκολα εφαρμόσιμο σε μεγάλο πλήθος κόμβων. Το κύριο μειονέκτημα του είναι η ανάγκη αποστολής μηνυμάτων συγχρονισμού από τους κόμβους σε πολύ συχνά διαστήματα κάτι το οποίο δημιουργεί μεγάλο φόρτο για τους κόμβους, απαιτεί την κατανάλωση ενέργειας και καταλαμβάνει μεγάλο μέρος του εύρους του δικτύου [152].

Παρόλη την ακρίβεια της τάξης των microsecond (μs) που πετυχαίνουν αρκετά πρωτόκολλά [144,148,138] , στην πλειοψηφία τους δεν είναι σχεδιασμένα να παρέχουν μια ιδανική ισορροπία ανάμεσα στην αποδοτική λειτουργία και στην εξοικονόμηση ενέργειας. Στην πράξη, κάθε πρωτόκολλο συγχρονισμού απευθύνεται σε συγκεκριμένο εύρος εφαρμογών. Για παράδειγμα, το σύστημα επιτήρησης μιας γέφυρας [149] απαιτεί ακρίβεια μερικών δεκάδων μs για την αποδοτική λήψη δεδομένων, ένα σύστημα ανίχνευσης παρεμβολών σε ένα δίκτυο [150] απαιτεί συγχρονισμό της τάξης μερικών milliseconds (ms) , ενώ ένα σύστημα επιτήρησης απαιτεί ακρίβεια συγχρονισμού 0.5 ~ 7 ms [33].

6.3.2.2 Χρονική ολίσθηση στους κόμβους Mica2

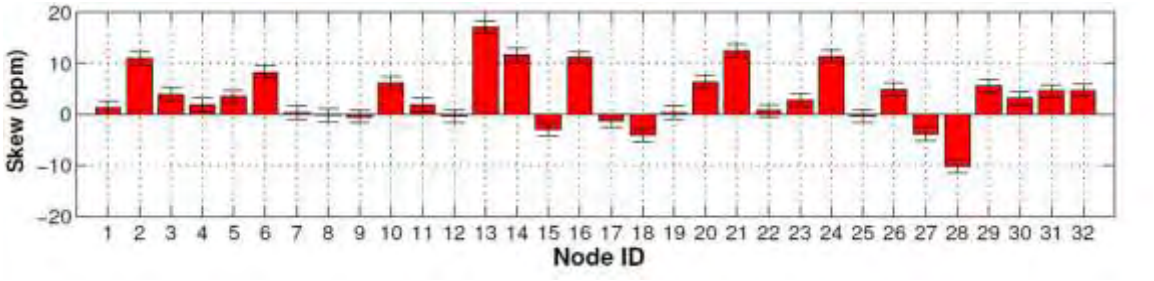
Οι ερευνητές στην μελέτη τους [151] κάνουν μια αναλυτική παρουσίαση της χρονικής ολίσθησης των ρολογιών που χρησιμοποιούνται από τους κόμβους των ασύρματων δικτύων αισθητήρων. Επιπλέον μέσω μιας πειραματικής διάταξης υπολογίζεται με ακρίβεια η χρονική ολίσθηση των ρολογιών των ασύρματων κόμβων Mica2 (πρόκειται για τους κύριους κόμβους που χρησιμοποιούνται στην συγκεκριμένη διατριβή).

Συγκεκριμένα, στην περίπτωση 2 ρολογιών έστω A & B, η συχνότητα ολίσθησης του A σε σχέση με το B μπορεί να υπολογισθεί από τον τύπο:

$$S_A^B = \frac{T_A - T_B}{T_B}$$

όπου το T_A είναι ο χρόνος που μέτρησε το ρολόι Α όταν το ρολόι Β μέτρησε τον αντίστοιχο χρόνο T_B. Η απόλυτη διαφορά των δύο αυτών τιμών | T_A - T_B | αποτελεί την ολίσθηση του Α σε σχέση με το Β. Στην περίπτωση όπου το Α ρολόι λειτουργεί ταχύτερα από ότι το Β, τότε θα ισχύει $T_A > T_B \Rightarrow S_A^B > 0$, διαφορετικά θα ισχύει $S_A^B < 0$. Η συχνότητα ολίσθηση εκφράζεται σε ppm (parts per million) και το σύνηθες εύρος τιμών της είναι από ±5 ppm έως ±100 ppm [35]. Έτσι, όταν η συχνότητα ολίσθησης του ρολογιού Α υπολογισθεί σε S_A^B = 20 ppm, συνεπάγεται ότι το ρολόι Α προηγείται 20μsec του ρολογιού Β για κάθε 1 sec.

Για την λεπτομερή μελέτη συμπεριφοράς του ρολογιού που διαθέτουν οι κόμβοι Mica χρησιμοποιήθηκε η ακόλουθη πειραματική διάταξη. Ένας κόμβος στέλνει περιοδικά ένα μήνυμα σε όλους τους κόμβους που βρίσκονται εντός της περιοχής εμβέλειας του. Οι κόμβοι-παραλήπτες των μηνυμάτων καταγράφουν την χρονική στιγμή άφιξης του κάθε μηνύματος. Κατά την διάρκεια του πειράματος εκτελέστηκαν 1000 εκπομπές μηνυμάτων και λήφθηκαν 25809 μηνύματα από 32 κόμβους-παραλήπτες. Η παρακάτω Εικόνα παρουσιάζει την χρονική ολίσθηση των κόμβων-παραληπτών σε σχέση με τον κόμβο-αποστολέα των μηνυμάτων. Όπως φαίνεται από το γράφημα η μέγιστη χρονική ενός κόμβου-παραλήπτη σε σχέση με τον κόμβο-αποστολέα είναι λίγο λιγότερο από 20 μs (20 ppm). Οπότε η μέγιστη χρονική ολίσθηση που μπορεί να έχουν δύο κόμβοι μεταξύ του σε διάστημα 1 δευτερολέπτου είναι ±40 μs (40 ppm). Η τιμή αυτής της μέγιστης χρονικής ολίσθησης ανάμεσα σε δύο κόμβους Mica2 αποτελεί σημαντική παράμετρος στην ανάπτυξη του πρωτόκολλου συγχρονισμού που ακολουθεί.



Εικόνα 50: Η χρονική ολίσθηση 35 κόμβων Mica2 σε σχέση με έναν κόμβο αναφορά [151].

6.3.2.3 Το πρωτόκολλο συγχρονισμού

Η χρήση των πρωτοκόλλων συγχρονισμού που περιγράφηκαν παραπάνω δεν αποτελούν αποδοτική λύση στην περίπτωση των μεθόδων επιτήρησης χώρου που μελετάμε. Τα υφιστάμενα πρωτόκολλα είναι πρωτόκολλα γενικού σκοπού. Στοχεύουν, δηλαδή, στην ευκολία χρησιμοποίησης τους από διαφορετικά είδη εφαρμογών επιτυγχάνοντας συγχρονισμό ανάμεσα στους ασύρματους κόμβους. Αυτή η γενικότητα όμως, έχει σαν αποτέλεσμα τα πρωτόκολλα αυτά αν μην είναι βέλτιστα από άποψη

κατανάλωσης πόρων (κατανάλωση ενέργεια, χρήση του ασύρματου πομποδέκτη, επεξεργαστική ισχύ, απαίτησης σε μνήμη) για τους κόμβους και για το δίκτυο συνολικά.

Παρακάτω προτείνεται ένα πρωτόκολλο συγχρονισμού το οποίο αναπτύχτηκε λαμβάνοντας υπόψη τις ιδιαιτερότητες και τις απαιτήσεις των μεθόδων εντοπισμού και χαρακτηρισμού απειλής που περιγράφουμε στην υφιστάμενη διατριβή. Πρόκειται για έναν μηχανισμό ο οποίος δανείζεται στοιχεία από δύο πολύ γνωστά πρωτόκολλα, το FTSP και το RBS, και στοχεύει στην ελαχιστοποίηση της κατανάλωσης ενέργειας των κόμβων προσφέροντας συγχρονισμό ακρίβειας της τάξης μερικών milliseconds ανάμεσα τους.

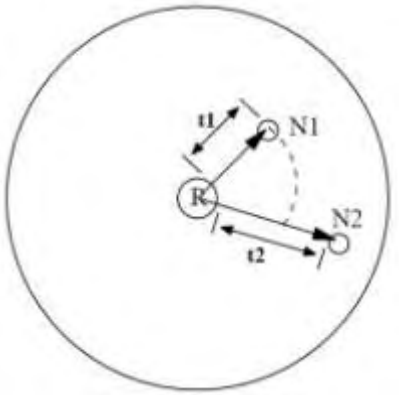
Στην πλειοψηφία τους τα πρωτόκολλα συγχρονισμού υπολογίζουν την χρονική ολίσθηση του ρολογιού του κάθε κόμβου και χρησιμοποιώντας κατάλληλες μεθόδους (αλλαγή της τιμής του ρολογιού ή reset του ρολογιού) επεμβαίνουν σε αυτά ώστε να κάνουν τις απαραίτητες χρονικές διορθώσεις. Το μειονέκτημα χρήσης αυτών των διορθωτικών διαδικασιών είναι ότι απαιτούν κατανάλωση πόρων για την εκτέλεση τους. Επίσης συνήθως είναι αρκετά εξειδικευμένες για συγκεκριμένους τύπους ρολογιών (π.χ. ένας τύπος ρολογιού δέχεται μόνο το reset ενώ άλλος τύπος ρολογιού προσφέρει την δυνατότητα ορισμού της τιμής του). Το πρωτόκολλο που περιγράφεται προκειμένου να αποφύγει την χρήση αυτών των μεθόδων μεταφέρει τον συγχρονισμό από το επίπεδο του κόμβου στο επίπεδο ενός κόμβου αναφοράς. Στην περίπτωσή μας τον ρόλο του κόμβου αναφοράς αναλαμβάνει ο σταθμός βάσης του δικτύου.

Συγκεκριμένα, ο σταθμός βάσης περιοδικά εκπέμπει ένα μήνυμα συγχρονισμού σε όλους τους κόμβους. Ο κάθε κόμβος που δέχεται το μήνυμα καταγράφει την στιγμή άφιξης του. Στην συνέχεια ο κάθε κόμβος στέλνει στον σταθμό βάσης ένα μήνυμα που περιέχει την καταγεγραμμένη χρονοσφραγίδα του ειδικού μηνύματος συγχρονισμού. Ο σταθμός βάσης συλλέγει και αποθηκεύει τις χρονοσφραγίδες από όλους τους κόμβους σε έναν πίνακα. Με την λήψη κάθε νέας χρονοσφραγίδας από κάθε κόμβο ο σταθμός βάσης ανανεώνει την αντίστοιχη θέση του στον πίνακα. Έτσι ο πίνακας αυτός περιέχει το χρόνο T_i του κάθε κόμβου i που αντιστοιχεί στον χρόνο T_0 του σταθμού βάσης. Με αυτόν τον τρόπο, ο κόμβοι μεταξύ τους μένουν ασυγχρόνιστοι, αλλά ο σταθμός βάσης γνωρίζει κάθε στιγμή την χρονική ολίσθηση του ρολογιού του κάθε κόμβου και κάνει τις απαραίτητες διορθώσεις μόνο στο επίπεδο εφαρμογών που εκτελεί.

Για την σωστή λειτουργία του παραπάνω μηχανισμού θεωρούμε ότι:

1. **Ο σταθμός βάσης έχει περισσότερους πόρους σε σχέση με τους ασύρματους κόμβους.** Συγκεκριμένα θεωρούμε ότι διαθέτει συνεχή παροχή ρεύματος, υψηλή επεξεργαστική ισχύ και αρκετή μνήμη.
2. **Η εμβέλεια του σταθμού βάσης είναι αρκετά μεγαλύτερη από αυτή των κόμβων.** Με αυτό τον τρόπο ο σταθμός βάσης μπορεί να επικοινωνεί άμεσα με όλους τους κόμβους (single hop επικοινωνία).
3. **Ο χρόνος μετάδοσης του μηνύματος από τον σταθμό βάσης στους διαφορετικούς κόμβους του δικτύου είναι ίδιος.** Όπως φαίνεται και στην Εικόνα 51, σταθμός βάσης εκπέμπει ένα μήνυμα στου κόμβους N1 και N2 που βρίσκονται εντός της εμβέλειας εκπομπής του. Ο χρόνος που απαιτείται για την διάδοση του μηνύματος στους κόμβους N1 και N2 είναι t1 και t2 αντίστοιχα. Στην πραγματικότητα οι χρόνοι αυτοί διαφέρουν. Όμως λαμβάνοντας υπόψη ότι η απόσταση ανάμεσα στους κόμβους κυμαίνεται από μερικά μέτρα έως μερικές δεκάδες μέτρα και ότι η ταχύτητα διάδοσης ενός

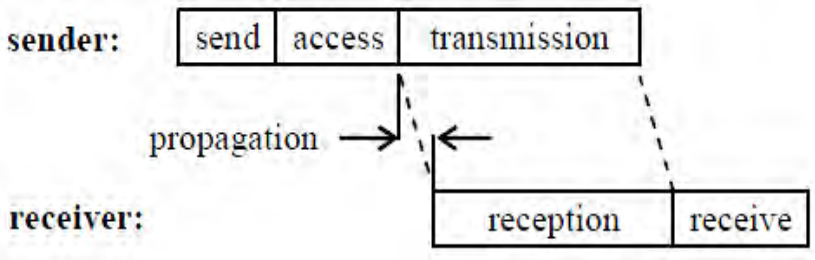
ηλεκτρομαγνητικού σήματος στον αέρα είναι αρκετά κοντά με την ταχύτητα διάδοσης του φωτός, η διαφορά που δημιουργείται ανάμεσα στους χρόνους διάδοσης t1 και t2 είναι της τάξης μερικών nanoseconds, η οποία θεωρείται αμελητέα σε σχέση με της απαιτήσεις των μεθόδων [138, 151].



Εικόνα 51: Η διαφορά διάδοσης ενός μηνύματος στην εμβέλεια του σταθμού βάσης.

Σημαντικό παράγοντα λάθους στον υπολογισμό της χρονικής ολίσθησης του κάθε κόμβου αποτελεί ο χρόνος που μεσολαβεί μεταξύ αποστολής του μηνύματος συγχρονισμού από τον σταθμό βάσης και της λήψης του μηνύματος από τους κόμβους. Ο χρόνος αυτός μπορεί να χωριστεί σε επιμέρους χρονικά διαστήματα [138, 143, 153]. Τα επιμέρους αυτά χρονικά διαστήματα είναι:

- *Ο χρόνος αποστολής (send time),* αντιστοιχεί στον χρόνο δημιουργίας του μηνύματος πριν το επίπεδο MAC στην πλευρά του αποστολέα. Η διάρκεια του δεν είναι ντετερμινιστική καθώς εξαρτάται σε μεγάλο βαθμό από τον φόρτο του συστήματος. Είναι της τάξης μερικών εκατοντάδων milliseconds.
- *Ο χρόνος πρόσβασης (access time),* αντιστοιχεί στον χρόνο που απαιτείται ώστε να βρεθεί ελεύθερο για αποστολή το ασύρματος κανάλι. Η διάρκειά του εξαρτάται σε μεγάλο βαθμό από τον φόρτο του δικτύου και κυμαίνεται από μερικά milliseconds μέχρι και μερικά seconds.
- *Ο χρόνος μετάδοσης (transmission time),* περιλαμβάνει τον χρόνο που απαιτεί το σύστημα να μεταδώσει το μήνυμα. Εξαρτάται σε μεγάλο βαθμό από τον από την ταχύτητα του πομποδέκτη και το μέγεθος του μηνύματος. Είναι της τάξης μερικών milliseconds.
- *Ο χρόνος διάδοσης (propagation time),* όπως περιγράφτηκε και παραπάνω ο χρόνος διάδοσης του μηνύματος είναι της τάξης των μερικών nanoseconds , οπότε και δεν λαμβάνεται υπόψη.
- *Ο χρόνος υποδοχής (reception time),* πρόκειται για τον χρόνο λήψης του μηνύματος από τον παραλήπτη. Είναι το αντίστοιχο χρονικό διάστημα του χρόνου μετάδοσης στον αποστολέα
- *Ο χρόνος λήψης (receive time),* πρόκειται για τον χρόνο που χρειάζεται το ληφθέν μήνυμα να μεταφερθεί από τον πομποδέκτη του παραλήπτη στην εφαρμογή του. Είναι το αντίστοιχο χρονικό διάστημα του χρόνου αποστολής στον αποστολέα.



Εικόνα 52: Τα χρονικά διαστήματα που απαιτούνται για την αποστολή ενός μηνύματος.

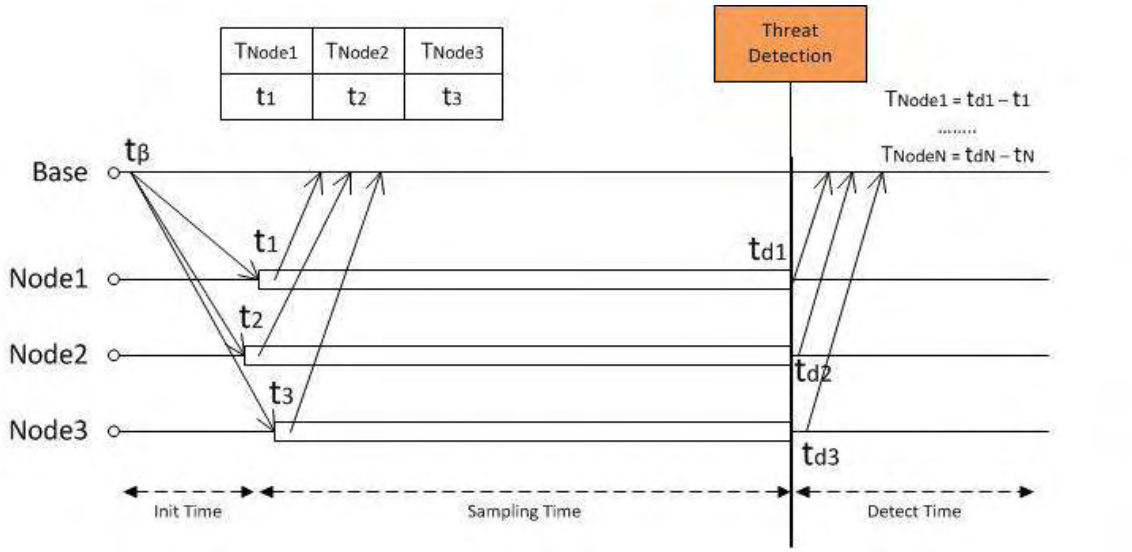
Όπως είναι φανερό τα χρονικά διαστήματα που βρίσκονται στα «άκρα» της διαδικασίας αποστολής (διάστημα αποστολής, μετάδοσης, λήψης) ενός μηνύματος παρουσιάζουν μεγάλη αβεβαιότητα όσον αφορά την διάρκειά τους. Αυτό αναγκάζει τον μηχανισμό να λαμβάνει τις χρονοσφραγίδες αποστολής και λήψης του μηνύματος σε όσο το δυνατόν χαμηλότερο επίπεδο. Η βελτίωση της χρονικής ασάφειας επιτυγχάνεται με την λήψη των χρονοσφραγίδων στο επίπεδο MAC. Με αυτόν τον τρόπο, η χρονική καθυστέρηση των χρονοσφραγίδων του μηνύματος εξαρτάται αποκλειστικά από τους χρόνους μετάδοσης, διάδοσης και υποδοχής του μηνύματος. Ο χρόνος διάδοσης είναι αμελητέος οπότε και δεν υπολογίζεται. Όσον αφορά τους χρόνους μετάδοσης και υποδοχής, εξαρτώνται σε μεγάλο βαθμό από το μέγεθος του μηνύματος, δεδομένου όμως ότι τα μηνύματα συγχρονισμού που ανταλλάσσονται έχουν πολύ μικρό μέγεθος (μερικά byte), θεωρούμε ότι αυτοί οι χρόνοι είναι αρκετά μικροί.

Στην Εικόνα 53 φαίνεται η διαδικασία συγχρονισμού των ασύρματων κόμβων. Παρατηρώντας την εικόνα εύκολα γίνεται αντιληπτό ότι ο μηχανισμός συγχρονισμού είναι ενσωματωμένος μέσα στην μέθοδο ανίχνευσης των κόμβων. Αυτή η στενή ενσωμάτωση των δύο ανεξάρτητων μηχανισμών βελτιώνει την αποτελεσματικότητα τους ενώ επιτρέπει στους κόμβους να κάνουν μια καλύτερη διαχείριση των πόρων τους, βελτιώνοντας έτσι την διάρκεια ζωής τους.

Πιο αναλυτικά, βλέπουμε ότι η διάρκεια λειτουργίας των κόμβων χωρίζεται σε 3 διακριτές περιόδους οι οποίες εναλλάσσονται περιοδικά. Οι τρείς αυτές περίοδοι είναι:

- **Η περίοδος αρχικοποίησης (init time):** κατά την διάρκεια της οποίας οι κόμβοι ανταλλάσουν μηνύματα μεταξύ τους ώστε να γίνουν οι απαραίτητες αρχικοποιήσεις. Οι κόμβοι έχουν ενεργοποιημένους του πομποδέκτες τους και λειτουργούν σε πλήρη ισχύ, έχοντας απενεργοποιημένα όμως τα αισθητήρια όργανά τους.
- **Η περίοδος δειγματοληψίας (sampling time):** κατά την διάρκεια αυτής της περιόδου οι κόμβοι καταγράφουν και επεξεργάζονται τα ακουστικά κύματα που φτάνουν στα αισθητήρια όργανά τους. Οι κόμβοι βρίσκονται σε πλήρη ισχύ, με ενεργοποιημένα τα αισθητήρια όργανα αλλά με απενεργοποιημένους τους πομποδέκτες τους.
- **Η περίοδος ανίχνευσής (detect time):** Οι κόμβοι βρίσκονται στην συγκεκριμένη περίοδο όταν ανιχνεύσουν κάποια απειλή. Ουσιαστικά πρόκειται για την περίοδο όπου οι κόμβοι αποστέλλουν της πληροφορίες που κατέγραψαν στον σταθμό βάσης για την περεταίρω επεξεργασίας τους και ακριβής ανίχνευση της απειλής. Κατά την διάρκεια αυτής της περιόδου, οι

κόμβοι βρίσκονται σε πλήρη ισχύ έχοντας ενεργοποιημένους τους πομποδέκτες τους και απενεργοποιημένα τα αισθητήρια όργανά τους.



Εικόνα 53: Μηχανισμός συγχρονισμού των κόμβων στην περίπτωση εντοπισμού μιας απειλής.

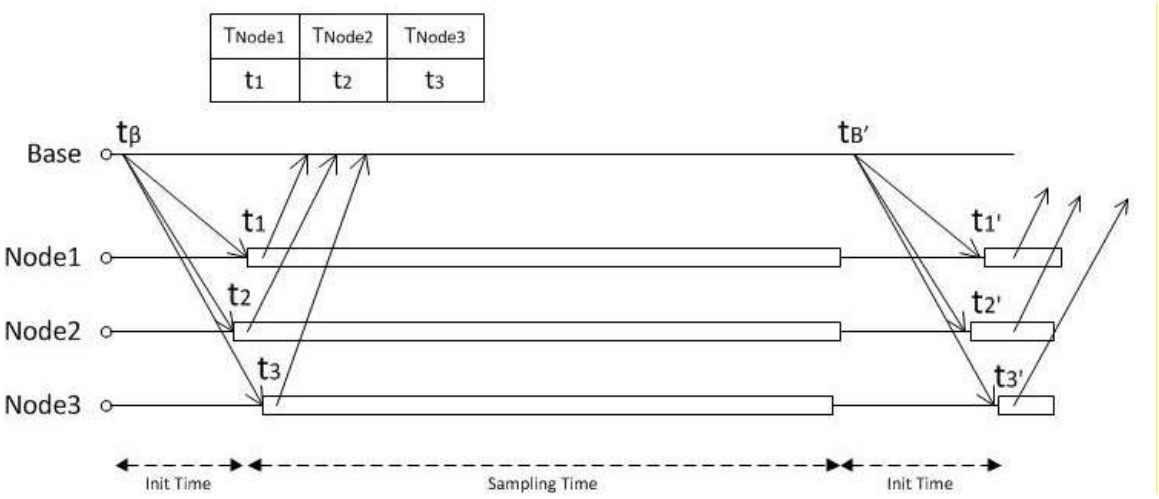
Οι κόμβοι αρχικά βρίσκονται στο στάδιο της αρχικοποίησης. Ο σταθμός βάσης στέλνει στους κόμβους ένα ειδικό μήνυμα συγχρονισμού. Έτσι t_β ο χρόνος αποστολής του μηνύματος από τον σταθμός βάσης και t_1,t_2,t_3 οι χρόνοι λήψης του μηνύματος από τους αντίστοιχος κόμβους (θεωρούμε ότι η χρονική διαφορά άφιξης του μηνύματος συγχρονισμού από τον σταθμό βάσης στους κόμβους είναι πολύ μικρή). Όταν κάποιος κόμβος λάβει το μήνυμα συγχρονισμού, καταγράφει την χρονοσφραγίδα λήψης του και την αποστέλλει πίσω στον σταθμό βάσης. Ο σταθμός βάσης λαμβάνει από όλους του κόμβους τις χρονοσφραγίδες λήψης του ειδικού μηνύματος. Οι χρονοσφραγίδες αυτές αποθηκεύονται σε έναν πίνακα, τον **πίνακα συγχρονισμού.**

Αφού οι κόμβοι στείλουν στον σταθμό βάσης το μήνυμα με την χρονοσφραγίδα λήψης μεταβαίνουν στο στάδιο δειγματοληψίας, όπου και γίνεται καταγραφή των ακουστικών κυμάτων. Όταν κάποιος κόμβος εντοπίσει κάποια πιθανή απειλή (ισχυρό ακουστικό κύμα το οποίο έχει ένταση μεγαλύτερη της έντασης του κατωφλίου) γίνεται υπολογισμού της στιγμής άφιξης του (χρήση ενός χαρακτηριστικού σημείου του κύματος, Κεφάλαιο 6.3.1.2). Ο κόμβος μεταβαίνει στο στάδιο ανίχνευσης, ενεργοποιεί τον πομποδέκτη τους και στέλνει στον σταθμό βάσης ένα μήνυμα με τα χαρακτηριστικά του κύματος, όπως ο χρόνος άφιξης του. Έστω οι χρόνοι άφιξης t_{d1}, t_{d2}, t_{d3} του κύματος στους αντίστοιχους κόμβους.

Ο σταθμός βάσης συλλέγει τους χρόνους άφιξης του κύματος σε όλους του κόμβους. Οι χρόνοι αυτοί προέρχονται από κόμβους οι οποίοι είναι ασυγχρόνιστοι μεταξύ τους, οπότε και οι χρόνοι αυτοί θα παρουσιάζουν σημαντικές διαφορές. Ο σταθμός βάσης προκειμένου να διορθώσει αυτές τις χρονικές ολισθήσεις χρησιμοποιεί τις χρονοσφραγίδες που περιέχονται μέσα στους πίνακα συγχρονισμού του. Έτσι ο χρόνος για τον κόμβο 1 (αντίστοιχα ισχύει και για τους υπόλοιπους κόμβους) υπολογίζεται ως:

$T_{node1} = t_{d1} - t_1$

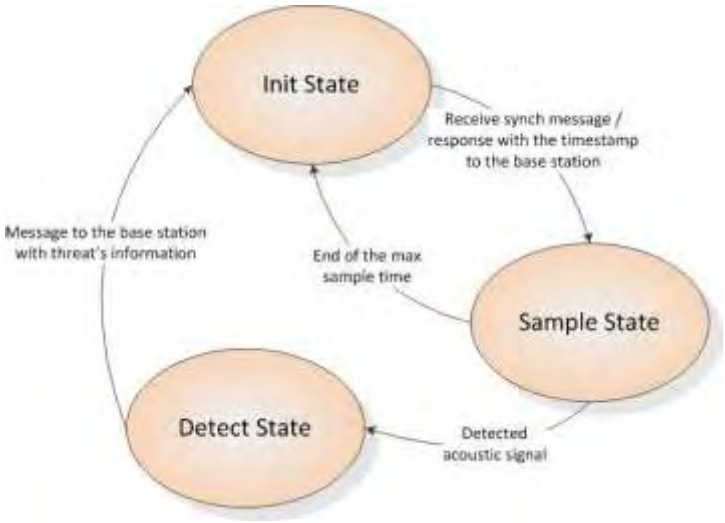
Με αυτό τον τρόπο ο σταθμός βάσης υπολογίζει τον σχετικό χρόνο που πέρασε από την στιγμή αρχικοποίησης των κόμβων μέχρι την στιγμή καταγραφής του ακουστικού κύματος. Η ακρίβεια υπολογισμού του χρόνου είναι ικανοποιητική και αποφεύγει τις όποιες χρονικές ολισθήσεις παρουσιάσουν τα ρολόγια των κόμβων κατά την διάρκεια της περιόδου δειγματοληψίας. Στην πραγματικότητα ο μηχανισμός εκμεταλλεύεται το γεγονός ότι τα ρολόγια για μικρό χρονικό διάστημα παρουσιάζουν μικρή χρονική ολίσθηση (π.χ. οι κόμβοι Mica2 παρουσιάζουν ±40 μs σε διάστημα 1 δευτερολέπτου). Έτσι στην περίπτωση όπου η χρονική διάρκεια του σταδίου δειγματοληψίας είναι μικρή, ο μηχανισμός παρουσιάζει πολύ καλή ακρίβεια υπολογισμού του χρόνου άφιξης του κύματος. Σε αντίθετη περίπτωση, όσο η χρονική διάρκεια του σταδίου μεγαλώνει, τόσο μεγαλώνουν οι χρονικές αποκλίσεις των ρολογιών των κόμβων (που συμβαίνουν κατά την διάρκεια αυτού του διαστήματος) οπότε και η ακρίβεια του μηχανισμού μειώνεται.



Εικόνα 54: Μηχανισμός συγχρονισμού των κόμβων στην περίπτωση μη-εμφάνισης κάποιας απειλής

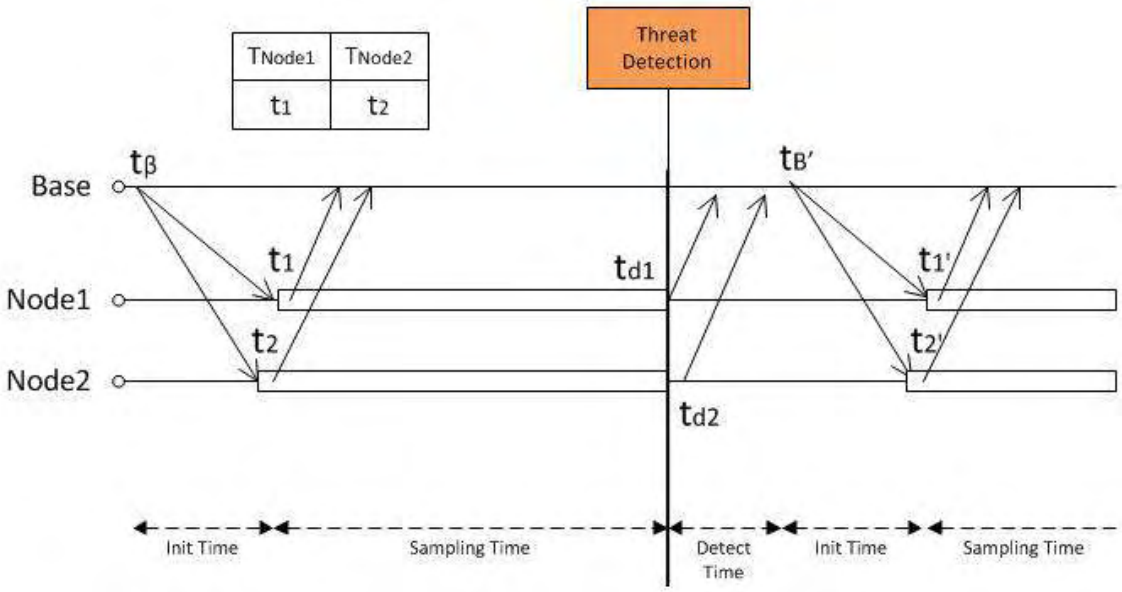
Μια βελτίωση όπου θα μπορούσε να λύσει το πρόβλημα της αργοπορημένης ή και μη εμφάνισης ενός ακουστικού κύματος απειλής φαίνεται στην Εικονα 54. Αυτό που προτείνεται είναι το στάδιο δειγματοληψίας των κόμβων να έχει κάποια μέγιστη χρονική διάρκεια Τ. Ο κόμβος δηλαδή μετά το στάδιο της αρχικοποίησης του θα βρίσκεται στο στάδιο της δειγματοληψίας μέχρι είτε να περάσει ο χρόνος Τ, είτε να εντοπιστεί κάποια απειλή. Έπειτα ανάλογα με την περίπτωση, ο κόμβος μεταβαίνει είτε στο στάδιο αρχικοποίησης είτε στο στάδιο ανίχνευσης.

Στην περίπτωση της μεθόδου ανίχνευση απειλών μέσω της καταγραφής ακουστικών κυμάτων, ο μέγιστος χρόνο Τ του σταδίου δειγματοληψίας θα μπορούσε να οριστεί ίσο με 15 λεπτά. Έτσι για τους κόμβους Mica2 και για Τ =15 min. έχουμε μέγιστη δυνατή ολίσθηση ±3,6 ns ανά κόμβο, οπότε και 7,1 ns μέγιστη χρονική ολίσθηση ανάμεσα στους κόμβους.



Εικόνα 55: Οι καταστάσεις λειτουργίας που μεταβαίνουν οι κόμβοι.

Τέλος, παρακάτω περιγράφεται μια επιπλέον βελτίωση η οποία θα μπορούσε να αυξήσει σε μεγάλο βαθμό την ακρίβεια του υπολογισμού της χρονικής άφιξης ενός ακουστικού κύματος. Βασίζεται και πάλι στο γεγονός ότι τα ρολόγια για μικρό χρονικό διάστημα παρουσιάζουν μικρή χρονική ολίσθηση.



Εικόνα 56: Βελτίωση μηχανισμού συγχρονισμού των κόμβων.

Έστω, ότι οι κόμβοι βρίσκονται στο στάδιο αρχικοποίησης και ο σταθμός βάσης στέλνει το μήνυμα συγχρονισμού. Ο χρόνος αποστολής του μηνύματος ορίζεται ως t_β και οι χρονοσφραγίδες λήψης του μηνύματος από τους κόμβους 1 και 2 ως t_1 και t_2 αντίστοιχα. Οι κόμβοι συνεχίζουν στο στάδιο δειγματοληψίας και την στιγμή t_{d1} και t_{d2} ,αντίστοιχα, ανιχνεύουν μια απειλή και στέλνουν τα μηνύματα στον σταθμό βάσης.

Στο στάδιο αυτό δεν γίνεται υπολογισμός και διόρθωση των t_{d1} και t_{d2} (όπως περιγράφτηκε παραπάνω), αλλά συνεχίζει η διαδικασία μεταβαίνοντας οι κόμβοι ξανά στο στάδιο αρχικοποίησης. Στο νέο στάδιο αρχικοποίησης λαμβάνονται οι χρονικές τιμές $t_{\beta'}$, $t_{1'}$ και $t_{2'}$. Στην συνέχεια γίνεται υπολογισμός του χρόνου που έχει περάσει ανάμεσα στα δύο διαδοχικά στάδια αρχικοποίησης κάθε κόμβου και υπολογίζουμε την χρονική ολίσθηση των κόμβων σε σχέση με το ρολόι του σταθμού βάσης.

$$T_\beta = t_{\beta'} - t_\beta$$

$$T_1 = t_{1'} - t_1$$

$$T_N = t_{N'} - t_N$$

όπου T_N ο χρόνος ανάμεσα σε 2 διαδοχικά στάδια αρχικοποίησης για τον κόμβο N.

$$\Delta T_1 = T_1 - T_\beta$$

$$\Delta T_N = T_N - T_\beta$$

Όπου ΔT_N , η διαφορά του χρόνου για δύο διαδοχικά στάδια αρχικοποίησης ανάμεσα στον κόμβο N και στον σταθμό βάσης. Ουσιαστικά η τιμή ΔT_N δίνει την χρονική ολίσθηση του κόμβου N σε σχέση με τον σταθμό βάσης.
Έτσι ο χρόνος άφιξης του κύματος στους κόμβους μπορεί να υπολογισθεί από τις παρακάτω σχέσεις:

$$T_1 = t_{d1} - t_1 - \Delta T_1$$

$$T_N = t_{dN} - t_N - \Delta T_N$$

Το στάδιο δειγματοληψίας είναι το μεγαλύτερο σε διάρκεια από τα τρία στάδια, οπότε είναι ασφαλές να θεωρηθεί ότι το μεγαλύτερο ποσοστό της χρονικής ολίσθησης ΔT_N του κόμβου N προκλήθηκε στο στάδιο δειγματοληψίας και όχι στο στάδιο της ανίχνευσης (το οποίο δεν λαμβάνεται υπόψη στον παραπάνω τύπο.)

6.3.3 Υπολογισμός κατωφλίου

Ουσιώδες στοιχείο της μεθόδου ανίχνευσης απειλής αποτελεί η χρήση ενός χαρακτηριστικού κατωφλίου. Το χαρακτηριστικό αυτό κατώφλι λειτουργεί σαν μέτρο σύγκρισης της έντασης των ηχητικών κυμάτων που καταγράφονται από τους ακουστικούς αισθητήρες. Η υπέρβαση της έντασης ενός ακουστικού κύματος από το κατώφλι αντιστοιχεί στην ύπαρξη κάποιας απειλής στην περιοχή και σηματοδοτεί την εκτέλεση κατάλληλων, για τον εντοπισμό του, ενεργειών.

Όπως είναι φανερό, ο προσδιορισμός του κατωφλίου επιδρά σημαντικά στην απόδοση της μεθόδου ανίχνευσης. Έτσι ο ορισμός του ύψος του κατωφλίου σε μια υψηλή στάθμης έντασης έχει ως αποτέλεσμα τον εντοπισμό μικρού πλήθους απειλών, καθώς θα εντοπίζονται μόνο οι απειλές που προκαλούν ηχητικά κύματα μεγάλης

έντασης. Αντίθετα, ο ορισμός του κατωφλίου σε στάθμη χαμηλής έντασης έχει ως αποτέλεσμα την ύπαρξη πολλών λανθασμένων ανιχνεύσεων. Αυτό το γεγονός δημιουργεί το πρόβλημα εμφάνισης μεγάλου πλήθους λανθασμένων ανιχνεύσεων. Το μεγάλο ποσοστό των λανθασμένων ανιχνεύσεων οφείλεται στη χαμηλότερη ένταση του κατωφλίου από την ένταση του θορύβου του περιβάλλοντος, όπου εφαρμόζεται η μέθοδος (π.χ. ο ήχος που προκαλεί ο άνεμος της περιοχής). Αυτό προκαλεί την λανθασμένη ανίχνευση των συνθηκών του περιβάλλοντος ως απειλές.

Η λύση σε αυτό το πρόβλημα είναι η χρήση ενός μεταβλητού κατωφλίου το οποίο θα προσαρμόζεται στις συνθήκες που επικρατούν κάθε στιγμή στον χώρο εφαρμογής της μεθόδου. Για τον δυναμικό προσδιορισμό του κατωφλιού αναπτύχθηκε ένας αλγόριθμος ο οποίος λαμβάνει υπόψη τις ιδιαιτερότητες των κόμβων. Πρόκειται για έναν απλό αλγόριθμο, που περιοδικά καταγράφει τον ένταση του θορύβου και την ταχύτητα του ανέμου προκειμένου να υπολογίσει την στάθμη του κατωφλίου.

Αναλυτικά η μέθοδος:

1. Δέχεται ένα μήνυμα από τον σταθμό βάσης. Το μήνυμα αυτό περιέχει το επίπεδο θορύβου όπως αυτό προσδιορίζεται από την ταχύτητα του ανέμου.
2. Καταγράφει για κάποιο σύντομο διάστημα τα ακουστικά κύματα.
3. Χρησιμοποιεί τα καταγεγραμμένα ακουστικά κύματα προκειμένου να εντοπίσει την μέγιστη τιμή έντασης του κύματος. Αυτή αντιστοιχεί στην μέγιστη καταγεγραμμένη τιμή θορύβου του περιβάλλοντος για το συγκεκριμένο χρονικό διάστημα.
4. Συγκρίνει το επίπεδο θορύβου που προσδιορίστηκε από την ταχύτητα του ανέμου και το επίπεδο θορύβου που προσδιορίστηκε από την καταγραφή των ακουστικών κυμάτων.
5. Επιλέγεται το υψηλότερο, από τα δύο, επίπεδο θορύβου. Σε αυτό προστίθεται μια σταθερά ίση με το 50% της έντασης αυτού του επιπέδου.
6. Το αποτέλεσμα που προκύπτει αποτελεί το κατώφλι διαχωρισμού των ακουστικών κυμάτων ανάμεσα σε κύματα θορύβου και κύματα απειλών.

Στο βήμα 2 περιγράφεται η εκτέλεση ενός σύντομου διαστήματος καταγραφής των ακουστικών κυμάτων. Η διάρκεια αυτού του διαστήματος πρέπει να είναι αρκετά μεγάλο ώστε να γίνει καταγραφή ενός σημαντικού πλήθους δειγμάτων. Από την άλλη, η μεγάλη διάρκεια καταγραφής αυξάνει αρκετά την πιθανότητα καταγραφής κάποιας απειλής. Το γεγονός αυτό θα έχει ως αποτέλεσμα την αύξηση της στάθμης κατωφλίου, άρα και την μείωση της ικανότητας ανίχνευσης των απειλών.

Το χρονικό διάρκεια που επιλέγεται για την καταγραφή των ακουστικών κυμάτων προκειμένου να υπολογισθεί η στάθμη του κατωφλίου είναι ίσο με 15 sec. Η χρονική αυτή διάρκεια κρίνεται ικανοποιητική καθώς αντιστοιχεί μόλις στο ~1.5% του χρόνου ανίχνευσης απειλών από το σύστημα για κάθε γύρο εκτέλεσης της μεθόδου, ελαχιστοποιώντας έτσι την πιθανότητας θεώρησης του ήχου μίας απειλής ως θόρυβο του περιβάλλοντος.

6.3.4 Καταγραφή των περιβαλλοντικών συνθηκών και υπολογισμού της ταχύτητας διάδοσης του ακουστικού κύματος.

Η διάδοση του ακουστικού κύματος στον χώρο εξαρτάται σε μεγάλο βαθμό από τις συνθήκες που επικρατούν στον συγκεκριμένο χώρο. Πιο αναλυτικά, όπως περιγράφεται στο Κεφάλαιο 2, η ταχύτητα διάδοσης του ακουστικού κύματος εξαρτάται από την

θερμοκρασία, την υγρασία και την ατμοσφαιρική πίεση που επικρατούν στον χώρο όπου διαδίδεται το κύμα. Ακόμα η ταχύτητα του ανέμου επηρεάζει σε μεγάλο βαθμό τον θόρυβο που επικρατεί στην συγκεκριμένη περιοχή. Οπότε η καταγραφή της κρίνεται αναγκαία. Για την μέτρηση των συγκεκριμένων περιβαλλοντικών συνθηκών χρησιμοποιήθηκε ένα δίκτυο αισθητήρων αποτελούμενο από ασύρματους κόμβους iSense.

Το ασύρματο δίκτυο αισθητήρων που χρησιμοποιήθηκε αποτελείται από 2 τύπους κόμβων:

- τον κόμβο καταγραφής
- τον σταθμό συλλογής.

Το ασύρματο δίκτυο περιλαμβάνει ένα πλήθος κόμβων καταγραφής. Πρόκειται για του ασύρματους κόμβους iSense Core Module, στους οποίους έχει ενσωματωθεί η πλακέτα επέκτασης για την μέτρηση των περιβαλλοντικών συνθηκών (iSense Weather Module). Το μέγεθος των δύο επιμέρους πλακετών που απαρτίζουν το σύστημα είναι αρκετά μικρό καθιστώντας έτσι το συνολικό μέγεθος του κόμβου καταγραφής να είναι μικρό και ικανό να τοποθετηθεί τόσο σε φορητά (τοποθετημένα πάνω στην στολή των στρατιωτών/φυλάκων) όσο και σε σταθερά συστήματα επιτήρησης (σε σταθερά σημεία/κεραίες επιτήρησης). Επιπλέον στο δίκτυο καταγραφή περιβαλλοντικών συνθηκών λειτουργούν και μερικοί κόμβοι iSense (1 αρκεί), οι οποίοι έχουν ενσωματωμένο ένα αισθητήρα καταγραφής των ιδιοτήτων ανέμου (ανεμόμετρο). Οι κόμβοι καταγραφής περιοδικά καταγράφουν τις περιβαλλοντικές συνθήκες του περιβάλλοντα χώρου και τις αποστέλλουν στον σταθμό βάσης. Οι συνθήκες που καταγράφουν είναι: η θερμοκρασία του περιβάλλοντος, η σχετική υγρασία και η ατμοσφαιρική πίεση και η ταχύτητα του ανέμου. Η συχνότητα αλλαγής των συγκεκριμένων μεταβλητών στο περιβάλλον είναι σχετικά αργή, οπότε η καταγραφή τους σε συχνότητα της τάξης των 10 λεπτών είναι ικανοποιητική.

Το δίκτυο περιλαμβάνει μόνο ένα σταθμό συλλογής ο οποίος βρίσκεται στο σταθμό βάσης του υπόλοιπου συστήματος. Αναλαμβάνει να συλλέξει τα περιβαλλοντικά δεδομένα από τους κόμβους καταγραφής του δικτύου. Τα δεδομένα αυτά αποθηκεύονται σε μία βάση δεδομένων ώστε να είναι εύκολα προσβάσιμα από τον σταθμό βάσης του συστήματος. Τα δεδομένα αυτά είναι απαραίτητα στους υπολογισμούς που διενεργούνται από τον σταθμό βάσης του συστήματος προκειμένου να υπολογίσει την θέση της απειλής

Στην ιδανική περίπτωση, ο κόμβος καταγραφής των περιβαλλοντικών συνθηκών θα ήταν ενσωματωμένος με τον κόμβο καταγραφής των ακουστικών κυμάτων του συστήματος. Παρόλα αυτά, στα πλαίσια της συγκεκριμένης διατριβής περιγράφεται κυρίως η λειτουργία και αποτελεσματικότητα των μεθόδων εντοπισμού και χαρακτηρισμού απειλών σε έναν χώρο. Έτσι η χρήση ενός ξεχωριστού δικτύου αισθητήρων για την καταγραφή των περιβαλλοντικών συνθηκών δεν χαλάει την αποτελεσματικότητα και γενικότητα των μεθόδων.

6.3.5 Τη καταγραφή της θέσης των κόμβων.

Στην προηγούμενη παράγραφο, περιγράφτηκε ένα ασύρματο δίκτυο αισθητήρων το οποίο λειτουργεί ανεξάρτητα από το δίκτυο των ακουστικών αισθητήρων. Το δίκτυο αυτό αναλαμβάνει να εφοδιάζει το σύστημα με της περιβαλλοντικές συνθήκες της περιοχής.

Προκειμένου να γίνεται καταγραφή των σημείων επιτήρησης του συστήματος (είτε φορητών είτε σταθερών), επεκτείνουμε τους κόμβους καταγραφής του δικτύου αυτού ώστε να παρέχουν την συγκεκριμένη λειτουργικότητα. Η λειτουργικότητα αυτή επιτυγχάνεται με την ενσωμάτωση μιας επιπλέον πλακέτας επέκτασης στους κόμβους καταγραφής. Η πλακέτα επέκτασης είναι η iSense GPS Module. Ανά περιοδικά διαστήματα αναλαμβάνει να καταγράψει την θέση του και να αποστείλει τις συντεταγμένες στον σταθμό συλλογής. Ο σταθμός συλλογής αποθηκεύει τα δεδομένα στην βάση δεδομένων του συστήματος ώστε να είναι προσβάσιμα από τις μεθόδους εντοπισμού της θέσης μίας απειλής που εκτελούνται στο σταθμό βάσης του συστήματος. Η συχνότητα καταγραφής της θέσης εξαρτάται από το τύπο του σημείου επιτήρησης όπου είναι τοποθετημένος ο κόμβος καταγραφής.. Έτσι στην περίπτωση όπου το σημείο επιτήρησης είναι ένα φορητό σώμα (π.χ. ένας φύλακας), η συχνότητα καταγραφής της θέσης του θα πρέπει να είναι σχετικά μεγάλη, της τάξης του 1 λεπτού. Αντίθετα, στην περίπτωση όπου το σημείο επιτήρησης είναι σταθερό, η συχνότητα καταγραφής της θέσης του θα πρέπει να είναι μικρή, της τάξης των 30 λεπτών (ίσως και μικρότερη.)

6.4 Υλοποίηση

Όπως έγινε αντιληπτό στις παραπάνω παραγράφους, η μέθοδος εντοπισμού απειλών μέσω της χρήσης ασύρματων ακουστικών αισθητήρων αποτελεί ένα σύνολο τεχνικών, πρωτοκόλλων επικοινωνίας και διαχείρισης των ασύρματων κόμβων καθώς και επεξεργασίας των δεδομένων τους. Η υλοποίηση όλων αυτών των παράλληλων λειτουργιών μπορεί να περιγράφει μέσω του διαχωρισμού τους σε δύο ομάδες: τις λειτουργίες που αφορούν του ασύρματους κόμβους που βρίσκονται κατανεμημένοι στον χώρο και τις λειτουργίες που αφορούν στο σταθμό βάσης του συστήματος που βρίσκεται σε ένα σταθερό σημείο.

Οι ασύρματοι κόμβοι αναλαμβάνουν να καταγράφουν τα ακουστικά κύματα, να τα επεξεργάζονται και στην περίπτωση εντοπισμού μιας απειλής να στέλνουν τις απαραίτητες πληροφορίες στον σταθμό βάσης. Ο ρόλος του σταθμού βάσης είναι να λαμβάνει τις πληροφορίες από τους κόμβους και να τις συνδυάζει ώστε να εντοπίσει την πηγή του ακουστικού κύματος (απειλή). Ακόμα ο σταθμός βάσης είναι επιφορτισμένος με την λειτουργία του συγχρονισμού των ασύρματων κόμβων.

6.4.1 Υλοποίηση ασύρματων κόμβων

Οι ασύρματοι κόμβοι που χρησιμοποιήθηκαν είναι οι κόμβοι Mica2. Στους συγκεκριμένος κόμβους υπάρχει ενσωματωμένη η πλακέτα επέκτασης αισθητήρων MTS310. Η συγκεκριμένη πλακέτα περιέχει τον ακουστικό αισθητήρα LM567 της εταιρείας National Semiconductor ο οποίος ικανοποιεί τις ανάγκες της μεθόδου για την καταγραφή των ακουστικών κυμάτων.

Ο ασύρματος αισθητήρας κατά την διάρκεια εκτέλεσης της μεθόδου ανίχνευσης απειλών μεταβαίνει σε διάφορα στάδια λειτουργίας. Κάθε ένα από τα στάδια αυτά ικανοποιούν διαφορετικές απαιτήσεις τις εφαρμογής. Έτσι, κατά την εκκίνηση του ο ασύρματος κόμβος θέτει σε πλήρη λειτουργία τον μικρο-ελεγκτή του και τον πομποδέκτη του, ώστε να μπορέσει να εκτελέσει τις απαραίτητες λειτουργίες αρχικοποίησης του. Στην συνέχεια, ο κόμβος ενεργοποιεί την πλακέτα επέκτασης αισθητήρων MTS310 και ιδιαίτερα τον ακουστικό αισθητήρα που έχει ενσωματωμένο.

Το επόμενο στάδιο περιλαμβάνει την αρχικοποίηση και προθέρμανσή του ακουστικού αισθητήρα (διάρκειας 1.2 δευτερολέπτων).

Μετά την ολοκλήρωση των σταδίων ενεργοποίησης και αρχικοποίησης του κόμβου και των απαραίτητων υποσυστημάτων του, ο κόμβος μεταβαίνει σε μια συνεχή περιοδική εναλλαγή καταστάσεων. Πρόκειται για ένα σύνολο καταστάσεων λειτουργίας που αναλαμβάνουν τον συγχρονισμό, την καταγραφή των ακουστικών κυμάτων, την ανίχνευση απειλής αλλά και την διαχείριση του ίδιου του κόμβου.

Έτσι ο κάθε ασύρματος κόμβος του δικτύου, αφού ολοκληρώσει τα στάδια αρχικοποίησης του, περιμένει από τον σταθμό βάσης ένα μήνυμα συγχρονισμού. Την στιγμή λήψης αυτού του μηνύματος γίνεται καταγραφή της χρονοσφραγίδας του στο επίπεδο MAC. Έπειτα αυτή η χρονοσφραγίδα αποστέλλεται στον σταθμό βάσης και ο κόμβος μεταβαίνει στις καταστάσεις που είναι υπεύθυνες για την καταγραφή και επεξεργασία των ακουστικών κυμάτων. Κατά την διάρκεια εκτέλεσης αυτών των καταστάσεων δεν υπάρχει καμία ανάγκη επικοινωνίας του κόμβου με τους γειτονικούς του ή με τον σταθμό βάσης, οπότε και απενεργοποιούμαι το πομποδέκτη του. Με αυτό τον τρόπο μειώνουμε σε μεγάλο ποσοστό την κατανάλωση ενέργειας του κόμβου.

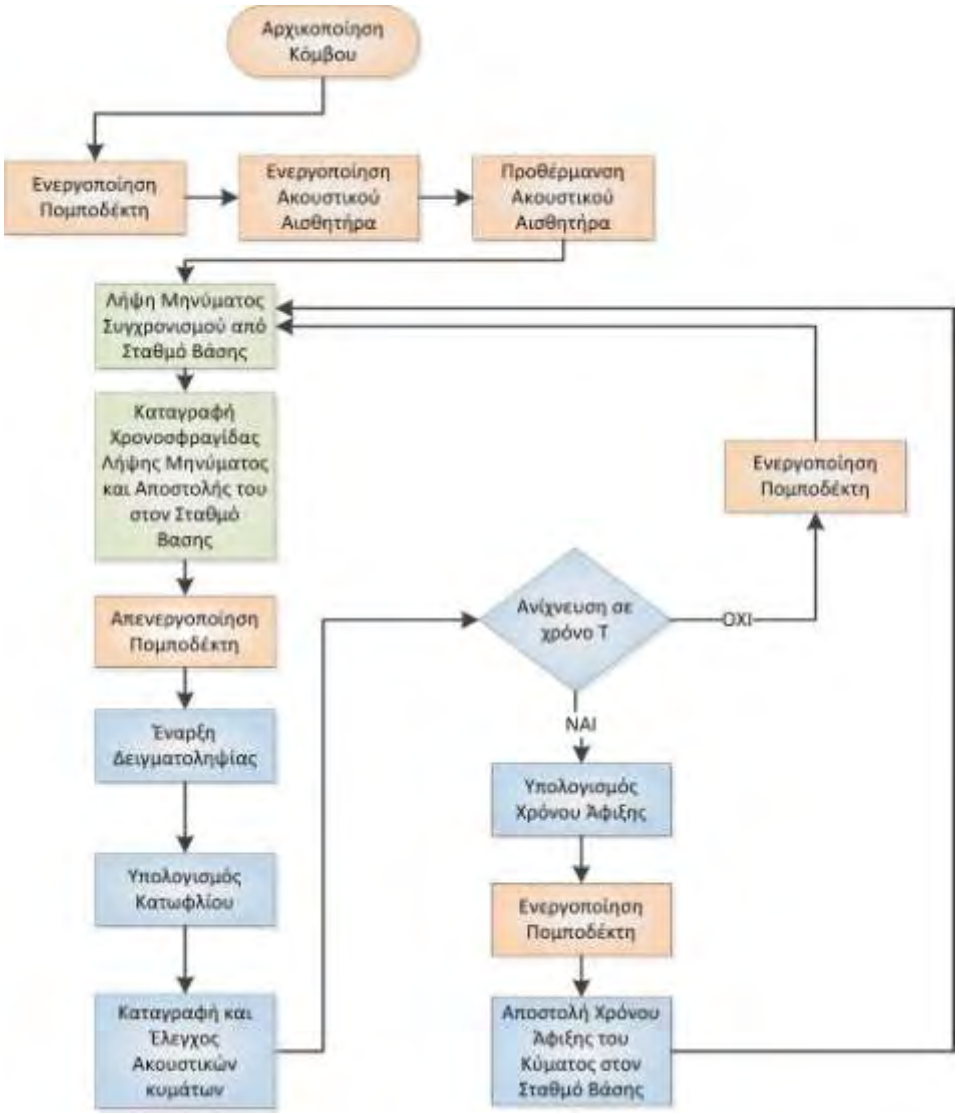
Έπειτα ο κόμβος λαμβάνει από τον σταθμό βάσης ένα μήνυμα με την ταχύτητα του ανέμου και καταγράφει για ένα μικρό χρονικό διάστημα τον θόρυβο του περιβάλλοντος λειτουργίας του. Η ταχύτητα του ανέμου και το μέγιστο επίπεδο θορύβου που καταγράφηκε κατά το τρέχον διάστημα θα χρησιμοποιούν για τον υπολογισμό του επίπεδου κατωφλίου. Αυτό το επίπεδο είναι σταθερό καθόλη την διάρκεια καταγραφής των ακουστικών κυμάτων για διάστημα Τ, είτε μέχρι τον εντοπισμό μιας απειλής. Το μήνυμα με την ταχύτητα του ανέμου μπορεί να σταλεί από τον σταθμό βάσης προς τον κάθε κόμβο κατά την διάρκεια της συγκεκριμένη κατάσταση λειτουργίας. Παρόλα αυτά, επειδή η λήψη ενός επιπλέον μηνύματος από τους ασύρματους κόμβους συμβάλει στην αύξηση του ενεργειακού κόστους, επιλέγεται οι πληροφορίες του ανέμου να ενσωματώνονται στο μήνυμα συγχρονισμού. Το γεγονός αυτό προκαλεί την εξοικονόμηση αρκετής ενέργειας .(το ποσοστό της εξοικονόμησης θα μελετηθεί σε παρακάτω ενότητα)

Στη συνέχεια, ο κόμβος ξεκινάει την καταγραφή των ακουστικών κυμάτων και τον έλεγχο τους για την ανίχνευση πιθανής απειλής. Η καταγραφή των ακουστικών κυμάτων γίνεται με συχνότητα δειγματοληψίας ~ 10KHz.

Στην περίπτωση όπου ο κόμβος δεν ανιχνεύσει μια απειλή για διάστημα T = 15 min (Ενότητα 6.3.2.3), ο κόμβος ενεργοποιεί τον πομποδέκτη του και μεταβαίνει σε κατάσταση συγχρονισμού. Περιμένει ένα νέο μήνυμα συγχρονισμού από τον σταθμό βάσης, ώστε να ξεκινήσει από την αρχή την αλληλουχία καταστάσεων συγχρονισμού και ανίχνευσης απειλής.

Στην περίπτωση όπου ο κόμβος ανιχνεύσει μια απειλή, ενεργοποιεί τον πομποδέκτη του στέλνει στον σταθμό βάσης την χρονική στιγμή άφιξης του κύματος στον κόμβο. Η χρονική στιγμή άφιξης του κύματος ορίζεται ως η χρονική στιγμή του πρώτου μηδενισμού του κύματος μετά την υπέρβασή του από το επίπεδο κατωφλίου του κόμβου (Ενότητα 6.3.1.2). Στην συνέχεια ο κόμβος μεταβαίνει σε κατάσταση συγχρονισμού όπου και περιμένει ένα νέο μήνυμα συγχρονισμού από τον σταθμό βάσης.

Τα παραπάνω παρουσιάζονται σχηματικά στο διάγραμμα ροής της λειτουργίας του κόμβου (Εικόνα 57).



Εικόνα 57: Διάγραμμα ροής της μεθόδου ανίχνευσης απειλών των ασύρματων κόμβων του δικτύου αισθητήρων.

Για τον προγραμματισμό των κόμβων χρησιμοποιήθηκε η γλώσσα nesC και το λειτουργικό σύστημα TinyOS 2. Η εφαρμογή αποτελείται από βασικό (configuration) αρχείο SurveilAppC, το οποίο ορίζει τις συνδέσεις (wirings) μεταξύ των διάφορων στοιχείων και των διεπαφών τους. Τα στοιχεία που χρησιμοποιούνται είναι:

- **MainC:** αποτελεί το βασικό στοιχείο κάθε TinyOS εφαρμογής
- **LedsC:** παρέχει πρόσβαση στα leds του κόμβου (χρήσιμα για την απασφαλμάτωση του προγράμματος).
- **LocalTime:** πρόκειται για έναν 32-bit μετρητή ο οποίος περιέχει κάθε φορά την τρέχων χρονική στιγμή του κόμβου.
- **ActiveMessageC:** προσφέρει τις βασικές λειτουργίες για την ασύρματη επικοινωνία του κόμβου καθώς και για την καταγραφή των χρονοσφραγίδων λήψης των μηνυμάτων. (Πλέον στο κείμενο θα χρησιμοποιείται με το όνομα *Radio*)

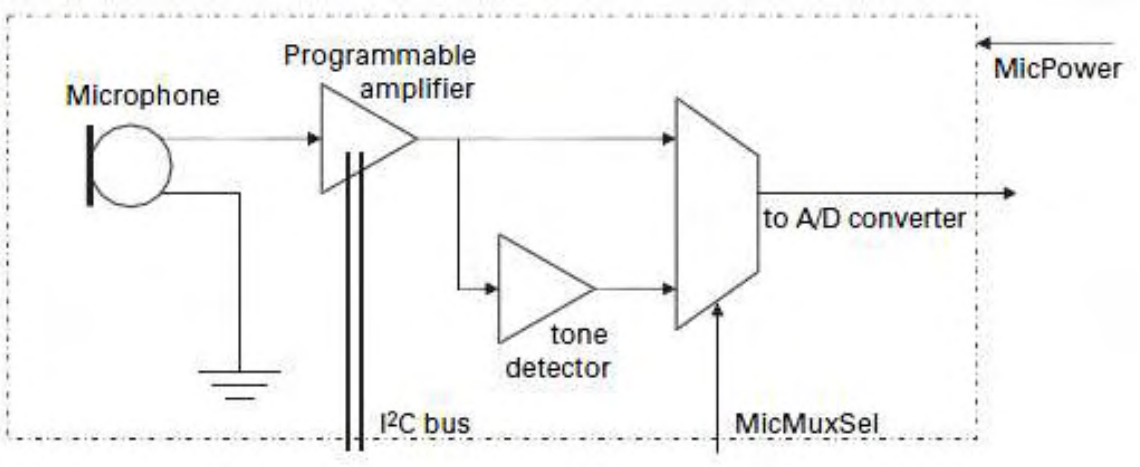
- **MicrophoneC:** ενεργοποιεί τον ακουστικό αισθητήρα, τον προθερμαίνει, ρυθμίζει διάφορα χαρακτηριστικά της λειτουργίας του (π.χ. gain) και δειγματοληπτεί τον αισθητήρα
- **DetectC:** αναλαμβάνει την χρήση των ακουστικών δεδομένων για τον υπολογισμό του κατωφλίου, τον έλεγχο ενός ακουστικού κύματος για την υπέρβασή του καθώς και τον εντοπισμό του μηδενικού του σημείου για τον υπολογισμό του χρόνου άφιξης του κύματος.
- **SurveilC:** πρόκειται για το κεντρικό αρχείο του προγράμματος, το οποίο αναλαμβάνει να διαχειριστεί όλα τα υπόλοιπα στοιχεία και διεπαφές ώστε ο κόμβος να εκτελεί σωστά τις διάφορες λειτουργίες και μεθόδους του καθώς και να μεταβαίνει στις αντίστοιχες κάθε φορά καταστάσεις λειτουργίας του.

Με την εκκίνηση του κόμβου, το πρόγραμμα ξεκινάει με την εκτέλεση του SurveilC και συγκεκριμένα με την μέθοδο ***Boot.booted()***. Η συγκεκριμένη μέθοδος αρχικοποιεί κατά σειρά τα υποσυστήματα των leds, του πομποδέκτη (***ActiveMessageC.start()***) και του ακουστικού αισθητήρα (***MicrophoneC.start()***).

Παρακάτω περιγράφονται με λεπτομέρεια τα κυριότερα αρχεία του προγράμματος

MicrophoneC

Πρόκειται για τον κώδικα ο οποίος αναλαμβάνει να χειριστεί τον ακουστικό αισθητήρα της πλακέτας MTS310. Το σχηματικό διάγραμμα του ακουστικού αισθητήρα φαίνεται στην Εικόνα 58.Το μικρόφωνο ενεργοποιείται μέσω μιας ψηφιακής I/O εισόδου (MicPower) από τον μικρο-ελεγκτή. Τα ανεπεξέργαστα (raw) δεδομένα που καταγράφονται από τον ακουστικό αισθητήρα ενισχύονται με την χρήση ενός ενισχυτή. Το μέγεθος της ενίσχυσης των δεδομένων ορίζεται μέσα στο αρχείο από την σταθερά MIC_GAIN. Η τιμή της μεταβλητή MIC_GAIN έχει εύρος 0 – 255 και καθορίζεται σε μεγάλο βαθμό από την ευαισθησία των ακουστικών αισθητήρων, το περιβάλλον τοποθέτησης του κόμβου, του είδους και της έντασης των ακουστικών κυμάτων που καταγράφονται και γενικά το είδος της εφαρμογής που χρησιμοποιείται. Στην συγκεκριμένη περίπτωση, μετά από δοκιμές, καταλήξαμε στην τιμή της μεταβλητής MIC_GAIN = 64. Τέλος, ο κώδικας αναλαμβάνει την προθέρμανση του ακουστικού αισθητήρα για χρονικό διάστημα ίσο με 1.2 δευτερόλεπτα.



Εικόνα 58: Η δομή του ακουστικού αισθητήρας της πλακέτας επέκτασης MTS310 [66].

DetectC

Πρόκειται για τον κώδικα ο οποίος αναλαμβάνει να διαχειρισθεί για μετρήσεις του ακουστικού αισθητήρα του κόμβου. Συγκεκριμένα, αναλαμβάνει να καταγράψει την τιμή του αισθητήρα που λαμβάνεται από το ***MicrophoneC,*** να υπολογίσει το επίπεδο του κατωφλίου, να εντοπίσει την ύπαρξη κάποιας απειλής (υπέρβαση του κατωφλίου) και τέλος να υπολογίσει τον χρόνο άφιξης του κύματος στον κόμβο. Όπως είναι φανερό, ο κώδικας αυτός αναλαμβάνει μερικές από τις σημαντικότερες λειτουργίες του κόμβου, οπότε και η αποδοτική υλοποίησή τους είναι ζωτικής σημασίας για την αποτελεσματικότητα της μεθόδου εντοπισμού.

Προκειμένου να υπολογιστεί με ακρίβεια και ταχύτητα αν ένα κύμα υπερβαίνει το επίπεδο του κατωφλίου, ο κώδικας θα πρέπει να δειγματοληπτεί τον ακουστικό αισθητήρα με την μέγιστη δυνατή συχνότητα. Επιπλέον, θα πρέπει να υπάρχει η ελάχιστη δυνατή χρονική ολίσθηση ανάμεσα στην στιγμή όπου ο μικρο-ελεγκτής λαμβάνει την τιμή από τον A/D του αισθητήρα και την στιγμή όπου η τιμή αυτή ελέγχεται από το DetectC ώστε να διαπιστωθεί αν υπερβαίνει το κατώφλι. Η χρονική αυτή καθυστέρηση προσθέτει μια επιπλέον πηγή ανακρίβειας στον χωρικό προσδιορισμό της απειλής. Ενδεικτικά αναφέρουμε ότι η χρονική καθυστέρηση που προκαλεί η υψηλού επιπέδου διεπαφή λήψης δεδομένων από αισθητήρες ***Read*** (του λειτουργικού συστήματος TinyOS) είναι της τάξης των 50-100 μs.

Για την μείωση αυτής της καθυστέρησης, ο κώδικας του ***DetectC*** χρησιμοποιεί τον A/D μετατροπέα που προσφέρεται από τον μικρο-ελεγκτή ATmega128 (ο μικρο-ελεγκτής του κόμβου Mica2). Αυτός ο A/D μετατροπέας είναι διαθέσιμος μέσω της παρακάτω διεπαφής Atm128AdcC:

```
interface Atm128AdcSingle {
        async command bool getData(uint8_t channel , uint8_t refVoltage ,
                                   bool leftJustify , uint8_t prescaler );

        async event void dataReady(uint16_t data , bool precise );

        async command bool cancel ();
}
```

Η συγκεκριμένη διεπαφή επιτρέπει στο ***DetectC*** να δειγματολειπτεί το ακουστικό αισθητήρα σε πολύ μεγάλη συχνότητα και με πολύ μικρή καθυστέρηση ανίχνευσης της απειλής. Επιπλεόν, η εντολή getData της διεπαφή δίνει την δυνατότητα ορισμού μιας παραμέτρου η οποία ορίζει τον επιθυμητό χρόνο μετατροπή ενός δεδομένου στον A/D μετατροπέα. Μειώνοντας τον χρόνο μετατροπής μειώνεται και η ακρίβεια της μετατροπής του A/D μετατροπέα. Έτσι στην περίπτωση όπου η παράμετρος έχει την μέγιστη τιμή, οπότε και την μέγιστη δυνατή ακρίβεια, ο χρόνος που απαιτείται για την εκτέλεση μιας μετατροπής είναι 113 μs.

Παρόλα αυτά, στην περίπτωση της μεθόδου εντοπισμού απειλής, ο έλεγχος μιας τιμής αν ξεπερνάει ένα κατώφλι είναι μια πολύ απλή διαδικασία και δεν απαιτεί την μέγιστη ακρίβεια του A/D μετατροπέα. Έτσι στο κώδικα του ***DetectC,*** η εντολή ***getData*** δέχεται ως παράμετρο μια χαμηλή τιμή (την προκαθορισμένη σταθερά ATM128_ADC_PRESCALE_16) η οποία δίνει μία ακρίβεια μετατροπής στα 16-bit και μειώνει το χρόνο μετατροπής του A/D στα 28 μs.

Ο χρόνος ανάμεσα σε δύο διαδοχικές δείγματα του κύματος επιλέγεται να είναι 100 μs. Αυτός ο ελεύθερος χρόνος ανάμεσα σε 2 δείγματα (72 μsec), επιτρέπει την εκτέλεση των απαραίτητων έλεγχων και εντολών επεξεργασίας που είναι απαραίτητες για την ανίχνευση των απειλών. Έτσι η τελική συχνότητα δειγματοληψίας που χρησιμοποιούν οι κόμβοι είναι της τάξης των 10 kHz.

Για την λήψη δειγμάτων του ακουστικού κύματος, ο κόμβος καλεί την συνάρτηση ***Atm128AdcSingle.getData(…)*** . Η συνάρτηση αυτή αναλαμβάνει να εκκινήσει την διαδικασία λήψης ενός δείγματος. Η διαδικασία λήψης ενός δείγματος ολοκληρώνεται με την εκτέλεση του γεγονότος ***event void Atm128AdcSingle.dataReady(uint16_t data).*** Η παράμετρος ***uint16_t data*** περιέχει την τιμή που μόλις καταγράφτηκε από τον κόμβο. Στην συνέχεια εκτελούνται τα βήματα για τον έλεγχο και την επεξεργασία της τιμής, σύμφωνα με τα στάδια λειτουργίας του κόμβου. Έτσι οι ενέργειες που εκτελούνται είναι:

```
event void Atm128AdcSingle.dataReady(uint16_t data){

        if ( data > threshold ){
                Εντοπισμός απειλής.
                Καλούμε την συνάρτηση Atm128AdcSingle.getData(…) ώστε να
                λάβουμε το επόμενο δείγμα και να βρούμε το σημείο μηδενισμού
                του κύματος
        }

        if  (έχει εντοπισθεί απειλή  &  data >= επίπεδο μηδενισμού) {
        t1 = localTime();
                Atm128AdcSingle.getData(…)
        }

        if  (έχει εντοπισθεί απειλή  &  data < επίπεδο μηδενισμού) {
        t2 = localTime();
                Εντοπίστηκε η χρονική στιγμή μηδενισμού του κύματος. Είναι το
                t0 = ( t2 – t1) / 2 ,  το οποίο στην συνέχεια αποστέλλεται στον
                σταθμό βάσης.
        }
}
```

Ως επίπεδο μηδενισμού του κύματος ορίζεται το επίπεδο όπου το κύμα έχει μηδενική ενέργεια. Στην συγκεκριμένη περίπτωση η καταγραφή του κύματος από τους ακουστικούς αισθητήρες και η μετατροπή τους από τον A/D μετατροπέα επιστρέφει θετική τιμή εκφρασμένη σε mV. Το εύρος δυνατόν τιμών που μπορεί να πάρει η καταγεγραμμένη τιμή του ακουστικού κύματος είναι 0 – 1000 mV. Οπότε το επίπεδο μηδενισμού έχει την τιμή 500 mV.

SurveilC

Πρόκειται για το κεντρικό κομμάτι του προγράμματος, το οποίο είναι υπεύθυνο για την εκτέλεση όλων των λειτουργιών του κόμβου. Ουσιαστικά, ο κώδικας του SurveilC αναλαμβάνει να διαχειριστεί και να συντονίσει όλα τα υποσυστήματα του κόμβου ώστε να παρέχουν την επιθυμητή λειτουργικότητα.

Η βασική αλληλουχία των εντολών του SurveilC ξεκινάει με την λήψη του μηνύματος συγχρονισμού από τον σταθμό βάσης. Η λήψη του μηνύματος σηματοδοτείται με το γεγονός ***Radio.receive(message)***. Στον εσωτερικό του κώδικα χειρισμού της λήψης του μηνύματος καλείται η εντολή ***PacketTimeStamp.timestamp(message)***. Η εντολή αυτή επιστρέφει την χρονοσφραγίδα λήψης του μηνύματος. Έτσι η σειρά των εντολών είναι:

```
event message_t* Radio.receive(message).

        //Ελεγχος αν έχει λειφθεί σωστά το πακέτο και μπορούμε να
        καταγράψουμε την χρονοσφραγίδα λήψης του
        if (call PacketTimeStamp.isValid(message)) {

                //Λήψη της χρονοσφραγίδας και ανάθεσή της στην μεταβλητη rxTimestamp
                rxTimestamp = call PacketTimeStamp.timestamp(message);

                //Δημιουργία νέου πακέτου αποστολής δεδομένων msg
                TimestampMsg msg;

                //Αποθήκευση των δεδομένων στο πακέτο αποστολής
                msg->id = TOS_NODE_ID;
                msg->roundNum = roundNum;
                msg->timestamp = rxTimestamp;

                //Αποστολή του πακέτου στον σταθμό βάσης
                send(AM_BASE_ADDR, &msg)
        }
}
```

Αφού ολοκληρωθεί η αποστολή του μηνύματος στον σταθμό βάσης (σηματοδοτείται με το γεγονός ***Radio.sendDone()***) , ο κόμβος εκτελεί την εντολή ***Radio.stop()*** ώστε να απενεργοποιήσει τον πομποδέκτη. Στην συνέχεια ξεκινάει η δειγματοληψία των ακουστικών κυμάτων ώστε να γίνει υπολογισμός του κατωφλίου και ανίχνευση απειλών (μέσω του DetectC). Στην περίπτωση όπου ανιχνευτεί μια απειλή, ενεργοποιείται ο πομποδέκτης και στέλνεται στον σταθμό βάσης ο χρόνος άφιξης του κύματος της

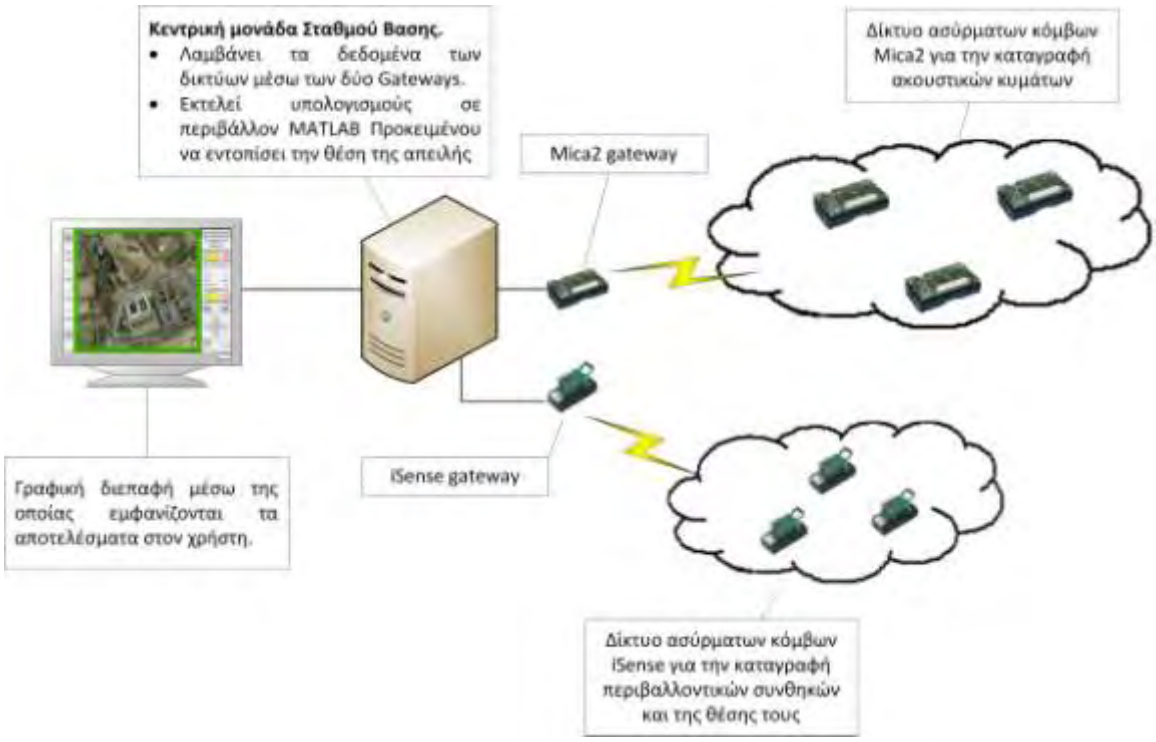
απειλής. Στην συνέχεια ο κόμβος ξεκινάει την ίδια διαδικασία συγχρονισμού και δειγματοληψίας. Στην περίπτωση όπου δεν εντοπισθεί κάποια απειλή, ο κόμβος συνεχίζει την δειγματοληψία για διάστημα Τ. Μετά το πέρας αυτού του χρονικού διαστήματος ο κόμβος ενεργοποιεί τον πομποδέκτη του και επαναλαμβάνει την αλληλουχία καταστάσεων συγχρονισμού και ανίχνευσης απειλής.

6.4.2 Υλοποίηση σταθμού βάσης

Ο σταθμός βάσης αποτελεί το κεντρικό σημείο του συστήματος το οποίο αναλαμβάνει να εκτελέσει όλες τι πολύπλοκες αλγοριθμικές διαδικασίες που απαιτούνται για τον ακριβή εντοπισμό της θέσης μιας απειλής. Συγκεκριμένα ο σταθμός βάσης αναλαμβάνει να:

- Επικοινωνήσει με τους ασύρματους κόμβους που φέρουν τους ακουστικούς αισθητήρες ώστε να συλλέξει όλες τις απαραίτητες πληροφορίες (χρόνο άφιξης του κύματος στους κόμβους) για τον εντοπισμό της πηγής.
- Επικοινωνήσει με τους ασύρματους κόμβους ώστε να συλλέξει πληροφορίες για τον συγχρονισμό τους.
- Εκτελέσει πολύπλοκές διαδικασίες για τον συνδυασμό των πληροφοριών από τους κόμβους και τον εντοπισμό της απειλής.
- Συλλέξει και αποθηκεύσει τα δεδομένα από τους κόμβους συλλογής περιβαλλοντικών δεδομένων.
- Συλλέξει και αποθηκεύσει δεδομένα σχετικά με την θέση των κόμβων.
- Παρουσιάσει την θέση της πηγής στον χρήστη του συστήματος.

Βασικό στοιχείο του σταθμού βάσης αποτελεί η κεντρική μονάδα. Πρόκειται για μια μονάδα ικανή να εκτελέσει πολύπλοκους υπολογισμούς σε προγραμματιστικό περιβάλλον MATLAB και ικανή να αποθηκεύσει τα αποτελέσματα των υπολογισμών καθώς και τα δεδομένα των κόμβων. Η επικοινωνία της κεντρικής μονάδας με τα δύο ασύρματα δίκτυα των αισθητήρων (Mica2 και iSense) επιτυγχάνεται με τη χρήση δύο κόμβων ειδικών λειτουργιών (gateways). Έναν κόμβο τύπου Mica2 ο οποίος λειτουργεί ως γέφυρα επικοινωνίας ανάμεσα στο ασύρματο δίκτυο των κόμβων Mica2 και στην κεντρική μονάδα και έναν κόμβο τύπου iSense ο οποίος λειτουργεί ως γέφυρα μεταφοράς δεδομένων ανάμεσα στο δίκτυο των ασύρματων κόμβων iSense και την κεντρική μονάδα. Τέλος ο σταθμός βάσης κάνει χρήση μιας οθόνης η οποία παρουσιάζει τα αποτελέσματα των μεθόδων στον χρήστη του συστήματος. Η παρουσίαση αυτή γίνεται μέσω μιας γραφικής διεπαφής (GUI).



Εικόνα 59: Η αρχιτεκτονική του συστήματος και οι διασυνδέσεις του σταθμού βάσης

Κατά την διάρκεια λειτουργίας του, ο σταθμός βάσης εκτελεί διάφορες διαδικασίες ανάλογα με το στάδιο λειτουργίας όπου βρίσκεται. Κάθε μια από τις διαδικασίες αυτές ικανοποιούν διαφορετικές απαιτήσεις τις εφαρμογής. Έτσι, κατά την εκκίνηση του ο σταθμός βάσης θέτει σε πλήρη λειτουργία την κεντρική μονάδα επεξεργασίας του, καθώς και τους δύο κόμβους που λειτουργούν σαν gateways για τα ασύρματα δίκτυα αισθητήρων. Οι πομποδέκτες που βρίσκονται ενσωματωμένοι στους δύο gateways κόμβους θέτονται σε πλήρη λειτουργία. Κατά την διάρκεια λειτουργίας του σταθμού βάσης, η κατάσταση λειτουργίας των πομποδεκτών θα μείνει αμετάβλητη, καθώς δεν υπάρχει ανάγκη εξοικονόμησης πόρων από του κόμβους (θεωρούμε ότι ο σταθμός βάσης έχει συνεχή παροχή ρεύματος).

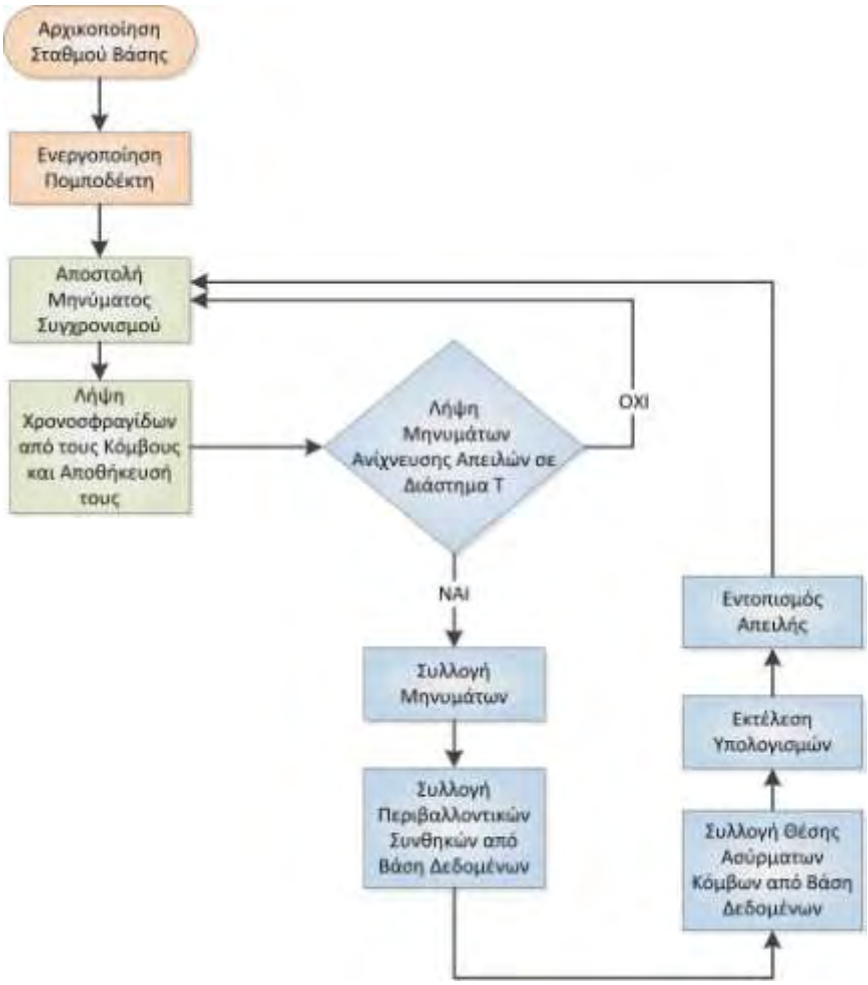
Στην συνέχεια, ο σταθμός βάσης, μέσω της gateway τύπου Mica2, στέλνει ένα μήνυμα συγχρονισμού στο δίκτυο αισθητήρων υπεύθυνο για την καταγραφή των ακουστικών κυμάτων. Οι ασύρματοι κόμβοι του δικτύου, αφού λάβουν το μήνυμα καταγράφουν τον χρόνο λήψης του μηνύματος, τον οποίο και στέλνουν πίσω στον σταθμό βάσης. Ο σταθμός βάσης αφού λάβει τις χρονοσφραγίδες από όλους τους κόμβος του δικτύου, δημιουργεί ένα πίνακα: τον ***Πίνακα Συγχρονισμού.*** Ο συγκεκριμένος πίνακας διαθέτει μια καταγραφή για κάθε κόμβο του δικτύου. Αυτή η καταγραφή θα χρησιμοποιηθεί σε επόμενο στάδιο προκειμένου να υπολογισθεί, με ακρίβεια, η χρονική ολίσθηση του κάθε κόμβου (Ενότητα 6.3.2.3).

Μετά το στάδιο του συγχρονισμού, οι ασύρματοι κόμβοι του δικτύου καταγράφουν και ελέγχου τα ακουστικά κύματα. Την ίδια στιγμή ο σταθμός βάσης περιμένει την λήψη μηνυμάτων ανίχνευσης απειλής από τους κόμβους. Η αναμονή τους σταθμού βάσης για την λήψη μηνυμάτων ανίχνευσης διαρκεί T = 15 λεπτά. Στην περίπτωση όπου μέσα στο χρονικό διάστημα T γίνει λήψη κάποιου μηνύματος ανίχνευσης απειλών, ο σταθμός βάσης εκτελεί τις απαραίτητες διαδικασίες για τον υπολογισμό της θέσης της απειλής. Σε

διαφορετική περίπτωση, ο σταθμός βάσης αρχίζει ένα νέο γύρω καταγραφής ξεκινώντας με τον συγχρονισμό των κόμβων (στάδιο αποστολής μηνύματος συγχρονισμού).

Παράλληλα, ο σταθμός βάσης αναλαμβάνει να συλλέξει τα περιβαλλοντικά δεδομένα καθώς και τα δεδομένα θέσης από το 2ο ασύρματο δίκτυο αισθητήρων (κόμβοι iSense). Οι κόμβοι του 2^{ου} δικτύου αισθητήρων περιοδικά καταγράφουν τις συνθήκες του περιβάλλοντος και την θέση τους. Τα δεδομένα αυτά αποστέλλονται στον σταθμό βάσης μέσω του αντίστοιχου gateway. Ο σταθμός βάσης, αφού λάβει τα δεδομένα, τα αποθηκεύει σε μία βάση δεδομένων, ώστε να είναι διαθέσιμα για χρήση οποιαδήποτε στιγμή.

Τα παραπάνω παρουσιάζονται σχηματικά στο διάγραμμα ροής της λειτουργίας του κόμβου (Εικόνα 60).



Εικόνα 60: Διάγραμμα ροής της μεθόδου ανίχνευσης απειλών του σταθμού βάσης.

Ο υπολογισμός της θέσης μιας απειλής προϋποθέτει την χρήση δεδομένων που είτε βρίσκονται αποθηκευμένα στην βάση δεδομένων του σταθμού βάσης, είτε συλλέγονται εκείνη την στιγμή από τους κόμβους. Τα δεδομένα αυτά είναι:

- Οι χρονοσφραγίδες των κόμβων που βρίσκονται αποθηκευμένες στο Πίνακα Συγχρονισμού που διατηρεί ο σταθμός βάσης.

- Οι χρόνοι άφιξης του ακουστικού κύματος στους κόμβους. Ο σταθμός βάσης λαμβάνει τους χρόνους αυτούς σε πραγματικό χρόνο, κατά την ανίχνευση ,δηλαδή, του ακουστικού κύματος της απειλής.
- Τα περιβαλλοντικά δεδομένα που βρίσκονται αποθηκευμένα στην βάση δεδομένων του σταθμού βάσης.
- Τα δεδομένα θέσης των κόμβων, τα οποία βρίσκονται αποθηκευμένα στην βάση δεδομένων του σταθμού βάσης.

Το πρόγραμμα συλλογής, επεξεργασίας των δεδομένων καθώς και διενέργειας των υπολογισμών για τον εντοπισμό της θέσης μιας απειλής είναι υλοποιημένο στο περιβάλλον προγραμματισμού MATLAB. Το πρόγραμμα αποτελείται από 2 κύρια μέρη. Το πρώτο μέρος έχει να κάνει με την παραλαβή των δεδομένων από τους ασύρματους κόμβους μέσω της θύρας USB σύνδεσης του σταθμού βάσης με τις gateways. Στο δεύτερο μέρος βάσει των δεδομένων που έχουν ληφθεί εκτελείται ο αλγόριθμος εντοπισμού θέσης της ηχητικής πηγής που αναλύθηκε σε προηγούμενη ενότητα και απεικονίζουμε την πρόβλεψη μας.

Λήψη μηνυμάτων από τους κόμβους μέσω των αντίστοιχων gateways

Κάθε μήνυμα του στέλνεται από τους ασύρματους κόμβους λαμβάνεται από την gateway του αντίστοιχου δικτύου. Στην συνέχεια προωθείται στην USB θύρα σύνδεσής της με τον σταθμό βάσης. Αρμοδιότητα του συγκεκριμένου προγράμματος είναι να διαβάσει τα πακέτα δεδομένων που προωθούνται στις δύο USB θύρες σύνδεσης και να τα επεξεργαστεί.

Τα πακέτα δεδομένων που αποστέλλονται από τους ασύρματους κόμβους, εκτός από τα χρήσιμα δεδομένα, περιέχουν μερικά επιπλέον byte στην αρχή και στο τέλος του πακέτου. Τα επιπλέον αυτά byte χρησιμοποιούνται για την αποθήκευση πληροφοριών χρήσιμων για την επιτυχή ασύρματη αποστολή του μηνύματος (όπως είναι η διεύθυνση παραλήπτη κλπ). Οι πληροφορίες αυτές δεν είναι χρήσιμες για τον υπολογισμό της θέσης μιας απειλής, οπότε και θα πρέπει να μην χρησιμοποιούνται. Οι μη-χρήσιμες πληροφορίες που βρίσκονται στην αρχή του πακέτου είναι 11 bytes.

Εικόνα 61: Η δομή ενός πακέτου ασύρματης επικοινωνίας

Το πρόγραμμα αφού εξάγει τα χρήσιμα δεδομένα, τα επεξεργάζεται ώστε να αναγνωρίσει τον τύπο των δεδομένων (ανίχνευση απειλής, περιβαλλοντικά δεδομένα κλπ) , και τον αποστολέα τους. Στην συνέχεια ανάλογα με τον τύπο των δεδομένων είτε τα αποθηκεύει στην βάση δεδομένων, είτε τα προωθεί στο πρόγραμμα εκτέλεσης υπολογισμών για τον εντοπισμό της θέσης.

Η σειρά εκτέλεσης των εντολών του προγράμματος φαίνονται παρακάτω:

```
function readData{

        s = serial ('COM9')              //σύνδεση με την θύρα σύνδεσης της gateway

        while (1){
                packet = freads (s)                    //διάβασμα του πακέτου από την θύρα
                data = packet [11, packetSize] //λήψη μόνο των χρήσιμων
                                                       //δεδομένων
                data_type = data[0]                    //αναγνώριση του είδους του πακέτου
                data_sender = data[1]      //αναγνώριση του αποστολέα του
                                                       //πακέτου
                if ( data_type == 0  ){    //ανίχνευση απειλής
                        Εξόρυξη των δεδομένων
                        Μετατροπή τους από bytes στους πραγματικούς τύπους μεταβλητών
                        τους
                        Αποστολή τους στο πρόγραμμα εντοπισμού της απειλής
                } else if (data_type == 1) {          //περιβαλλονικά δεδομένα
                        Εξόρυξη των δεδομένων
                        Μετατροπή τους από bytes στους πραγματικούς
                        τύπους μεταβλητών τους
                        Αποθήκευση τους στην βάση δεδομένων
                } else if (data_type == 2){           //δεδομένα θέσης κόμβου
                        Εξόρυξη των δεδομένων
                        Μετατροπή τους από bytes στους πραγματικούς
                        τύπους μεταβλητών τους
                        Αποθήκευση τους στην βάση δεδομένων
                }
}
```

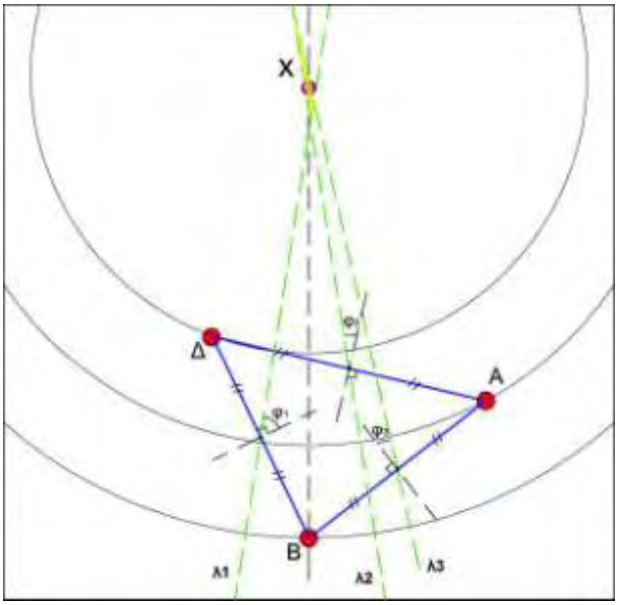
Αλγόριθμος εντοπισμού

Ο αλγόριθμός εντοπισμού μιας απειλής είναι υλοποιημένος στο προγραμματιστικό περιβάλλον MATLAB. Αποτελείται από τρείς συναρτήσεις: την συνάρτηση ***sound_speed***, την συνάρτηση ***source*** και την συνάρτηση ***angle***. Οι συναρτήσεις αυτές αναλαμβάνουν να εκτελέσουν τον αλγόριθμο εντοπισμού που περιγράφτηκε παραπάνω, στο Κεφάλαιο 6.2.

Η συνάρτηση ***sound_speed*** αναλαμβάνει να συλλέξει τα τρέχων περιβαλλοντικά δεδομένα από την βάση δεδομένων και να υπολογίσει την ταχύτητα του ήχου την συγκεκριμένη στιγμή στον συγκεκριμένο χώρο. Τα δεδομένα αυτά αφορούν την θερμοκρασία, την σχετική υγρασία και την ατμοσφαιρική πίεση του περιβάλλοντος την τρέχων χρονική στιγμή. Ο αλγόριθμος υπολογισμού της ταχύτητας του ήχου βασίζεται στην εξίσωση που προτείνεται από τον ερευνητή Owen Creamer στην μελέτη του "*The variation of the specific heat ratio and the speed of sound in air with temperature, pressure, humidity, and CO2 concentration"* [156-157].

Η συνάρτηση ***source*** υπολογίζει με ακρίβεια την θέση της ηχητικής πηγής του κύματος. Χρησιμοποιεί σαν δεδομένα τις θέσεις των κόμβων, τους χρόνους άφιξης του ηχητικού κύματος σε αυτούς και την ταχύτητα του κύματος και υπολογίζει την θέση της

πηγής εκτελώντας τον αλγόριθμο εντοπισμού που περιγράφτηκε στο Κεφάλαιο 6.2 και απεικονίζεται στην παρακάτω εικόνα.



Εικόνα 62: Απεικόνιση μεθόδου εντοπισμού μιας απειλής.

Η συνάρτηση ***source*** χρησιμοποιεί τις θέσεις των τριών κόμβων Α, Β, Γ προκειμένου να υπολογίσει την μεταξύ τους απόσταση. Ακόμα ενημερώνεται σχετικά με την ταχύτητα του ήχου καλώντας την συνάρτηση ***sound_speed***.

Η συνάρτηση για κάθε ζευγάρι κόμβων υπολογίζει την ευθεία που ενώνει τους κόμβους αυτούς. Στο μέσο της κάθε ευθείας υπολογίζεται μια νέα ευθεία **(ευθείες λ1,λ2,λ3)** η οποία έχει γωνία φ με την μεσοκάθετο της ευθείας αυτής. Οι γωνίες φ υπολογίζονται από την συνάρτηση ***angle.*** Τέλος λύνοντας τα γραμμικά συστήματα που προκύπτουν από τις 3 ευθείες λ1,λ2,3 υπολογίζουμε τις τομές τους. Οι τομές αυτές αποτελούν τα όρια της περιοχής εντοπισμού της ηχητικής πηγής.

Η συνάρτηση ***angle*** καλείται για κάθε ζευγάρι κόμβων μέσα από την source για την εύρεση των κρίσιμων γωνιών που δημιουργούν τις ευθείες λ1,λ2 και λ3. Δέχεται ως είσοδο τους αντίστοιχους χρόνους αφίξεων των δύο κάθε φορά κόμβων και υπολογίζει την γωνία που σχηματίζεται ανάμεσα στην μεσοκάθετο της ευθείας που συνδέει τους δύο κόμβους και την ευθεία η οποία περνά από την θέση της ηχητικής πηγής. Για να γίνει ο υπολογισμός αυτός πρέπει να υπολογιστεί η απόσταση που διένυσε το μέτωπο του ηχητικού κύματος από την στιγμή του στον $1^{ο}$ κόμβο μέχρι την στιγμή άφιξής του στον $2^{ο}$. Η συνάρτηση διαχωρίζει τους κόμβους σαν $1^{ο}$ και $2^{ο}$ σύμφωνα με την κατεύθυνση του ηχητικού κύματος. Έτσι ο κόμβος που έχει τον μικρότερο, από τους δύο, χρόνους άφιξης του κύματος, θεωρείται ότι βρίσκεται πιο κοντά στην ηχητική πηγή και χαρακτηρίζεται ως $1^{ος}$. Γίνεται η θεώρηση, δηλαδή, ότι το κύμα κατευθύνεται από το $1^{ο}$ προς τον $2^{ο}$ κόμβο. Η απόσταση που διανύει το κύμα ανάμεσα στους δύο κόμβους υπολογίζεται από την διαίρεση της διαφοράς των χρόνων άφιξης του μετώπου κύματος στους δύο αισθητήρες με την ταχύτητα του ήχου.

6.4.3 Πακέτα ασύρματης επικοινωνίας

Όπως περιγράφτηκε αναλυτικά παραπάνω, η αποτελεσματική εκτέλεση των διαδικασιών για τον συγχρονισμό των κόμβων και τον εντοπισμό των απειλών προϋποθέτει την ασύρματη επικοινωνία ανάμεσα στους κόμβους. Τα πακέτα που ανταλλάσσονται ανάμεσα στους κόμβους περιέχουν χρήσιμα δεδομένα για την εκτέλεση των αλγορίθμων. Το μέγεθός τους πρέπει να είναι το βέλτιστο καθώς η ασύρματη αποστολή τους επηρεάζει σημαντικά την κατανάλωση ενέργειας των ασύρματων κόμβων.

Τα πακέτα δεδομένων που χρησιμοποιούνται από το ασύρματο δίκτυο καταγραφής των ακουστικών κυμάτων και ανίχνευσης απειλών, είναι τα παρακάτω:

- **SynchMsg –** αποστέλλεται από σταθμό βάσης προς όλους του κόμβους του δικτύου που έχουν σαν αρμοδιότητα να καταγράφουν τα ακουστικά κύματα. Επιπλέον, με σκοπό την μείωση της κατανάλωσης ενέργειας του κόμβου μέσω της μείωσης του πλήθους μηνυμάτων, το μήνυμα αυτό χρησιμοποιείται για την αποστολή της τρέχον ταχύτητας του ανέμου από τον σταθμό βάσης προς τους κόμβους.
- **TimestampMsg** - περιέχει την χρονοσφραγίδα λήψης των **μηνυμάτων συγχρονισμού** από τους ασύρματους κόμβους καταγραφής των ακουστικών κυμάτων. Το μήνυμα αυτό αποστέλλεται από τους κόμβους του δικτύου προς τον σταθμό βάσης μετά την λήψη από αυτούς του **μηνύματος συγχρονισμού.**
- **EventMsg –** Χρησιμοποιείται από τους ασύρματους κόμβους καταγραφής ακουστικών κυμάτων προκειμένου να ενημερώσουν τον σταθμό βάσης για την πιθανή ύπαρξη μιας απειλής. Στέλνεται όταν κάποιος κόμβος εντοπίσει μια απειλή. Περιέχει πληροφορίες οι οποίες είναι χρήσιμες για τον υπολογισμό της θέσης της απειλής.

Εικόνα 63: Τα μηνύματα που ανταλλάσσονται κατά την διάρκεια εκτέλεσης της μεθόδου εντοπισμού απειλής ανάμεσα στον σταθμό βάσης και στους ασύρματους κόμβους του δικτύου καταγραφής ακουστικών κυμάτων.

Κάθε πακέτο περιέχει τη μεταβλητή ***roundNum***. Η συγκεκριμένη μεταβλητή αποθηκεύει έναν αριθμό ο οποίος αντιστοιχεί στον αύξοντα αριθμό του γύρου συγχρονισμού και καταγραφής των ακουστικών κυμάτων από τους ασύρματους κόμβους. Όπως είδαμε παραπάνω, οι κόμβοι του δικτύου μετά τα στάδια αρχικοποίησης τους μεταβαίνουν περιοδικά σε έναν κύκλο καταστάσεων λειτουργίας. Η μεταβλητη ***roundNum*** περιέχει το αύξοντα αριθμό του τρέχον κύκλου καταστάσεων λειτουργίας του κάθε κόμβου.

Τα πακέτα δεδομένων που χρησιμοποιούνται από το ασύρματο δίκτυο καταγραφής των περιβαλλοντικών δεδομένων και της θέσης των κόμβων, είναι τα παρακάτω:

- **EnvironmentalMsg –** περιέχει τις τελευταίες περιβαλλοντικές μετρήσεις του κάθε κόμβου του δικτύου. Αποστέλλονται από τους κόμβους προς τον σταθμό βάσης.
- **WindMsg -** περιέχει τις τελευταίες καταγραφές σχετικά με την ταχύτητα και την κατεύθυνση του ανέμου. Αποστέλλονται από τον ειδικό κόμβο που έχει ενσωματωμένο το ανεμόμετρο προς τον σταθμό βάσης.
- **GPSMsg –** περιέχει δεδομένα για τον προσδιορισμό της θέσης του κάθε κόμβου. Αποστέλλονται από τους κόμβους προς τον σταθμό βάσης.

Εικόνα 64: Η μορφή των μηνυμάτων που στέλνονται από το δίκτυο αισθητήρων καταγραφής περιβαλλοντικών δεδομένων προς τον σταθμό βάσης.

6.5 *Ανάλυση κατανάλωσης ενέργειας*

6.5.1 Το δίκτυο καταγραφής των ακουστικών κυμάτων.

Όπως έχουμε αναφέρει και παραπάνω, ένα από τους σημαντικότερους περιορισμούς που εισάγει η χρήση των ασύρματων δικτύων αισθητήρων είναι η περιορισμένη διαθεσιμότητα πόρων που έχουν. Για παράδειγμα, οι ασύρματοι κόμβοι συνήθως χρησιμοποιούν ενεργειακούς συσσωρευτές προκειμένου να έχουν αποθηκευμένη την ενέργεια που πρόκειται να καταναλώσουν. Η περιορισμένη ενεργειακή χωρητικότητα των συσσωρευτών αναγκάζει του κόμβους να χρησιμοποιούν με έναν ενεργειακά βέλτιστο τρόπο τα υποσυστήματα τους. Η ενεργειακή πολιτική που υλοποιεί κάθε ασύρματος κόμβος καθορίζει σε μεγάλο βαθμό την διάρκεια ζωής/λειτουργίας του ίδιου του κόμβου και κατ'επέκταση ολόκληρου του ασύρματου δικτύου αισθητήρων.

Η αποτελεσματικότητα της μεθόδου εντοπισμού απειλών που περιγράφουμε εξαρτάται σε μεγάλο βαθμό από την διάρκεια λειτουργίας των κόμβων που χρησιμοποιούνται. Αυτό οφείλεται στο γεγονός ότι πολλές φορές τα υποσυστήματα ενός συστήματος παρακολούθησης πρέπει να βρίσκονται σε λειτουργία για αρκετές ημέρες χωρίς την δυνατότητα αντικατάστασης νέων συσσωρευτών ενέργειας. Παρακάτω παρουσιάζεται μια ανάλυση της κατανάλωσης ενέργειας των κόμβων που υλοποιούν την παραπάνω μέθοδο εντοπισμού. Τέλος γίνεται μια εκτίμηση της πιθανής διάρκεια λειτουργίας των κόμβων άρα και ολόκληρου του συστήματος.

Σύμφωνα με τον πίνακα 7, η κατανάλωση ενέργειας του κόμβου Mica2 στην κατάσταση πλήρους λειτουργίας είναι 117mW. Η συγκεκριμένη κατανάλωση ενέργειας ισοδυναμεί σε $\frac{117mW}{3.3V} = 39mA$. Επιπλέον σημαντικό ποσοστό ενέργειας καταναλώνεται και από την πλακέτα αισθητήρων MTS310 και συγκεκριμένα τον ακουστικό αισθητήρα που έχει ενσωματωμένο. Αυτή η επιπλέον κατανάλωση ενέργειας είναι 0.813mA. Οι ενεργειακοί συσσωρευτές που χρησιμοποιούν οι κόμβοι Mica2 είναι τύπου AA και έχουν χωρητικότητα ίση με 2700mAh. Αυτή η ενεργειακή χωρητικότητα δίνει στον κόμβο την δυνατότητα συνεχούς λειτουργίας για $\frac{2700mAh}{39mA + 0.813mA} = 67.81$ώρες.

Όπως βλέπουμε, η διαθέσιμη ενέργεια που έχουν οι ασύρματοι κόμβοι όταν βρίσκονται σε κατάσταση πλήρους λειτουργίας επαρκεί για περίπου 3 ημέρες. Αυτή η διάρκεια λειτουργίας δεν μπορεί να χαρακτηριστεί ως ικανοποιητική για ένα σύστημα εντοπισμού απειλών. Έτσι παρακάτω γίνεται μια περιγραφή τεχνικών μείωσης της κατανάλωσης ενέργειας του κόμβου προκειμένου να βελτιώσουμε την διάρκεια ζωής του, προσφέροντας παράλληλα την επιθυμητή λειτουργικότητα.

Μια ολοκληρωμένη ενεργειακή πολιτική μπορεί να οδηγήσει σε σημαντική βελτίωση της διάρκεια λειτουργίας του κόμβου. Τα βασικά βήματα που πρέπει να υλοποιηθούν προκειμένου να μειωθεί αισθητά η κατανάλωση ενέργειας είναι:

- Να τροφοδοτούνται με ενέργεια μόνο τα υποσυστήματα του κόμβου που είναι απαραίτητα κάθε στιγμή. Προτείνεται δηλαδή, μια περιοδική απενεργοποίηση και ενεργοποίηση των υποσυστημάτων σύμφωνα με τις ανάγκες τις εφαρμογής. Με αυτό τον τρόπο, κάθε στιγμή θα γλυτώνουμε την περιττή κατανάλωση ενέργειας από υποσυστήματα που δεν εκτελούν κάποια απαραίτητη λειτουργία. Κατά την χρήση αυτής της προσέγγισης θα πρέπει να

δοθεί ιδιαίτερη προσοχή στους χρόνους ενεργοποίησης και απενεργοποίησης της κάθε συσκευής.

- Να μειωθεί η ασύρματη επικοινωνία. Σύμφωνα με έναν γενικό κανόνα, το 80 % της κατανάλωσης ενέργειας ενός κόμβου προέρχεται από την κατανάλωση του πομποδέκτη του. Έτσι η ελαχιστοποίηση της ασύρματης επικοινωνίας, μέσω της μείωσης του πλήθους και του μεγέθους των πακέτων επικοινωνίας τους κόμβου, επιφέρει σημαντική εξοικονόμηση ενέργειας.
- Η λειτουργία του μικρο-ελεγκτή σε όσο το δυνατόν χαμηλότερη κατάσταση κατανάλωσης ενέργειας. Ο μικρό-ελεγκτής θα πρέπει να βρίσκεται στην κανονική κατάσταση λειτουργίας του μόνο κατά την περίοδο όπου έχει να εκτελέσει κάποιους πολύπλοκούς υπολογισμούς. Σε διαφορετική περίπτωση, η μετάβασή του σε κάποια κατάσταση χαμηλής κατανάλωσης ενέργειας (σύμφωνα με τις απαιτήσεις της εφαρμογής) εξοικονομεί σημαντική ποσότητα ενέργειας.
- Η χρήση αλγορίθμων μικρής πολυπλοκότητας, προσαρμοσμένους για την εκτέλεσή τους σε 8-bit (είτε 16-bit) μικροελεγκτές.

Πρώτο βήμα για την υλοποίηση μια ολοκληρωμένης ενεργειακή πολιτικής είναι η ανάλυση των απαιτήσεων ενέργειας των κυριότερων λειτουργιών του κόμβου (Εικόνα 52).

Η ανάλυση του ενεργειακού κόστους της μεθόδου ανίχνευσης απειλών, που ακολουθεί, βασίστηκε στο περιβάλλον προσομοίωσης Avrora [95]. Συγκεκριμένα, το ενεργειακά μοντέλο που χρησιμοποιήθηκε φαίνεται στον παρακάτω πίνακα:

Πίνακας 16: Η κατανάλωση ενέργειας διάφορων υποσυστημάτων του κόμβου [94].

Κατάσταση Λειτουργίας Υποσυστήματος		**Κατανάλωση Ρεύματος (mA)**
CPU	**Idle**	3.3
	Active	7.6
	Sleep	0.24
Led		2.2
Πλακέτα Αισθητήρων – Μικρόφωνο Ενεργό		0.8
Πομποδέκτης	**Σε Κατάσταση Λήψης**	16.8
	Σε Κατάσταση Αποστολής	17.1

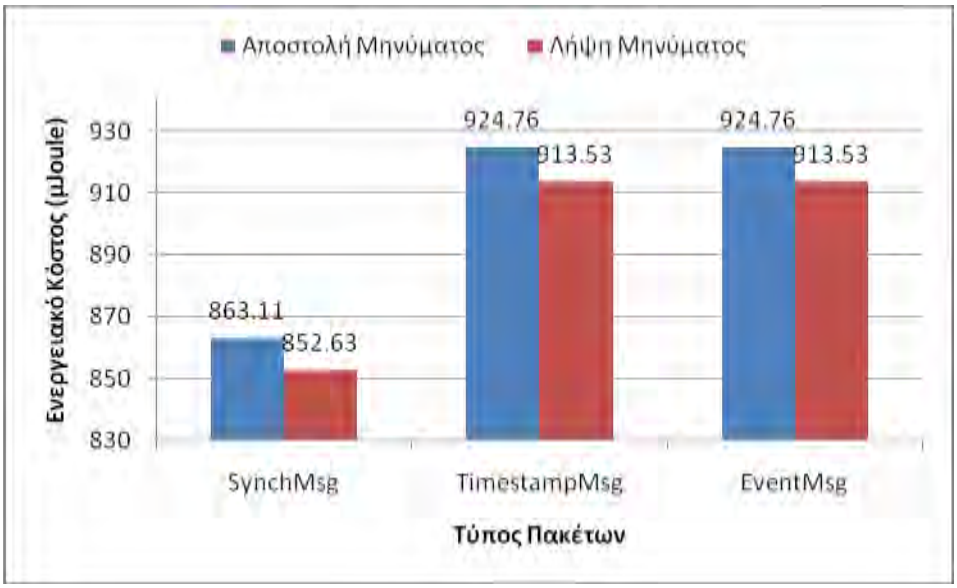
6.5.1.1 Ασύρματη λήψη – αποστολή πακέτων.

Κατά την διάρκεια λειτουργίας του, ο κάθε ασύρματος κόμβο ανταλλάσει με το σταθμό βάσης 3 διαφορετικά είδη πακέτων. Τα αποτελέσματα φαίνονται στον παρακάτω πίνακα:

Πίνακας 17: Ενεργειακή κατανάλωση των 3 πακέτων επικοινωνίας

Πακέτο	Μέγεθος Πακέτου	Ενεργειακό Κόστος Λήψης Πακέτου (μJoule)			Ενεργειακό Κόστος Αποστολής Πακέτου (μJoule)		
		Μικρο-ελεγκτή	Πομποδέκτης	Σύνολο	Μικρο-ελεγκτή	Πομποδέκτης	Σύνολο
SynchMsg	28 byte (22 βοηθητικά + 6 δεδομένων)	265.57	587.05	852.63	265.57	597.54	863.11
Timestamp Msg	30 byte (22 βοηθητικά + 8 δεδομένων)	284.54	628.9	913.53	284.54	640.2	924.76
EventMsg	30 byte (22 βοηθητικά + 8 δεδομένων)	284.544	628.992	913.53	284.544	640.224	924.76

Στην παρακάτω Εικόνα απεικονίζεται το ενεργειακό κόστος αποστολής και λήψης των τριών πακέτων.



Εικόνα 65: Το ενεργειακό κόστος για την αποστολή και την λήψη των τριών τύπων μηνυμάτων

Όπως αναφέρθηκε σε προηγούμενη ενότητα (Ενότητα 6.3.3), ένα προτεινόμενο επίπεδο κατωφλίου που αντιστοιχεί στην ταχύτητα του ανέμου αποστέλλεται από τον σταθμό βάσης προς τους ασύρματους κόμβους με την χρήση του μηνύματος SynchMsg. Δηλαδή, μέσα στα δεδομένα του μηνύματος SynchMsg εμφωλεύεται και μια επιπλέον μεταβλητή, μεγέθους 2 byte, η οποία περιέχει την προτεινόμενη (βάση της τρέχον ταχύτητας του ανέμου) στάθμη κατωφλίου.

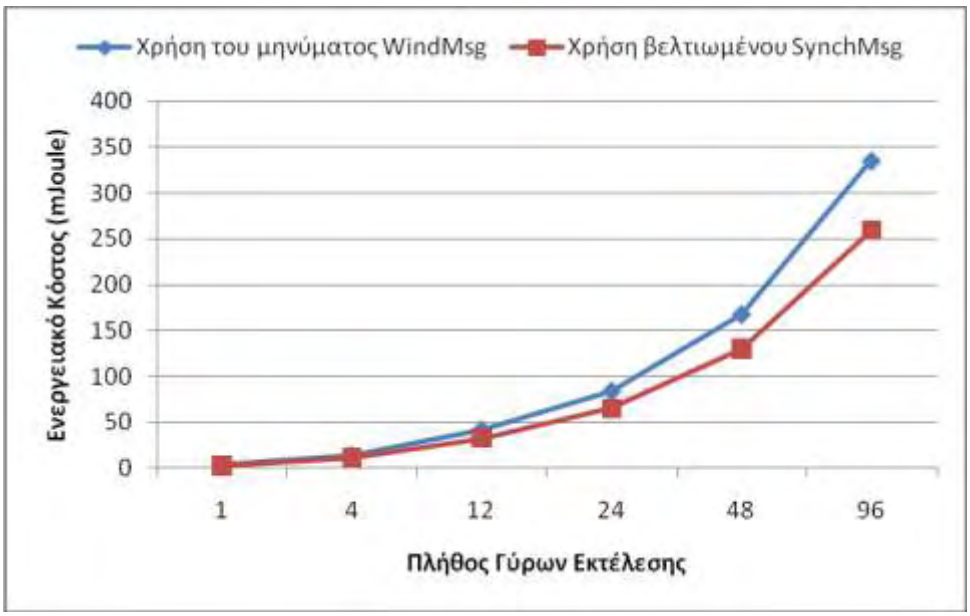
Ο λόγος που χρησιμοποιήθηκε αυτή η ενσωμάτωση των δεδομένων σε ένα κοινό πακέτο είναι η εξοικονόμηση ενέργειας που επιτυγχάνεται με την μείωση του πλήθους των ανταλλασσόμενων μηνυμάτων. Ο παρακάτω πίνακας απεικονίζει την κατανάλωση ενέργειας που έχουν οι κόμβοι στην περίπτωση χρήση ενός κοινού και μη-κοινού μηνύματος για την αποστολή των παραπάνω δεδομένων. (δεδομένα για τον συγχρονισμό + προτεινόμενο κατώφλι)

Πίνακας 18: Κατανάλωση ενέργειας των κόμβων στην περίπτωση χρήση ενός κοινού και μη-κοινού μηνύματος για την αποστολή των δεδομένων.

					Ενεργειακό κόστος ενός γύρου ανίχνευσης με την χρήση των μηνυμάτων	
Μήνυμα	**Λειτουργία**	**Μέγεθος μηνύματος**	**Ενεργειακό Κόστος (μJoule)**		**WindMsg και απλού SynchMsg**	**Βελτιωμένου SynchMsg**
Απλό SynchMsg	Αποστολή	26 byte (22βοηθητικά + 4 δεδομένων)	801.46			
	Λήψη		791.73		1 * 791.73	
SynchMsg + προτεινόμενο κατώφλι	Αποστολή	28 byte (22βοηθητικά + 6 δεδομένων)	863.11			
	Λήψη		852.63			1 * 852.63
TimestampMsg	Αποστολή	30 byte (22βοηθητικά + 8 δεδομένων)	924.76		1 * 924.76	1 * 924.76
	Λήψη		913.53			
EventMsg	Αποστολή	30 byte (22βοηθητικά + 8 δεδομένων)	924.76		1 * 924.76	1 * 924.76
	Λήψη		913.53			
WindMsg	Αποστολή	28 byte (22βοηθητικά + 6 δεδομένων)	863.11			
	Λήψη		852.63		1 * 852.63	
			Σύνολο		3493.88	2702.15

Στον παραπάνω πίνακα, πεδίο με όνομα «Απλό SynchMsg» αναφέρεται σε μήνυμα τύπου SynchMsg το οποίο δεν φέρει κανένα επιπλέον δεδομένο εκτός από αυτά του συγχρονισμού. Αντίθετα το πεδίο με όνομα «SynchMsg + προτεινόμενο κατώφλι» αναφέρεται σε μήνυμα τύπου SynchMsg στο οποίο όμως έχει προστεθεί και μια μεταβλητή με το προτεινόμενο κατώφλι. Τέλος, το πεδίο με όνομα «WindMsg» αναφέρεται σε ένα μήνυμα το οποίο περιέχει μια μεταβλητή με το προτεινόμενο κατώφλι. Το συγκεκριμένο μήνυμα είναι χρήσιμο μόνο στην περίπτωση όπου δεν χρησιμοποιηθεί η βελτιωμένη έκδοση του μηνύματος SynchMsg. Τα πεδία του συγκεκριμένου μηνύματος είναι: το NodeId (2 byte), το roundNum (2 byte), το propThresh (2 byte).

Η βελτίωση που προσφέρει η χρήση του βελτιωμένου μηνύματος SynchMsg στη κατανάλωση ενέργειας είναι ~ 25%. Η παραπάνω κατανάλωση ενέργειας προέρχεται μόνο από την αποστολή και λήψη μηνυμάτων για ένα γύρο εκτέλεσης της μεθόδου ανίχνευσης. Προκειμένου να υπολογίσουμε την μέγιστη κατανάλωσης ενέργειας για έναν γύρο υποθέτουμε ότι κατά την διάρκεια γίνεται ανίχνευση μιας απειλής, οπότε και στέλνεται ένα μήνυμα τύπου EventMsg. Η Εικόνα 66 απεικονίζει την ενέργεια που καταναλώνουν οι δύο διαφορετικές πολιτικές διαχείρισης των μηνυμάτων κατά την διάρκεια περισσότερων του ενός γύρους εκτέλεσης.



Εικόνα 66:Το ενεργειακό κόστος της χρήσης ή μη, βελτιωμένης πολιτικής διαχείρισης των μηνυμάτων συνάρτηση των γύρων εκτέλεσης της μεθόδου ανίχνευσης.

6.5.1.2 Καταγραφή χρονοσφραγίδας και αποστολή στον σταθμό βάσης

Κατά την διάρκεια της κατάστασης λειτουργίας "*Καταγραφή χρονοσφραγίδας και αποστολή στον σταθμό βάσης*" ο κόμβος καταγράφει την χρονοσφραγίδα του ληφθέντος μηνύματος SynchMsg. Στην συνέχεια αναλαμβάνει να στείλει ένα μήνυμα τύπου TimestampMsg προς τον σταθμό βάσης, το οποίο θα περιέχει την καταγεγραμμένη χρονοσφραγίδα.

Ο χρόνος που χρειάζεται η εκτέλεση της καταγραφής της χρονοσφραγίδας του μηνύματος υπολογίσθηκε από το περιβάλλον προσημείωσης Avrora στα 40μs. Ο χρόνος

αποστολής του μηνύματος TimestampMsg υπολογίσθηκε στα 12,5 msec. Παρόλα αυτά, η χρονική διάρκεια της κατάστασης τίθεται στα 5 sec. Αυτό οφείλεται στο γεγονός ότι το ασύρματο δίκτυο αποτελείται από πολλούς κόμβους οι οποίοι θα βρίσκονται όλοι στην παρόμοια κατάσταση. Έτσι στην περίπτωση όπου θελήσουν όλοι ταυτόχρονα να στείλουν το πακέτο TimestampMsg στο σταθμό βάσης, θα προκληθεί μεγάλο πλήθος συγκρούσεων στα πακέτα, με αποτέλεσμα την μη-επιτυχή παράδοσή τους.

Για την επίλυση των συγκρούσεων χρησιμοποιείτε ένα απλό πρωτόκολλο επίλυσης. Σύμφωνα με το πρωτόκολλο αυτό, ο κάθε κόμβος δεν στέλνει απευθείας το πακέτο του στον σταθμό βάσης, αλλά περιμένει για ένα τυχαίο χρονικό διάστημα. Το μέγιστο χρονικό διάστημα που θα μπορεί να περιμένει ο κάθε κόμβος είναι ~5 sec. Το διάστημα των 5 sec θεωρείται αρκετά μεγάλο, αλλά έχει ορισθεί με γνώμονα την ύπαρξη μεγάλου πλήθους ασύρματων κόμβων και την ελαχιστοποίηση της πιθανότητας δύο κόμβοι να χρησιμοποιήσουν την ίδια τυχαία τιμή.

Ο παρακάτω πίνακας περιέχει τους χρόνους λειτουργίας και το ενεργειακό κόστος της κάθε επιμέρους λειτουργίας της κατάστασης.

Πίνακας 19: Ενεργειακό κόστος για κάθε επιμέρους λειτουργία της κατάστασης

Κατάσταση Λειτουργίας Υποσυστήματος	**Χρόνος Λειτουργίας (msec)**	**Ενεργειακό κόστος (μAs)**
Καταγραφή Χρονοσφραγίδας	0.04	7.6 mA * 0.04 ms= 0.304
Πομποδέκτης σε λειτουργία ληψης	5000 – 12.5 = 4987.5	16.8mA * 4987.5 ms = 83790
Αποστολή Μηνύματος TimestampMsg	12,5	308
Cpu Active	5000	7.6mA * 5000 ms = 38000
	Σύνολο	122098

Οι τιμές που περιγράφονται στον παραπάνω πίνακα εμφανίζονται στην ιδανική περίπτωση όπου το δίκτυο αποτελείται μόνο από έναν ασύρματο κόμβο. Σε πραγματικές συνθήκες, όπου το πλήθος των ασύρματων κόμβων είναι μερικές δεκάδες οι τιμές αυτές είναι αρκετά μεγαλύτερες. Αυτό οφείλεται στην broadcast φύση της ασύρματης επικοινωνίας. Στην περίπτωση δηλαδή, όπου κάποιος κόμβος στείλει ένα μήνυμα στο σταθμό βάσης, αυτό θα φτάσει και σε όλους τους υπόλοιπους κόμβους του δικτύου που βρίσκονται εντός της εμβέλειάς του. Αυτές οι παρεμβολές που εμφανίζονται στους κόμβους από την λήψη «ξένων» πακέτων προκαλούν μεγάλη κατανάλωση ενέργειας.

Μια βελτίωση στο συγκεκριμένο φαινόμενο είναι η απενεργοποίηση του πομποδέκτη κάθε κόμβου όταν αυτός δεν χρησιμοποιείται. Έτσι ο κόμβος αφού ολοκληρώσει την

καταγραφή της χρονοσφραγίδας και υπολογίσει την τυχαία καθυστέρηση αποστολής του μηνύματος, μπορεί να απενεργοποιήσει τον πομποδέκτη του. Ο πομποδέκτης θα ενεργοποιηθεί μόλις λίγα ms πριν την λήξη της καθυστέρησης αποστολής. Ο χρόνος που θα πρέπει να μεσολαβήσει ανάμεσα στην ενεργοποίηση του πομποδέκτη και στην αποστολή του πακέτου εξαρτάται αποκλειστικά από τον πομποδέκτη. Ο χρόνος αυτός ονομάζεται *χρόνος ενεργοποίησης* και στην συγκεκριμένη περίπτωση είναι 1.8 ms. Κατά το χρονικό διάστημα όπου βρίσκεται απενεργοποιημένος ο πομποδέκτης, ο μικρο-ελεγκτής βρίσκεται σε κατάσταση χαμηλής λειτουργίας (idle) εξοικονομώντας έτσι επιπλέον ενέργεια. Μετά την ολοκλήρωση της αποστολής του μηνύματος ο πομποδέκτης απενεργοποιείται ξανά μέχρι το τέλος της καταγραφής των ακουστικών κυμάτων και την ανίχνευση απειλής.

Παρακάτω εμφανίζεται ένας συγκριτικός πίνακας των δύο πολιτικών λειτουργίας του πομποδέκτη.

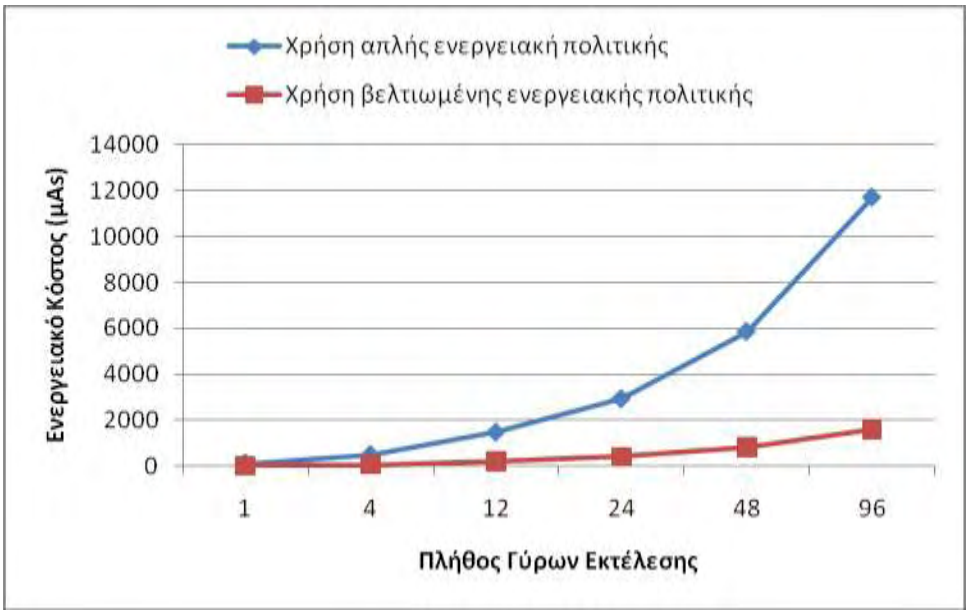
Πίνακας 20: Σύγκριση των 2 διαφορετικών ενεργειακών πολιτικών κατά την διάρκεια της κατάσταση λειτουργίας «*Καταγραφή χρονοσφραγίδας και αποστολή στον σταθμό βάσης*»

Λειτουργία	**Απλή Ενεργειακή Πολιτική**		**Βελτιωμένη Ενεργειακή Πολιτική**	
	Χρόνος (msec)	**Ενεργειακό Κόστος (μAs)**	**Χρόνος (msec)**	**Ενεργειακό Κόστος (μAs)**
Καταγραφή Χρονοσφραγίδας	0.04	7.6 mA * 0.04 ms= 0.304	0.04	7.6 mA * 0.04 ms= 0.304
Αποστολή Μηνύματος TimestampMsg	12,5	308	12,5	308
Πομποδέκτης σε λειτουργία λήψης	5000 – 12.5 = 4987.5	16.8mA * 4987.5 ms = 83790	0	0
Cpu Idle	0	0	(περίπτωση μέγιστης αναμονής για την αποστολή του μηνύματος) 5000 - 0.04- 12.5 - 1.8 -2 = 4985.66	4985.66 ms * 3.3 mA = 16452.678
Cpu Active	5000	7.6mA * 5000 ms = 38000	0.04 + 12.5 + 1.8 + 2= 14.34	13.34ms * 7.6 mA = 101.384
Σύνολο		122098		16862.366

Παρατηρώντας τις τιμές του παραπάνω πίνακα είναι εμφανές ότι υπάρχει μεγάλη βελτίωση στην περίπτωση εφαρμογής της βελτιωμένης ενεργειακής πολιτικής στην κατανάλωση του κόμβου. Το ποσοστό βελτίωσης είναι της τάξης του 85%.

Παρακάτω απεικονίζεται η βελτίωση της κατανάλωσης ενέργειας του κόμβου με την εφαρμογή της βελτιωμένης ενεργειακής πολιτικής για την συγκεκριμένη κατάσταση

λειτουργίας στην διάρκεια περισσότερων από 1 γύρους εκτέλεσης της μεθόδου ανίχνευσης.



Εικόνα 67: Σύγκριση των 2 διαφορετικών ενεργειακών πολιτικών κατά την διάρκεια της κατάσταση λειτουργίας «*Καταγραφή χρονοσφραγίδας και αποστολή στον σταθμό βάσης*» για διάρκεια λειτουργίας περισσότερων του ενός κύκλου εκτέλεσης της μεθόδου.

6.5.1.3 Κατάσταση υπολογισμού του κατωφλίου

Στην κατάσταση «*Υπολογισμού του κατωφλίου*» ο κόμβος χρησιμοποιεί των ακουστικό αισθητήρα προκειμένου να καταγράψει τα ακουστικά κύματα. Η καταγραφή διαρκεί για 15 sec και γίνεται με συχνότητα δειγματοληψίας τα 10 kHz. Μετά το πέρας αυτής της περιόδου ο κόμβος χρησιμοποιεί το μέγιστο επίπεδο έντασης που κατέγραψε και το προτεινόμενο κατώφλι που έλαβε από τον σταθμό βάσης. Το αποτέλεσμα του υπολογισμού είναι το κατώφλι που θα χρησιμοποιήσει η μέθοδος ανίχνευσης κατά τον τρέχον κύκλο εκτέλεσης.

Η λήψη του κάθε δείγματος διαρκεί 28 μsec, ενώ η χρονική διάρκεια ανάμεσα σε δύο δείγματα είναι 100 sec. Μετά την λήψη κάθε δείγματος, εκτελείται μια σειρά εντολών/ελέγχων από τον μικρο-ελεγκτή με σκοπό την επεξεργασία τους. Ο χρόνος εκτέλεσης αυτών των εντολών για κάθε δείγμα είναι 13 μsec. Τέλος ο υπολογισμός του κατωφλίου έχει διάρκεια 30μsec

Αξίζει να σημειωθεί ότι κατά την διάρκεια αυτής της κατάστασης, αλλά και την διάρκεια όλης της περιόδου καταγραφής για την ανίχνευση απειλής, ο πομποδέκτης των κόμβων παραμένει ανενεργός. Ο πομποδέκτης επανέρχεται σε κατάσταση αφύπνισης είτε στην περίπτωση εντοπισμού κάποιας απειλής, είτε μετά την ολοκλήρωση της περιόδου (T=15min) ανίχνευσης για τον εντοπισμό απειλών. Με αυτό τον τρόπο μειώνεται κατά πολύ η κατανάλωση ενέργειας κατά την διάρκεια αυτών των καταστάσεων.

Παρακάτω φαίνεται ο χρόνο εκτέλεσης κάθε επιμέρους λειτουργίας της κατάστασης καθώς και το αντίστοιχο ενεργειακό της κόστος.

Πίνακας 21: Ενεργειακό κόστος για κάθε επιμέρους λειτουργία της κατάστασης «Υπολογισμού του κατωφλίου»

Λειτουργία	Χρόνος (msec)	Ενεργειακό Κόστος (μAs)
Ακουστικός Αισθητήρας	15000	0.8 mA * 15000 ms= 12000
Λήψη δείγματος	0.028ms * 10 (δείγματα ανά msec) * 15000ms = 4200	7.6mA * 4200 ms = 31920
Έλεγχοι από την cpu μετά από κάθε δείγμα	0.013ms * 10 (δείγματα ανά ms) * 15000ms = 1950	7.6mA * 1950ms = 14,820
Τελικός υπολογισμός κατωφλίου	0.03ms	7.6mA * 0.03ms = 0.228
Cpu Idle	15000ms – 4200ms – 1950ms - 0.03ms = 8849	3.3mA * 8849ms = 29201
Σύνολο		87941.228

6.5.1.4 *Κατάσταση καταγραφής και ελέγχου ύπαρξης απειλών.*

Κατά την διάρκεια αυτής τη κατάστασης, ο κάθε κόμβος καταγράφει τα ακουστικά κύματα εκτελώντας δειγματοληψία στο ακουστικό τους αισθητήρα με συχνότητα 10kHz. Όπως και παραπάνω η λήψη του κάθε δείγματος διαρκεί 28 μsec, ενώ η χρονική διάρκεια ανάμεσα σε δύο δείγματα είναι 100 sec.

Μετά την λήψη κάθε δείγματος, ο μικρο-ελεγκτής ελέγχει το δείγμα για την υπέρβαση ή όχι της στάθμης του κατωφλίου. Η διάρκεια αυτού του ελέγχου είναι 15μsec για κάθε δείγμα .

Η διάρκεια της κατάσταση εξαρτάται από την ύπαρξη ή όχι απειλής. Στην περίπτωση μη εντοπισμού απειλής, η διάρκεια εκτίνεται στα 15 λεπτά. Με την ολοκλήρωση των 15 λεπτών, ο ακουστικός αισθητήρας απενεργοποιείται, ενεργοποιείται ο πομποδέκτης και ο κόμβος μεταβαίνει στην επόμενη κατάσταση. Αντίθετα, στην περίπτωση όπου γίνει εντοπισμός κάποιας απειλής, ο κόμβος υπολογίζει τον χρόνο άφιξης του ακουστικού κύματος στον κόμβο, απενεργοποιεί τον ακουστικό αισθητήρα, ενεργοποιεί τον πομποδέκτη, και στέλνει ένα πακέτο τύπου EventMsg στον σταθμό βάσης.

Στον υπολογισμό της συνολικής χρονικής διάρκεια της κατάστασης θα πρέπει να ληφθούν υπόψη:

- ο χρόνος που χρειάζεται ο μικρο-ελεγκτής να υπολογίσει τον χρόνος άφιξης του κύματος. Είναι 30 μsec.
- ο χρόνος δημιουργίας του πακέτου EventMsg. Υπολογίζεται στα 2.640μsec.
- ο χρόνος ενεργοποίησης του πομποδέκτη = 1.8 ms

- ο χρόνος για την αποφυγή των συγκρούσεων ανάμεσα στα μηνύματα διαφορετικών κόμβων. Όπως και πριν τίθεται ίσος με 5 sec.
- ο χρόνος που απαιτείται για την αποστολή του μηνύματος στον σταθμό βάσης. Υπολογίζεται στα 12.5 msec

Ο παρακάτω πίνακα περιγράφει αναλυτικά τους χρόνους εκτέλεσης και το ενεργειακό κόστος όλων των επιμέρους λειτουργιών της κατάστασης «καταγραφής και ανίχνευση απειλών». Συγκεκριμένα παρουσιάζεται το ενεργειακό κόστος εκτέλεσης της κατάσταση στην περίπτωση χρήσης

- μιας βασικής ενεργειακής πολιτικής όπου ο πομποδέκτης του κόμβου παραμένει ενεργός καθόλη την διάρκεια εκτέλεσής της
- μιας βελτιωμένης ενεργειακής πολιτικής όπου ο πομποδέκτης του κόμβου είναι ανενεργός κατά την μεγαλύτερη διάρκεια της κατάστασης. Τα βήματα που ακολουθούνται σε αυτή την περίπτωση περιγράφονται παραπάνω.

Η διάρκεια εκτέλεσης κατάσταση, εξαρτάται σε μεγάλο βαθμό από τον εντοπισμό ή όχι κάποιας απειλής. Έτσι , στον παρακάτω πίνακα παρουσιάζεται αναλυτική περιγραφή για δύο χρονικές διάρκεια της κατάστασης.

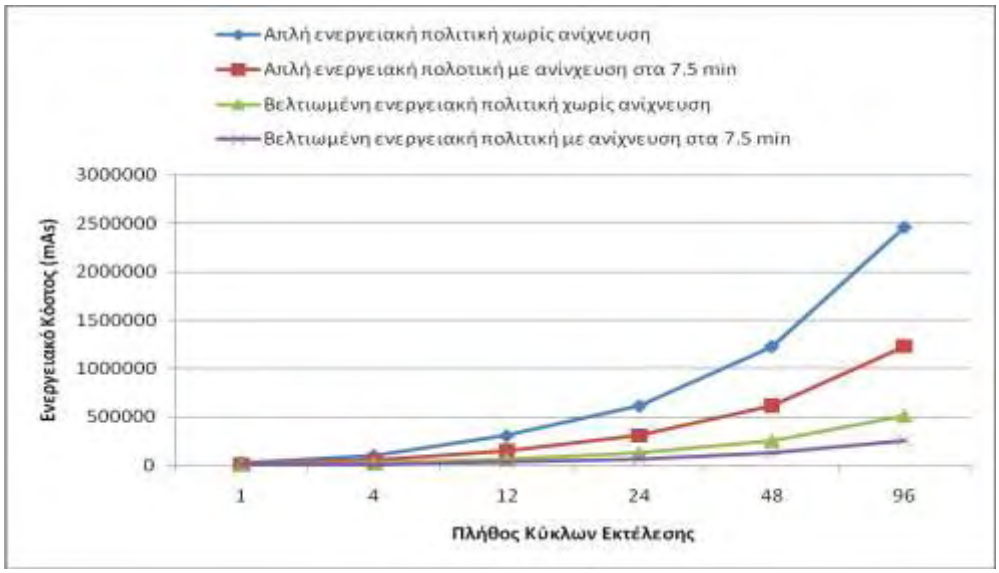
1. Την περίπτωση όπου δεν εντοπίζεται κάποια απειλή. Η διάρκεια εκτέλεσης είναι T = 15 min.
2. Την περίπτωση όπου εντοπίζεται κάποια απειλή, οπότε και εκτελούνται τα απαραίτητα βήματα υπολογισμού του χρόνου άφιξης του κύματος της. Σαν στιγμή εντοπισμού της απειλής χρησιμοποιήθηκε η μέση χρονική διάρκεια εκτέλεσης της κατάστασης 15/2 = 7.5 min.

Παρατηρώντας τις τιμές του παρακάτω πίνακα είναι εμφανές ότι υπάρχει μεγάλη βελτίωση στην περίπτωση εφαρμογής της βελτιωμένης ενεργειακής πολιτικής στην κατανάλωση του κόμβου. Το ποσοστό βελτίωσης είναι της τάξης του 80%.

Στην Εικόνα 68 απεικονίζεται η βελτίωση της κατανάλωσης ενέργειας του κόμβου με την εφαρμογή της βελτιωμένης ενεργειακής πολιτικής για την συγκεκριμένη κατάσταση λειτουργίας στην διάρκεια περισσότερων από 1 γύρους εκτέλεσης της μεθόδου ανίχνευσης. Απεικονίζεται η κατανάλωση ενέργεια της κατάστασης στην περίπτωση μη εντοπισμού και εντοπισμού απειλής κάθε 7.5 min.

Πίνακας 22: Ενεργειακό κόστος της των επιμέρους λειτουργιών της κατάστασης «Καταγραφής ακουστικών κυμάτων και ανίχνευσης απειλών»

	Χρήση απλής ενεργειακής πολιτικής				**Χρήση βελτιωμένης ενεργειακής πολιτικής**			
	Μη ανίχνευση απειλής για T=15 min		**Ανίχνευση απειλής μετά από 7.5 min**		**Μη ανίχνευση απειλής για T=15 min**		**Ανίχνευση απειλής μετά από 7.5 min**	
Λειτουργία	**Χρόνος (sec)**	**Ενεργειακό Κόστος (mAs)**	**Χρόνος (sec)**	**Ενεργειακό Κόστος (mAs)**	**Χρόνος (sec)**	**Ενεργειακό Κόστος (mAs)**	**Χρόνος (sec)**	**Ενεργειακό Κόστος (mAs)**
Ακουστικός Αισθητήρας	**900**	0.8 mA * 900s = **720**	**450**	0.8 mA * 450s = **360**	**900**	0.8 mA * 900s = **720**	**450**	0.8 mA * 450s = **360**
Λήψη δείγματος	0.028ms * 10 (δείγματα ανά msec) * 900000ms = **252**	7.6mA * 252s = **1915**	0.028ms * 10 (δείγματα ανά msec) * 450000ms = **126**	7.6mA * 126s = **957.6**	0.028ms * 10 (δείγματα ανά msec) * 900000ms = **252**	7.6mA * 252s = **1915**	0.028ms * 10 (δείγματα ανά msec) * 450000ms = **126**	7.6mA * 126s = **957.6**
Έλεγχοι από την cpu μετά από κάθε δείγμα	0.015ms * 10 (δείγματα ανά ms) * 900000ms = **135**	7.6mA * 135s = **1026**	0.015ms * 10 (δείγματα ανά ms) * 450000ms = **67.5**	7.6mA * 67.5s = **513**	0.015ms * 10 (δείγματα ανά ms) * 900000ms = **135**	7.6mA * 135s = **1026**	0.015ms * 10 (δείγματα ανά ms) * 450000ms = **67.5**	7.6mA * 67.5s = **513**
Υπολογισμό χρόνου άφιξης του κύματος	**0**	**0**	**0.00003**	7.6mA * 0.00003s = **0.000228**	**0**	**0**	**0.00003**	7.6mA * 0.00003s = **0.000228**
Ενεργοποίηση πομποδέκτη	**0**	**0**	**0**	**0**	**0.0018**	7.6mA * 0.0018s = **0.01368**	**0.0018**	7.6mA * 0.0018s = **0.01368**
Προετοιμασία μηνύματος EventMsg	**0**	**0**	**0.00264**	7.6mA * 0.00264s = **0.020064**	**0**	**0**	**0.00264**	7.6mA * 0.00264s = **0.020064**
Αναμονή αποστολής μηνύματος	**0**	**0**	(περίπτωση μέγιστης αναμονής για την αποστολή του μηνύματος) 5s - 0.0018s – 0.00264s = **4.99556**	3.3mA * 4.99556s = **16.485348**	**0**	**0**	(περίπτωση μέγιστης αναμονής για την αποστολή του μηνύματος) 5s - 0.0018s – 0.00264s = **4.99556**	3.3mA * 4.99556s = **16.485348**
Αποστολή μηνύματος	**0**	**0**	**0.0125**	**0.308**	**0**	**0**	**0.0125**	**0.308**
Πομποδέκτης και cpu σε λειτουργία λήψης	**900**	(7.6mA + 16.8mA) * 900s = **21960**	**450**	(7.6mA + 16.8mA) * 450s = **10980**	**0**	**0**	**0**	**0**
Cpu Idle	**0**	**0**	**0**	**0**	900s – 252s – 135s - 0.0018s = **512.99**	3.3mA * 512.99s = **1692**	450s – 126s– 67.5s = **256.5**	3.3mA * 256,5s = **846,45**
Σύνολο		25621		12827.4		5353		2693.8



Εικόνα 68:Το ενεργειακό κόστος της κατάστασης «*Καταγραφής ακουστικών κυμάτων και ανίχνευση απειλής*» για την περίπτωση χρήση 2 διαφορετικών ενεργειακών πολιτικών καθώς και την περίπτωση ανίχνευσης ή όχι απειλών

6.5.1.5 *Συνολική κατανάλωση ενέργειας της μεθόδου ανίχνευσης*

Όπως αναλύσαμε διεξοδικά παραπάνω, η μέθοδος ανίχνευσης απειλών αποτελείται από ένα σύνολο καταστάσεων. Στις προηγούμενες παραγράφους έγινε μια σύντομη ανάλυση της ενέργειας που καταναλώνει κάθε επιμέρους κατάσταση κατά την εκτέλεσή της. Το σύνολο αυτών των επιμέρους ενεργειακών κοστών αποτελεί τις συνολικές απαιτήσεις ενέργειας που έχει η μέθοδος ανίχνευσης.

Ο Πίνακα 23 παρουσιάζει το ενεργειακό κόστος κάθε επιμέρους κατάστασης καθώς και της μεθόδου συνολικά. Ακόμα παρουσιάζονται τα ποσοστά, με τα οποία συμμετέχει το κάθε υποσύστημα, στη συνολική κατανάλωση.

Το συνολικό ενεργειακό κόστος το οποίο καταναλώνει η μέθοδος ανίχνευσης κατά τη εκτέλεση ενός κύκλου εκτέλεσης είναι

- **5458mAs** για την περίπτωση μη ανίχνευσης απειλής
- **2798mAs** για την περίπτωση ανίχνευσης απειλής στα 7.5 sec.

Έτσι για την περίπτωση όπου δεν εντοπισθεί καμία απειλή η διάρκεια λειτουργίας των κόμβων χρησιμοποιώντας μια μπαταρία χωρητικότητας 2700mAh είναι:

Ενεργειακό κόστος ανά γύρο εκτέλεσης :

$$5458\text{mAs} = 1.516\,\text{mAh}$$

Μέγιστος δυνατός αριθμός κύκλων εκτέλεσης :

$$\frac{2700mAh}{1.516mAh} = 1781\,\text{αριθμός κύκλων εκτέλεσης}$$

Μέγιστη χρονική διάρκεια εκτέλεσης μεθόδου εντοπισμού απειλών (Λαμβάνοντας υπόψη ότι η διάρκεια εκτέλεσης ενός κύκλου εκτέλεσης χωρίς την ύπαρξη απειλών είναι ~15.5min**):**

$$\frac{1781*15.5}{60*24} = 19.1\,\text{ημέρες}$$

Σε μια ακραία περίπτωση, όπου γίνεται εντοπισμός απειλών σε κάθε κύκλο εκτέλεσης στα 7.5 λεπτά κάθε κύκλου η διάρκεια λειτουργίας των κόμβων χρησιμοποιώντας μπαταρίες χωρητικότητας 2700mAh είναι:

Ενεργειακό κόστος ανά γύρο εκτέλεσης :

$$2795\text{mAs} = 0.776\,\text{mAh}$$

Μέγιστος δυνατός αριθμός κύκλων εκτέλεσης :

$$\frac{2700mAh}{0.776mAh} = 3479\,\text{αριθμός κύκλων εκτέλεσης}$$

Μέγιστη χρονική διάρκεια εκτέλεσης μεθόδου εντοπισμού απειλών (Λαμβάνοντας υπόψη ότι η διάρκεια εκτέλεσης ενός κύκλου εκτέλεσης με την ανίχνευση απειλών στα 7.5 min είναι ~8min**):**

$$\frac{3479*8}{60*24} = 19.3\,\text{ημέρες}$$

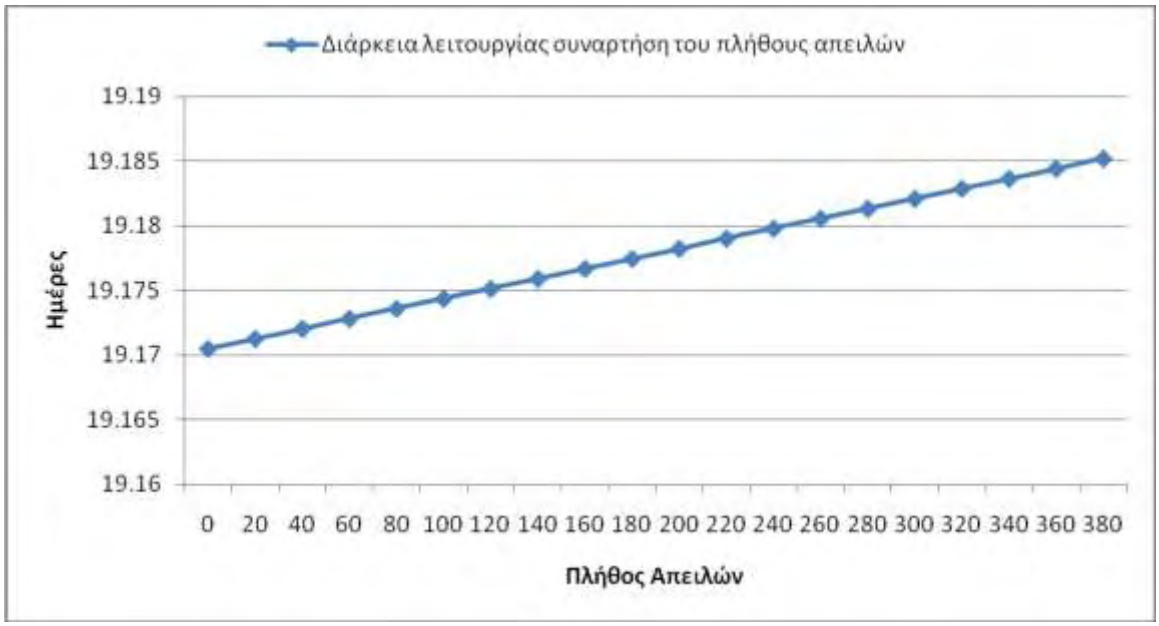
Παρατηρώντας την μέγιστη διάρκεια εκτέλεσης της μεθόδου εντοπισμού απειλών στην περίπτωση ύπαρξης ή όχι απειλών, γίνεται εύκολα αντιληπτό ότι η χρήση βελτιωμένων ενεργειακών πολιτικών έχει ως αποτέλεσμα την μείωση της συνολικής κατανάλωσης ενέργειας της μεθόδου. Αυτή η μείωση της κατανάλωσης έχει ως αποτέλεσμα την αύξηση της διάρκειας λειτουργίας των κόμβων κατά ~85%.

Αξίζει να παρατηρήσουμε ότι όσο αυξάνει ο αριθμός των ανιχνεύσεων αυξάνεται και η μέγιστη διάρκεια λειτουργίας των κόμβων του δικτύου (Εικόνα 70).

Πίνακας 23: Το ενεργειακό κόστος κάθε επιμέρους κατάστασης και της μεθόδου συνολικά, χρησιμοποιώντας μια βελτιωμένη ενεργειακή πολιτική.

	Μη ανίχνευση απειλής για T=15 min		**Ανίχνευση απειλής μετά από 7.5 min**	
Κατάσταση	**Ενεργειακό Κόστος (mAs)**	**% Ποσοστό συνολικού ενεργειακού κόστους**	**Ενεργειακό Κόστος (mAs)**	**% Ποσοστό συνολικού ενεργειακού κόστους**
Λήψη μηνύματος Συγχρονισμού	0.284	0.005	0.284	0.01
Καταγραφή χρονοσφραγίδας και αποστολή στον σταθμό βάσης	16.862	0.308	16.862	0.6
Υπολογισμού του κατωφλίου	87.941	1.611	87.941	3.15
Καταγραφής ακουστικών κυμάτων και ανίχνευσης απειλών	5353	98.076	2693	96.24
Σύνολο	**5458**	**100 %**	**2798**	**100 %**

Εικόνα 69: Ποσοστιαία συμμετοχή του κάθε επιμέρους κατάστασης λειτουργίας στην κατανάλωση ενέργειας



Εικόνα 70: Διάρκεια λειτουργίας κόμβων συναρτήσει του πλήθους απειλών που ανιχνεύουν.

6.5.2 Το δίκτυο καταγραφής των περιβαλλοντικών συνθηκών

Το δίκτυο καταγραφής των περιβαλλοντικών συνθηκών έχει κυρίως βοηθητική λειτουργία στην μέθοδο ανίχνευσης. Περιοδικά εφοδιάζει με τα δεδομένα σχετικά με το περιβάλλον τις μεθόδους υπολογισμού της θέσης της απειλής. Επομένως, η φύση της λειτουργίας του δικτύου αυτού δεν θέτει την ανάγκη ανάπτυξης και χρήσης μια εξειδικευμένης ενεργειακής πολιτικής για τους κόμβους. Επιπλέον, οι κόμβοι που απαρτίζουν το συγκεκριμένο δίκτυο αισθητήρων είναι οι iSense. Οι κόμβοι αυτοί διακρίνονται για τις πολύ χαμηλές απαιτήσεις ενέργειας που έχουν. Η κατανάλωσή του είναι μικρότερη σε ποσοστό ~50% σε σχέση με τους κόμβους Mica2 (Πίνακας 7).

Κατά την διάρκεια λειτουργίας τους, οι κόμβοι περιοδικά καταγράφουν τις απαραίτητες μετρήσεις (συνθήκες περιβάλλοντος, συνθήκες ανέμου και θέση κόμβου) και τις στέλνουν ασύρματα στον σταθμό βάσης. Οπότε, μια βασική πολιτική μείωσης της κατανάλωσης ενέργειάς του είναι ο μικρο-ελεγκτής και ο πομποδέκτης των κόμβων να λειτουργεί σε πλήρη ισχύ μόνο κατά την διάρκεια καταγραφής και αποστολής των δεδομένων. Κατά την διάρκεια της περιόδου που μεσολαβεί ανάμεσα σε δύο καταγραφές τα υποσυστήματα του κόμβου θα παραμένουν σε κατάσταση χαμηλής λειτουργίας.

Στην κατάσταση πλήρους λειτουργίας, η κατανάλωση το κόμβου είναι: $\frac{52.8mW}{3V} = 16mA$. Η ενσωμάτωση των διάφορων αισθητήριων οργάνων στον κόμβο ανεβάζει την κατανάλωση ενέργειάς του στα 17.4 mA. Οπότε με την χρήση των συσσωρευτών χωριτικότητας 2900mAh που χρησιμοποιούν οι συγκεκριμένοι κόμβοι, η διάρκεια συνεχούς λειτουργίας τους υπολογίζεται σε $\frac{2900mAh}{17.4mA} = 166$ ώρες, περίπου δηλαδή 7 ημέρες.

Η χρήση της απλής διαχείρισης των υποσυστημάτων των κόμβων που περιγράφτηκε παραπάνω μπορεί να οδηγήσει σε βελτίωση της κατανάλωσής τους κατά 90%, φτάνοντας σε διάρκεια λειτουργίας ~75 ημέρες

7 *Μέθοδος Χαρακτηρισμού Απειλών*

Η μέθοδος χαρακτηρισμού των απειλών μιας περιοχής επιτήρησης αφορά την εύρεση του είδους της απειλής. Η ανίχνευση του τύπου της απειλής επιτυγχάνεται μέσω της χρήσης ενός ασύρματου δικτύου αισθητήρων. Οι ασύρματοι αυτοί κόμβοι έχουν ενσωματωμένους ακουστικούς αισθητήρες οι οποίοι καταγράφουν τα ακουστικά κύματα που παράγει οι απειλή. Επεξεργάζοντας αυτά τα κύματα, η μέθοδος χαρακτηρισμού έχει την δυνατότητα να αναγνωρίσει τον τύπο της απειλής.

Η μέθοδος επεξεργασίας και ανάλυσης των κυμάτων προκειμένου να αναγνωριστεί ο τύπος της απειλής αποτελείται από 3 βασικά βήματα:

1. Δειγματοληψία: Συλλογή των ακουστικών κυμάτων που περιγράφουν τον τύπου της απειλής. Σε πολλές περιπτώσεις εκτελείται ένα είδος πρώιμης επεξεργασίας προκειμένου να μειωθεί ο θόρυβος του περιβάλλοντος από τα αυτά.
2. Εξαγωγή χαρακτηριστικών: Τα κύματα που συλλέχτηκαν, επεξεργάζονται προκειμένου να εξαχθούν οι ιδιότητές τους. Οι χαρακτηριστικές αυτές ιδιότητες συλλέγονται σε ένα διάνυσμα το οποίο αντιπροσωπεύει τον τύπο της απειλής που έχει καταγραφεί. Με αυτό τον τρόπο γίνεται ένα είδος φιλτραρίσματος, καθώς από το σύνολο των καταγεγραμμένων ακουστικών κυμάτων εξάγεται μόνο ένα χαρακτηριστικό διάνυσμα.
3. Ταξινόμηση/χαρακτηρισμός: Το χαρακτηριστικό διάνυσμα που εξάχθηκε από το προηγούμενο βήματα εφαρμόζεται σε έναν αλγόριθμο ταξινόμησης ώστε να γίνει ο τελικός χαρακτηρισμός του. Η λειτουργία αυτού του αλγορίθμου ταξινόμησης είναι να συγκεκριμένο το συγκεκριμένο χαρακτηριστικό διάνυσμα με ένα σύνολο γνωστών διανυσμάτων. Το αποτέλεσμα αυτής της σύγκρισης είναι η εξαγωγή του τύπου της απειλής [36].

Η επεξεργασία των ακουστικών κυμάτων μπορεί να τροφοδοτήσει την μέθοδο χαρακτηρισμών των απειλών με ένα μεγάλο πλήθος χαρακτηριστικών ιδιοτήτων. Οι χαρακτηριστικές αυτές ιδιότητες μπορεί να είναι απλές στατιστικές μετρήσεις (όπως είναι το ελάχιστη και το μέγιστη ενεργειακή στάθμη τους) μέχρι και αποτελέσματα πολύπλοκων υπολογισμών όπως είναι ο μετασχηματισμός Fourier των δεδομένων [160].

Όσων αφορά τον αλγόριθμο ταξινόμησης, υπάρχει μεγάλη εξάρτηση ανάμεσα στον τρόπο λειτουργίας του και το είδος των χαρακτηριστικών ιδιοτήτων που χρησιμοποιεί. Σε μελέτες έχει περιγραφεί ένα μεγάλο πλήθος αλγορίθμων ταξινόμησης με πιο χαρακτηριστικές αυτές της χρήσης δέντρου αποφάσεων, της χρήσης νευρωνικών δικτύων καθώς και της εύρεσης των "k κοντινότερων γειτόνων". Όσον αφορά την εφαρμογή αλγορίθμων ταξινόμησης στα ασύρματα δίκτυα αισθητήρων υπάρχουν δύο προσεγγίσεις:

1. **Κατανεμημένη Αξιολόγηση:** Η ταξινόμηση των χαρακτηριστικών διανυσμάτων να γίνεται τοπικά στον κόμβο όπου δημιουργήθηκαν. Το αποτέλεσμα της τοπικής ταξινόμησης αποστέλλεται στον σταθμό βάσης. Ο σταθμός βάσης με την σειρά του συλλέγει τις τελικές κλάσεις κατηγοριοποίησης όλων των κόμβων, τα συνδυάζει και εξάγει το τελικό χαρακτηρισμό της απειλής.
2. **Κεντρικοποιημένη Αξιολόγηση:** Στην περίπτωση χρήσης της κεντρικοποιημένης αξιολόγησης, οι κόμβοι αφού εξάγουν τα χαρακτηριστικά διανύσματα του ακουστικού κύματος, τα στέλνουν στον σταθμό βάσης. Πλέον οι υποχρεώσεις του σταθμού βάσης περιλαμβάνουν την συλλογής των διανυσμάτων από τους κόμβους, την αξιολόγηση τους και την εξαγωγή ενός τελικού χαρακτηρισμού για την απειλή.

Κάθε μια από τις δύο παραπάνω προσεγγίσεις έχει τα θετικά και τα αρνητικά της. Η προσέγγιση της κατανεμημένης αξιολόγησης μειώνει σε μεγάλο βαθμό τον όγκο των απαιτούμενων δεδομένων που πρέπει να σταλούν από τους κόμβους στον σταθμό βάσης, μειώνοντας έτσι το ενεργειακό κόστος. Από την άλλη όμως, η εκτέλεση της ταξινόμησης τοπικά στον κόμβο απαιτεί την υλοποίηση και εκτέλεση ειδικών αλγορίθμων ταξινόμησης. Οι ειδικοί αυτοί αλγόριθμοι παρέχουν μια ισορροπία ανάμεσα στην χρήση των πόρων του κόμβου και στην ποιότητα των αποτελεσμάτων της αξιολόγησης. Αντίθετα στην προσέγγιση της κεντρικοποιημένης αξιολόγησης η εκτέλεση των αλγορίθμων αξιολόγησης γίνεται στον σταθμό βάσης. Ο σταθμός βάσης παρέχει την ευκολία εκτέλεσης πολύπλοκων υπολογισμών προσφέροντας παράγοντας έτσι ποιοτικά αποτελέσματα αξιολόγησης. Από την μεριά του κόμβου απαιτείται η αποστολή μεγάλου όγκου δεδομένων (χαρακτηριστικό διάνυσμα) προς τον σταθμό βάσης.

Παρακάτω γίνεται μια σύντομη αναφορά στις υφιστάμενες μεθόδους χαρακτηρισμού απειλών. Το χαρακτηριστικό όλων των προσεγγίσεων, που περιγράφονται, είναι η ισορροπία που καλούνται να διαχειριστούν ανάμεσα στην χρήση πόρων και στην ποιότητα των αποτελεσμάτων τους.

7.1 Υφιστάμενες Μέθοδοι

Στην μελέτη [96] των Gu et al., περιγράφεται η εργασία VigilNet του οποίου στόχο είναι ο εντοπισμός οχημάτων ,ανθρώπων και ανθρώπων που φέρουν μεταλλικά αντικείμενα. Οι κόμβοι κατηγοριοποιούν τα γεγονότα με βάση τις τιμές που καταγράφουν ένα μαγνητόμετρο, ένας αισθητήρας κίνησης και ένα μικρόφωνο. Τα αποτελέσματα αποστέλλονται σε έναν δυναμικά καθορισμένο επικεφαλής μιας ομάδας για αποτίμηση και εντοπισμό. Οι πληροφορίες εντοπισμού αποστέλλονται στον σταθμό βάσης.

Μέρος της εργασίας SenseIT ,των Duarte και Hu[20] ήταν η αξιολόγηση αλγορίθμων κατηγοριοποίησης για τον εντοπισμό οχημάτων. Κάθε κόμβος συλλέγει ηχητικά και σεισμικά δεδομένα και κατηγοριοποιεί τα γεγονότα χρησιμοποιώντας χαρακτηριστικά τα οποία έχουν εξαχθεί από το φάσμα συχνοτήτων μετά την εφαρμογή γρήγορου μετασχηματισμού Fourier (FFT). Η αξιολόγηση περιλαμβάνει 3 αλγόριθμους κατηγοριοποίησης : k-στός πλησιέστερος γείτονας, ML, και support vector machine. Τα αποτελέσματα αποστέλλονται σε έναν σταθερά προκαθορισμένο κόμβο ενός cluster για

αξιολόγηση όπου και συνδυάζεται με τις αναφορές που έχουν παραληφθεί από άλλους κόμβους για τον εντοπισμό των οχημάτων.

Οι Tavakoli et al [114] περιγράφουν ένα σενάριο κατά το οποίο οι στόχοι εντοπίζονται με τη χρήση ενός υποθαλάσσιου δικτύου ακουστικών αισθητήρων . Ομοίως με τις προηγούμενες προσπάθειες οι κόμβοι αναφέρουν το τοπικό συμπέρασμα κατηγοριοποίησης στον επί κεφαλής ενός cluster ο οποίος μετά τη αξιολόγηση των αποτελεσμάτων έχει τη δυνατότητα να αποστείλει το αποτέλεσμα στον σταθμό βάσης. Επιπρόσθετα του πλήθους των αναφορών που λαμβάνει ο επί κεφαλής κόμβος λαμβάνει υπ όψιν του και την ακρίβεια των αναφορών που έχει παραλάβει στο παρελθόν από κάθε κόμβο.

Στόχος του συστήματος που προτάθηκε από τους Yang et al[35] είναι η αναγνώριση ανθρώπινων κινήσεων. Πρόκειται για ένα Body Area Network (BAN) που αποτελείται από 8 κόμβους προσκολλημένους στο σώμα ενός ανθρώπου ο οποίος έχει την δυνατότητα να εκτελέσει οποιαδήποτε από ένα σύνολο 12 κινήσεων. Τα χαρακτηριστικά εξάγονται από ένα επιταχυνσιόμετρο και ένα γυροσκόπιο και κατηγοριοποιούνται επί τόπου σε κάθε κόμβο. Αν κάποια από τις τοπικές κατηγοριοποιήσεις κρίνεται ασφαλής μεταδίδεται στον σταθμό βάσης και κατηγοριοποιείται μία ακόμα φορά. Η διαδικασία κατηγοριοποίησης ταχτοποιεί μία κίνηση ταιριάζοντας την γραμμική αναπαράσταση του διανύσματος των χαρακτηριστικών που έχουν γίνει αντιληπτά σε έναν από τους διάφορους υποχώρους κάθε ένας από τους οποίους αντιστοιχεί σε ένα είδος κίνησης.

Στην εργασία των Wang et al [115] περιγράφεται ένα σύστημα παρακολούθησης περιβάλλοντος το οποίο δύναται να αναγνωρίζει και να εντοπίζει τη θέση των ζώων μέσα σε αυτό, βασιζόμενο σε ακουστικά σήματα. Η υλοποίηση περιλαμβάνει έναν επί κεφαλής κόμβο με αυξημένη υπολογιστική ικανότητα ο οποίος έχει τη δυνατότητα να ζητήσει μη επεξεργασμένα δεδομένα από τους άλλους κόμβους για εκτέλεση κεντρικοποιημένης αξιολόγησης. Τα ζώα αναγνωρίζονται μέσω της μέγιστης τιμής ενός συντελεστή συσχέτισης ενός φασματογραφήματος από τα αποτελέσματα της παρακολούθησης και ένα φασματογράφημα αναφοράς. Με τη χρήση αναφορών από πολλαπλούς κόμβους γίνεται ο τοπικό εντοπισμός στο πεδίο.

Το κατανεμημένο σύστημα εντοπισμού που προτάθηκε από τους Martincic και Schwieber [158] ομαδοποιεί τους κόμβους σε κυψέλες με βάση τη γεωγραφική τους θέση. Όλοι οι κόμβοι μιας κυψέλης μεταδίδουν τα δεδομένα τους στον επί κεφαλής κόμβο της κυψέλης όπου υπολογίζεται ο μέσος όρος των αποτελεσμάτων όπως επίσης και οι μέσοι όροι των γειτονικών κυψελών. Η ανίχνευση των γεγονότων γίνεται στους επί κεφαλής κόμβους κάθε κυψέλης ι οποίοι σχηματίζουν έναν πίνακα με τα αποτελέσματα που έχουν συλλέξει συγκρίνοντας τον με έναν προκαθορισμένο πίνακα που περιγράφει το γεγονός. Στην περίπτωση που οι 2 πίνακες ταιριάζουν , ταχτοποιείται ένα γεγονός.

Στην εργασία των Li et al [159] χρησιμοποιείται το παράδειγμα ενός συστήματος παρακολούθησης ενός ανθρακωρυχείου για την αξιολόγηση ενός WSN το οποίο χρησιμοποιείται για την ανίχνευση γεγονότων σε τρισδιάστατο περιβάλλον χωρίς τη εξάρτηση από οριακές τιμές στα μη επεξεργασμένα δεδομένα. Το σύστημά τους λειτουργεί μέσω συσσώρευσης των δεδομένων στον σταθμό βάσης από τους κόμβους που έχουν αναπτυχθεί σε ολόκληρη την περιοχή με τη βοήθεια ενός προκαθορισμένου χάρτη επικοινωνίας. Ο εντοπισμός επιτυγχάνεται με ταίριασμα δεδομένων από

ακολουθιακά γεγονότα σε σχέση με τις ήδη γνωστές τιμές συγκεκριμένων γεγονότων, π.χ. διαρροή φυσικού αερίου.

7.1.1 Αξιολόγηση υφιστάμενων μεθόδων

Στις εργασίες των Duarte[20] και Wang[115] υπάρχει η απαίτηση για κόμβους με εκτεταμένες δυνατότητες υπολογισμού όπως για παράδειγμα η εκτέλεση FFT. Οι απαιτήσεις των συστημάτων των Tavakoli [114] και Yang [35] δεν είναι τόσο ξεκάθαρες, αλλά μέσω της προσέγγισης που ακολουθούν θα πρέπει να θεωρήσουμε ότι οι απαραίτητοι υπολογισμοί δεν μπορούν να εκτελεστούν από έναν συνηθισμένο κόμβο.

Στις περισσότερες προσεγγίσεις απαιτείται από τις WSN πλατφόρμες να παρέχουν ένα μηχανισμό διαχείρισης των clusters και εκλογής κόμβου επί κεφαλής. Στην εργασία του Gu [96] παρέχει μία υπηρεσία μετακίνησης του επί κεφαλής κόμβου ενός cluster με στόχο την υποστήριξη του εντοπισμού αντικείμενων. Στην εργασία [158] απαιτείται το ασύρματο δίκτυο αισθητήρων να διαχωριστεί σε κυψέλες και την ανάθεση των κόμβων σε μία από αυτές ανάλογα με την τοποθεσία τους. Αντίθετα οι εργασίες των Yang[35] και Li [159] δεν απαιτούν τέτοιο διαχωρισμό των κόμβων καθώς στις προσεγγίσεις αυτές όλοι οι κόμβοι επικοινωνούν απ' ευθείας με τον σταθμό βάσης.

Η «εκπαίδευση» του συστήματος με συγκεκριμένα σενάρια γεγονότων υποστηρίζεται από τις προσεγγίσεις των Yang[35] ,Duarte[20] και Martincic[158]. Οι εργασίες των Wang [115] και Li [159] μπορούν να θεωρηθούν ότι υποστηρίζουν ένα είδος τμηματικής «εκπαίδευσης» του συστήματος , καθώς στις υλοποιήσεις τους η κατηγοριοποίηση των γεγονότων βασίζεται σε μοτίβα καθορισμένα από το ν χρήστη με τη μορφή φασματογραφημάτων και ιδιότητες χρονικών ακολουθιών. Η εργασία του Gu [96] βασίζεται κυρίως σε προκαθορισμένες οριακές τιμές αντί για δεδομένα που παρέχονται από «εκπαίδευση» βασισμένη σε ανίχνευση γεγονότων. Από την άλλη πλευρά ο Takavoli [114] αναλύει την ανίχνευση γεγονότων βασισμένη σε δεδομένα από προσομοιωμένα γεγονότα και κατ' αυτόν τον τρόπο δεν βασίζεται στην «εκπαίδευση». Στο σημείο αυτό θα πρέπει να αναφερθεί ότι η υποστήριξη εκπαίδευσης σε γεγονότα δεν κρίνεται απαραίτητα ως θετικό για όλα τα είδη των σεναρίων . Πιο συγκεκριμένα , υπάρχουν περιπτώσεις όπου ιδανικά η ανίχνευση γεγονότων θα πρέπει να γίνεται μέσω ταξινόμησης με βάση εξειδικευμένα επιστημονικά δεδομένα αντίθετα με πειραματικά δεδομένα. Ειδικά για περιπτώσεις όπου είναι δύσκολο να προκύψουν πειραματικά δεδομένα ως αποτέλεσμα προσομοίωσης.

Οι εργασίες των Martincic[158] ,Yang[35] και Li[159] είναι οι μόνες προσεγγίσεις οι οποίες βασίζουν την κατηγοριοποίηση που πραγματοποιούν με διανύσματα χαρακτηριστικών δεδομένων από πολλαπλούς κόμβους. Τα διανύσματα χαρακτηριστικών που χρησιμοποιούνται στην εργασία του Martincic[158] περιορίζονται σε μία διάσταση ανά κόμβο , ενώ η εργασία του Li[9] εξαρτάται πλήρως από τον σταθμό βάσης για την κατηγοριοποίηση. Στις υπόλοιπες εργασίες πραγματοποιείται η κατηγοριοποίηση με βάση τα δεδομένα που συλλέγονται τοπικά και αργότερα τα αποτελέσματα συσσωρεύονται στον επί κεφαλής κόμβο κάθε cluster. Τέλος η εργασία του Gu[96] διαφέρει από τις υπόλοιπες στο γεγονός ότι ο επί κεφαλής κόμβος επαναξιολογεί τα αποτελέσματα που προκύπτουν από τους περιφερειακούς κόμβους.

7.2 Προτεινόμενη μέθοδος χαρακτηρισμού απειλών

Για την εφαρμογή λειτουργικότητας χαρακτηρισμού απειλών στα ασύρματα δίκτυα αισθητήρων προτείνεται μια υβριδική λύση. Η μέθοδος αυτή χρησιμοποιεί ένα σύνολο απλών στατιστικών αλλά και πιο πολύπλοκων υπολογισμών προκειμένου να εντοπίσει τον τύπο μιας απειλής. Οι χρήση των απλών στατιστικών υπολογισμών πάνω στα καταγεγραμμένα ακουστικά κύματα προορίζεται για τον χαρακτηρισμό απειλών που έχουν κάποιο συγκεκριμένο, εύκολα αναγνωρίσιμο, ακουστικό πρότυπο. Ο τύπος αυτών των απειλών μπορεί να είναι είτε ο ήχος μίας έκρηξης, είτε ο ήχος από το ανθρώπινο περπάτημα.

Από την άλλη, στην περίπτωση όπου δεν εντοπιστεί στα καταγεγραμμένα ακουστικά κύματα κάποιο, εύκολα αναγνωρίσιμο, πρότυπο, την επεξεργασία τους αναλαμβάνει ένα πιο σύνθετος αλγόριθμος. Ο αλγόριθμός αυτός μπορεί να εξάγει συμπεράσματα σχετικά με πιο πολύπλοκα ακουστικά κύματα όπως είναι αυτό των αυτοκινήτων, φορτηγών κλπ. Ο αλγόριθμος αυτός βασίζεται στην χρήση της μεθόδου TESPAR (Time Encoded Signal Processing and Recognition) [161]. Πρόκειται για έναν αλγόριθμό χαμηλής πολυπλοκότητας ο οποίος έχει χρησιμοποιηθεί επιτυχώς για την κατηγοριοποίηση σημάτων οριοθετημένης ζώνης (band-limited), όπως είναι αυτό της φωνής.

Παρακάτω ακολουθεί μια αναλυτική περιγραφή των 2 διαφορετικών μεθόδων χαρακτηρισμού των απειλών.

7.2.1 Μέθοδος ανίχνευσης με χρήση απλών στατιστικών υπολογισμών

Η ηχητική περιγραφή του ανθρώπινου βαδίσματος αλλά και της έκρηξης μπορεί να αναγνωριστεί εύκολα καθώς το ακουστικό κύμα τους αποτελείται από διακριτές περιοχές οι οποίες βρίσκονται πάνω από την στάθμη του κατωφλίου (σχετικά με την στάθμη του κατωφλίου υπάρχει αναλυτική περιγραφή στο Κεφάλαιο 6.3.3).

Για παράδειγμα, τα ακουστικά κύματα που παράγονται από τα ανθρώπινα βήματα, στο μεγαλύτερο διάστημα καταγραφής τους βρίσκονται κάτω από το επίπεδο του κατωφλίου. Ανά τακτά περιοδικά διαστήματα, όμως, η ένταση του κύματος υπερβαίνει για ένα μικρό χρονικό διάστημα το επίπεδο του κατωφλίου. Ουσιαστικά, αυτά τα περιοδικά διαστήματα που η ένταση του κύματος υπερβαίνει το κατώφλι οφείλονται στην ένταση που κάνει η επαφή του ανθρώπινου ποδιού με το έδαφος κατά την διάρκεια του βαδίσματος.

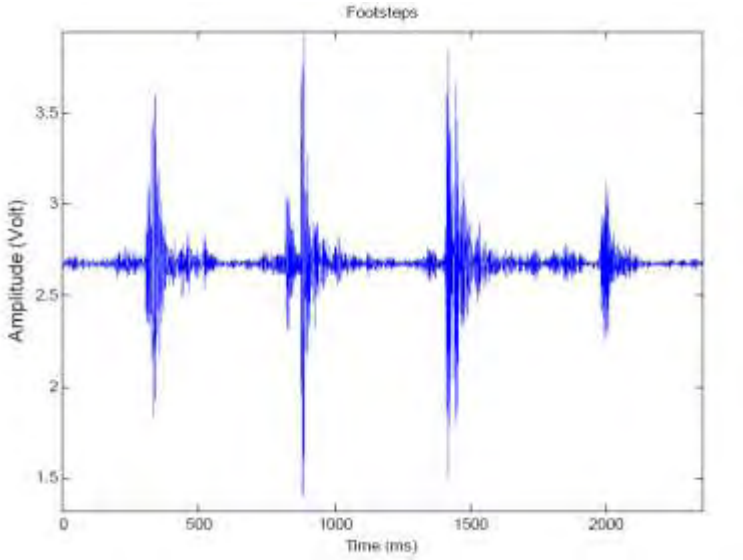
Από την άλλη, η μορφή του ακουστικού κύματος που δημιουργείται από μια έκρηξη αποτελείται από μια μόνο αιχμή. Η ένταση του ακουστικού κύματος καθόλη την διάρκεια καταγραφής του βρίσκεται κάτω από την στάθμη του κατωφλίου. Η μόνο στιγμή όπου γίνεται υπέρβαση της στάθμης αυτής είναι την στιγμή της έκρηξης και διαρκεί για μερικά δευτερόλεπτα.

Βασιζόμενοι σε αυτές τις χαρακτηριστικές ιδιότητες των ακουστικών κυμάτων των δύο παραπάνω περιπτώσεων, μπορούμε εύκολα χρησιμοποιώντας κάποιους στατιστικούς υπολογισμούς να τα ανιχνεύσουμε.

7.2.1.1 <u>Ανίχνευση ανθρώπινης παρουσίας μέσω του βαδίσματος</u>

Η ηχητική υπογραφή του ανθρώπινου βαδίσματος οφείλεται στην επαφή του ανθρώπινου ποδιού με το έδαφος. Το ακουστικό κύμα κάθε βήματος έχει μια χαρακτηριστική μορφή η οποία μπορεί να χρησιμοποιηθεί για την διάκριση της από τον θόρυβο υπερβάλλοντος. Το χαρακτηριστικό που διακρίνει το ακουστικό κύμα του

βαδίσματος από άλλα ακουστικά κύματα είναι η ύπαρξη μιας σειρά περιοδικών «αιχμών» που έχει (Εικόνα 71). Η ύπαρξη αυτών των περιοδικών αιχμών διαχωρίζει τα ακουστικά κύματα του βαδίσματος από αυτά του περιβαλλοντικού θορύβου αλλά και άλλων απειλών, όπως είναι τα οχήματα. Το χρονικό διάστημα που μεσολαβεί ανάμεσα στην εμφάνιση δύο διαδοχικών «αιχμών» εξαρτάται από τον τύπου του βαδίσματος (π.χ. αργό , τρέξιμο). Το μέσο χρονικό διάστημα είναι 2 Hz, αλλά η συχνότητα αυτή κυμαίνεται από 0.9-1 Hz, στην περίπτωση αργού βαδίσματος, μέχρι 3.5 Hz ,στην περίπτωση τρεξίματος. [162-164]

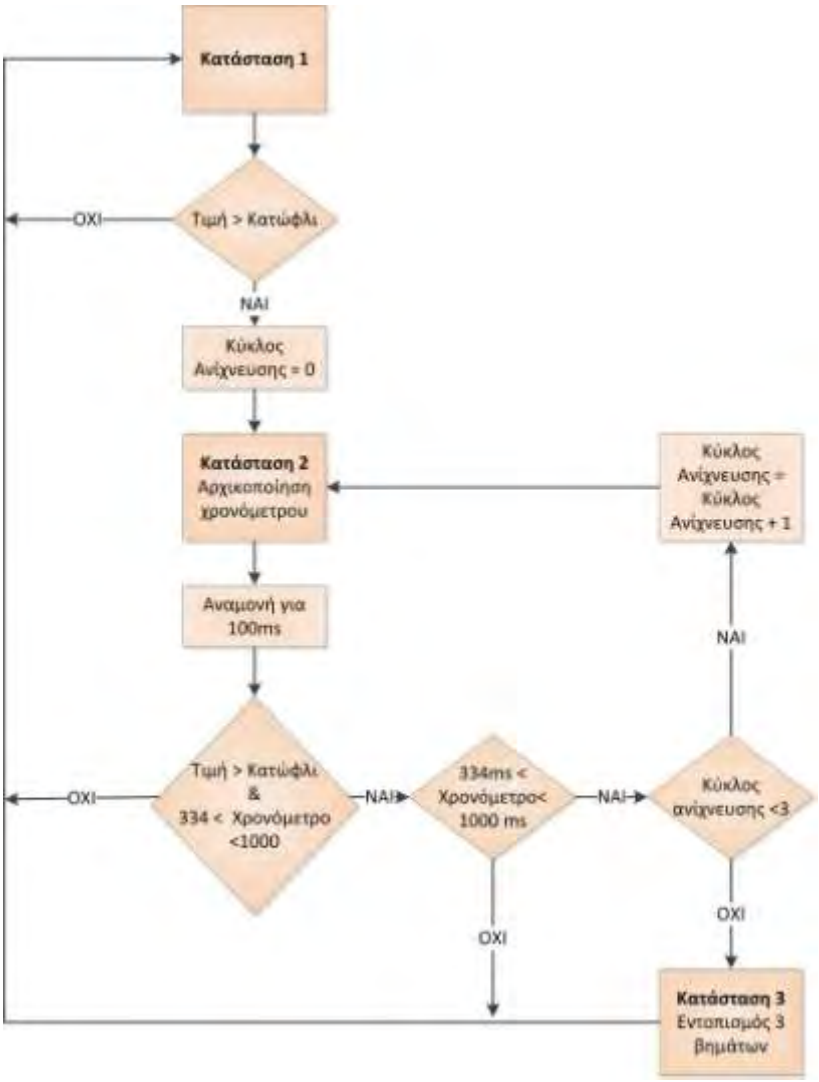


Εικόνα 71: Η μορφή ενός ακουστικού κύματος που προκαλείται από ανθρώπινο βάδισμα.

Ο αλγόριθμος που επεξεργάζεται ακουστικά κύματα προκειμένου να εντοπίσει τα ανθρώπινα βήματα βασίζεται σε μια ευρετική μέθοδο (heuristic). Αυτή η ευρετική μέθοδος βασίζεται σε αποτελέσματα που έχουν προκύψει μετά από μελέτη τόσο της βιβλιογραφίας, όσο και των δεδομένων που ελήφθησαν και δημιουργήθηκε με τις εξής προδιαγραφές:

1. Η ανίχνευση μιας απειλής ξεκινάει την στιγμή όπου η καταγεγραμμένη τιμή του ακουστικού κύματος ξεπερνάει την στάθμη του κατωφλίου.
2. Η μέση χρονική διάρκεια που το κύμα ενός βαδίσματος βρίσκεται πάνω από το κατώφλι είναι 100msec
3. Στην περίπτωση όπου κάποιος βαδίζει με αργό ρυθμό, ο χρόνος που μεσολαβεί ανάμεσα σε δύο διαδοχικές «αιχμές» είναι μικρότερο από 1 sec.
4. Στην περίπτωση όπου κάποιος βαδίζει με γρήγορο ρυθμό, ο χρόνος που μεσολαβεί ανάμεσα σε δύο διαδοχικές «αιχμές» είναι μεγαλύτερος από 334 msec.
5. Για την επιτυχή ανίχνευση ενός βαδίσματος, ο αλγόριθμός πρέπει να ανιχνεύσει 3 διαδοχικές «αιχμές».

Ο αλγόριθμος εντοπισμού ανθρώπινου βαδίσματος που αναπτύχθηκε, λαμβάνει υπόψη τις παραπάνω προδιαγραφές προκειμένου να κάνει την ανίχνευση με εύκολο και χαμηλής πολυπλοκότητας τρόπο. Έτσι οι καταστάσεις λειτουργίας του αλγορίθμου φαίνονται στο παρακάτω διάγραμμα.



Εικόνα 72: Η καταστάσεις λειτουργίας του αλγορίθμου χαρακτηρισμού ανθρώπινου βηματισμού.

Ο αλγόριθμος αρχικά βρίσκεται στην **Κατάσταση 1**, όπου και περιμένει την ύπαρξη κάποιου ακουστικού κύματος που θα υπερβεί την στάθμη του κατωφλίου. Όταν κάποιο κύμα ανιχνευτεί ως απειλή, ο αλγόριθμος μεταβαίνει στην **Κατάσταση 2**. Σε αυτή την κατάσταση ο κόμβος αναμένει την ανίχνευση της επόμενης «αιχμής».

Κατά την διάρκεια των πρώτων 100 ms όπου ο κόμβος βρίσκεται στην **Κατάσταση 2**, κανένας έλεγχος δεν γίνεται στην στάθμη του κύματος. Αυτό συμβαίνει γιατί ο αλγόριθμος περιμένει γίνει απόσβεση της «αιχμής» του προηγούμενου κύματος. Αφού ολοκληρωθούν τα 100ms, ξεκινάει ο έλεγχος για την εύρεση της νέας αιχμής. Αυτός ο έλεγχος έχει μέγιστη διάρκεια 1000ms.

Αν σε αυτό το διάστημα, δεν ανιχνευτεί κάποια νέα αιχμή, ο αλγόριθμος επιστρέφει στην **Κατάσταση 1**. Το συγκεκριμένο ακουστικό κύμα δεν προέρχεται από ανθρώπινο βάδισμα. Διαφορετικά, στην περίπτωση ανίχνευσης μιας νέας αιχμής σε αυτό το διάστημα, ο αλγόριθμος ελέγχει την χρονική στιγμή άφιξης του άφιξης της αιχμής. Αν η χρονική απόσταση ανάμεσα σε αυτή και την προηγούμενη αιχμή είναι μεγαλύτερη από

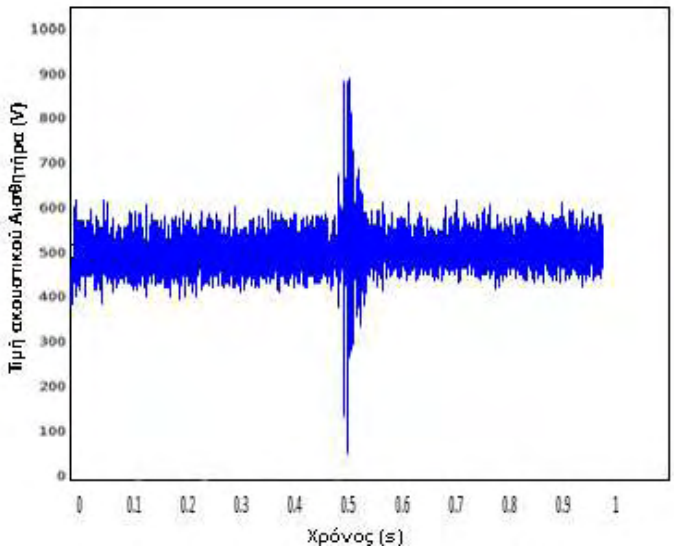
334ms τότε το κύμα πιθανώς να προέρχεται από ανθρώπινο βάδισμα. Σε διαφορετική περίπτωση, ο αλγόριθμος μεταβαίνει στην **Κατάσταση 1** καθώς το κύμα δεν προέρχεται από ανθρώπινο βάδισμα.

Ο αλγόριθμος θα πρέπει να επαναλάβει την παραπάνω διαδικασία τρεις φορές., καθώς μόνο στην περίπτωση όπου ανιχνευτούν τρείς διαδοχικές αιχμές, το κύμα μπορεί να χαρακτηριστεί ότι προέρχεται από ανθρώπινο βάδισμα. Ο χαρακτηρισμός του ακουστικού κύματος ως ήχος ανθρώπινου βήματος σηματοδοτείται με την μετάβαση του κόμβου στην **Κατάσταση 3**.

7.2.1.2 Ανίχνευση έκρηξης

Ο αλγόριθμος που επεξεργάζεται τα ακουστικά κύματα προκειμένου να ανιχνεύσει μια έκρηξη βασίζεται στην ανίχνευση των χαρακτηριστικών που έχει αυτός ο ήχος. Πρόκειται δηλαδή για μία ευρετική μέθοδο (heuristic) η οποία βασίζεται σε αποτελέσματα που έχουν προκύψει μετά από μελέτη τόσο της βιβλιογραφίας, όσο και των δεδομένων που ελήφθησαν.

Το κύριο χαρακτηριστικό του ακουστικού κύματος μιας έκρηξης είναι η πολύ μικρή χρονική διάρκεια που η ένταση του βρίσκεται πάνω από την στάθμη του κατωφλίου. Για την ακρίβεια, το ακουστικό κύμα της έκρηξης έχει στιγμιαία πολύ μεγάλη ένταση (στιγμή όπου γίνεται υπέρβαση του κατωφλίου) και στην συνέχεια επανέρχεται στην σχετική ηρεμία (επίπεδο περιβαλλοντικού θορύβου). Το διάστημα όπου η ένταση του κύματος υπερβαίνει αυτό του κατωφλίου είναι γύρω στα 100 ms.



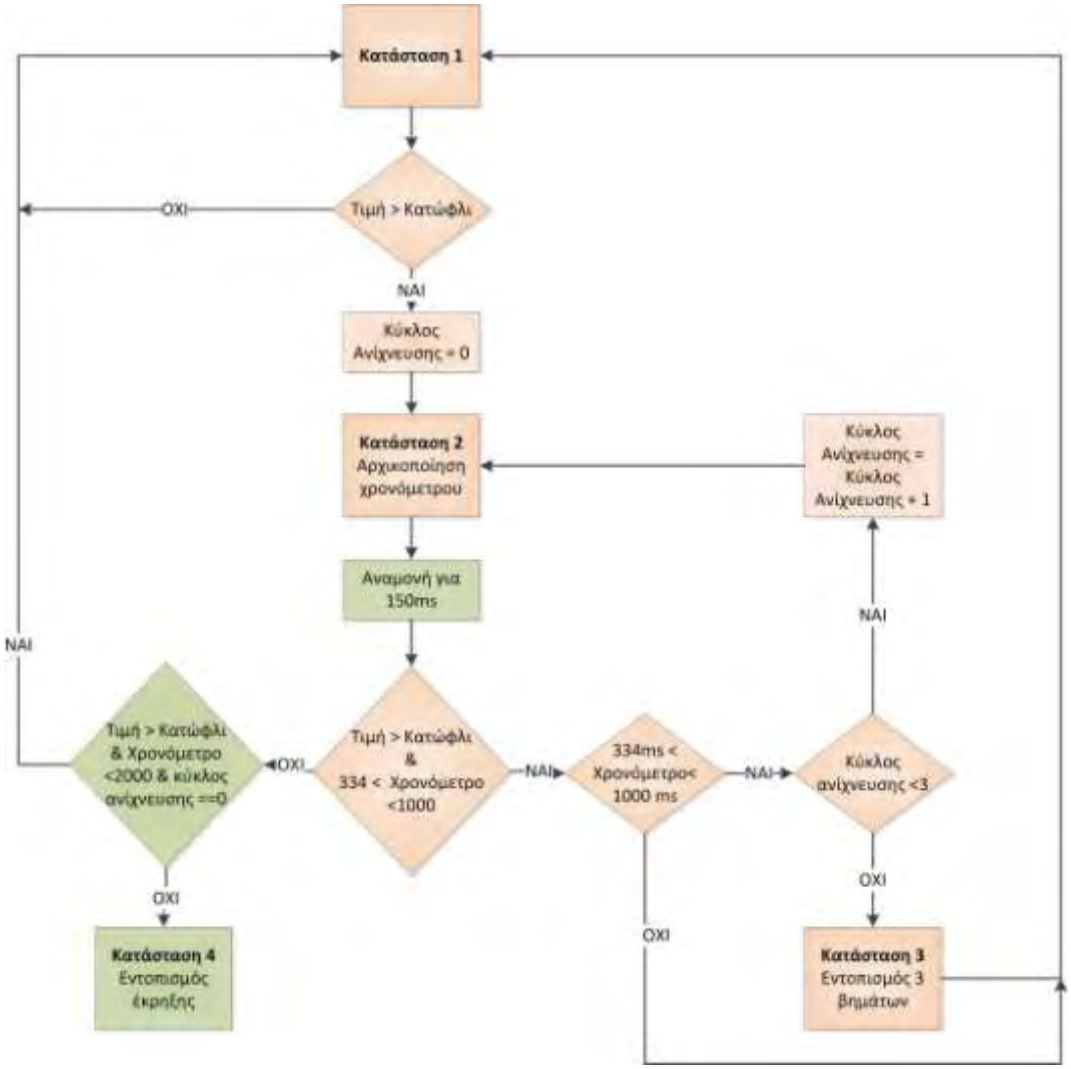
Εικόνα 73: Η μορφή του ακουστικού κύματος μίας έκρηξης.

Έτσι οι ιδιότητες που θα πρέπει να χρησιμοποιεί ο αλγόριθμος ανίχνευσης προκειμένου να εντοπίσει το ακουστικό κύμα μίας έκρηξης είναι:

- Η ένταση του ακουστικού κύματος να υπερβαίνει την στάθμη του κατωφλίου
- Το χρονικό διάστημα της υπέρβασης του κατωφλίου να έχει διάρκεια όχι μεγαλύτερη από 150 ms

- Μετά το διάστημα των 150ms, η ένταση του κύματος να κυμαίνεται στα επίπεδα του περιβαλλοντικού θορύβου χωρίς να υπάρχει καμία άλλη υπέρβαση του κατωφλίου.

Η παρακάτω εικόνα απεικονίζει τις καταστάσεις λειτουργίας του αλγορίθμου ανίχνευσης των ακουστικών κυμάτων που προέρχονται από έκρηξη. Οι καταστάσεις λειτουργίας του εμφανίζονται ενσωματωμένες με αυτές της ανίχνευσης ανθρώπινου βηματισμού καθώς παρουσιάζουν πολλές ομοιότητες στον τρόπο λειτουργίας τους και στις απαιτήσεις που έχουν.



Εικόνα 74: Οι καταστάσεις λειτουργίας του αλγορίθμου ανίχνευσης εκρήξεων (πράσινο χρώμα) σε συνδυασμό με αυτές της ανίχνευσης ανθρώπινου βηματισμού (ροζ χρώμα).

Οι καταστάσεις λειτουργίας του αλγορίθμου ανίχνευσης εκρήξεων παρουσιάζονται στην παραπάνω εικόνα με πράσινο χρώμα. Η μόνη αλλαγή που έχει γίνει στην λειτουργία του αλγορίθμου ανίχνευσης ανθρώπινου βηματισμού είναι η επέκταση της διάρκειας αναμονής χωρίς τον έλεγχο των κυμάτων για την υπέρβαση του κατωφλίου.

Ουσιαστικά αυτός ο χρόνος αναμονής αφορά το χρόνο απόσβεσης της αιχμής του κύματος. Ο χρόνος απόσβεσης του κύματος της έκρηξης είναι 50 ms μεγαλύτερος από τον αντίστοιχο του ανθρώπινου βηματισμού. Εφόσον αυτά τα 50ms δεν επηρεάζουν την ανίχνευση του ανθρώπινου βηματισμού (το επόμενο βήμα αναμένεται μετά από 334ms), ο χρόνος αναμονής τίθεται στα 150ms.

Αφού γίνει ο πρώτος έλεγχος της έντασης του κύματος και βρεθεί ότι υπερβαίνει την στάθμη του κατωφλίου, ο αλγόριθμός ανίχνευσης εκρήξεων αναμένει για 150 ms για την απόσβεση του κύματος. Στην συνέχεια εκτελείται μια λειτουργία όπου είναι κοινή για τους δύο αλγορίθμους. Στην περίπτωση όπου δεν εντοπισθεί κάποιο, η ένταση του οποίου να υπερβαίνει το κατώφλι, ο αλγόριθμος ανίχνευσης των εκρήξεων συνεχίζει τον έλεγχο για ακόμα 2 s. Αυτό το επιπλέον διάστημα ελέγχου γίνεται για την εξασφάλιση της μη ύπαρξης άλλη αιχμής, εκτός από την αρχική που εκκίνησε τον αλγόριθμο. Στην περίπτωση όπου δεν εντοπισθεί άλλη αιχμή, ο αλγόριθμος μεταβαίνει στην **Κατάσταση 4** όπου και σηματοδοτείται η αναγνώριση του κύματος ως έκρηξη. Σε διαφορετική περίπτωση, ο αλγόριθμος μεταβαίνει στην **Κατάσταση 1** καθώς το κύμα δεν προέρχεται ούτε από ανθρώπινο βάδισμα αλλά ούτε έκρηξη.

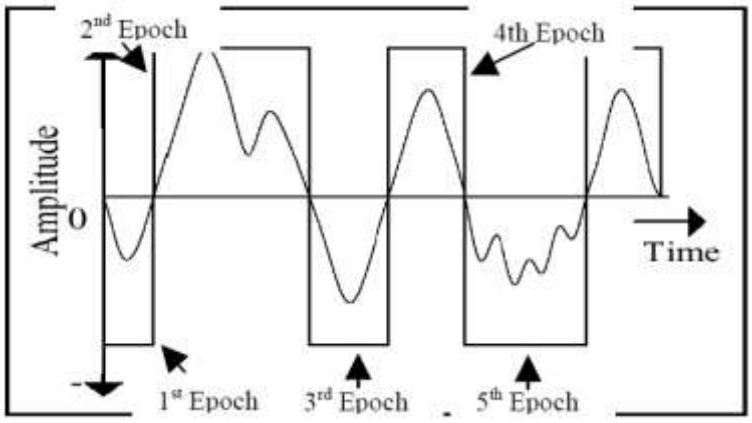
7.2.2 Μέθοδος ανίχνευσης με χρήση της μεθόδου TESPAR

Στην περίπτωση όπου κάποιο ακουστικό κύμα δεν μπορεί να αναγνωριστεί από τις 2 παραπάνω στατιστικές μεθόδους, την εξαγωγή συμπεράσματος σχετικά με την κατηγοριοποίηση του τύπου του κύματος αναλαμβάνει ένας πιο σύνθετος αλγόριθμος. Ο αλγόριθμος που χρησιμοποιείται είναι ο TESPAR (Time Encoded Signal Processing and Recognition).

Ο αλγόριθμος TESPAR περιγράφηκε πρώτη φορά στην μελέτη των King και Gosling [161] Πρόκειται για μία απλή και αποτελεσματική μέθοδο η οποία χρησιμοποιείται για την περιγραφή σύνθετων κυματομορφών με απλούς όρους. Είναι μια μέθοδος χαμηλής πολυπλοκότητας η οποία μπορεί να χρησιμοποιηθεί για την περιγραφή ενός μεγάλου πλήθους κυματομορφών, όπως ακουστικών, σεισμικών αλλά και ηλεκτρικών σημάτων. Η ανάλυση του κύματος γίνεται με την με την κωδικοποίησή τους σε μια σειρά από σύμβολα. Η λειτουργία της βασίζεται στην ανάλυση της μορφής του κύματος έτσι ώστε να την κωδικοποιήσει σε μια σειρά από σύμβολα. Αυτή σειρά από σύμβολα παίζει τον ρόλο ενός χαρακτηριστικού διανύσματος για το ακουστικό κύμα, η σύγκριση του οποίου με κάποια ήδη γνωστά διανύσματα εξάγει το αποτέλεσμα της κατηγοριοποίησης του κύματος.

7.2.2.1 Μέθοδος «Ατέρμων Ψαλιδισμός» (Infinite Clipping)

Πρωτεύων ρόλο στην ανάπτυξη της μεθόδου TESPAR κατέχει η μέθοδος του «Ατέρμονος Ψαλιδισμού» (Infinite Clipping). Η συγκεκριμένη μέθοδος προτάθηκε για πρώτη φορά από τους Licklidder and Pollack [165]. Σύμφωνα με αυτή την μέθοδο, η αφαίρεση της πληροφορίας του πλάτους από μια κυματομορφή ομιλίας και η διατήρηση μόνο των μηδενισμών (μεταβάσεων από το μηδενικό επίπεδο της κυματομορφής δεν επιφέρει σημαντική μείωση στην αναγνώριση και αντίληψη μίας λέξης από τον ακροατή. Η κατανόησης μιας λέξης που έχει επεξεργασθεί με την συγκεκριμένη μέθοδο αγγίζει το ποσοστό του 97.9% [166].



Εικόνα 75: Η μέθοδος του «Ατέρμονος Ψαλιδισμού» [166]

Η μέθοδος του «Ατέρμονος Ψαλιδισμού» αναπαριστά το χρονικό διάστημα ανάμεσα σε δύο διαδοχικούς μηδενισμούς ενός ακουστικού κύματος ομιλίας. Αυτά τα χρονικά διαστήματα είναι ανεξάρτητα της συχνότητας δειγματοληψίας του κύματος και εξαρτώνται αποκλειστικά από την μορφή του ίδιου του κύματος.

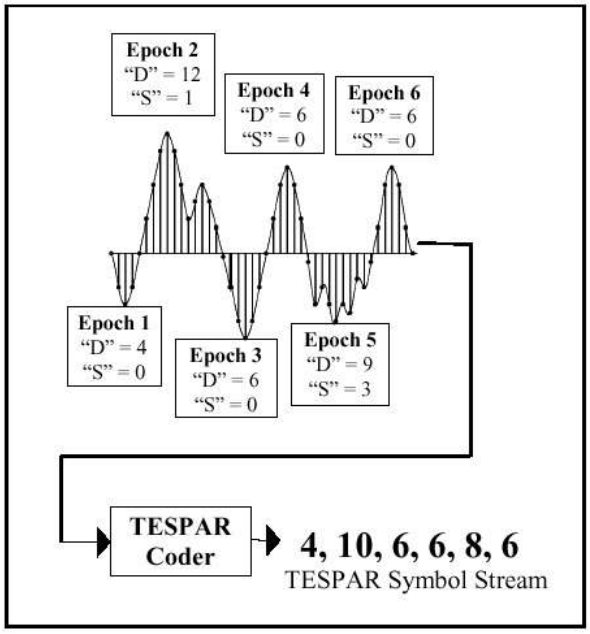
7.2.2.2 Η μέθοδος TESPAR

Όπως αναφέραμε παραπάνω, βασική λειτουργία της μεθόδου TESPAR είναι η κωδικοποίηση του ακουστικού κύματος σε μια σειρά από σύμβολα. Η κωδικοποίηση αυτή βασίζεται στην προσέγγιση της θέσης των πραγματικών και σύνθετων μηδενισμών πάνω στην κυματομορφή. Ως πραγματικός μηδενισμός ορίζεται η μετάβαση του ακουστικού κύματος από το μηδενικό επίπεδο έντασης του. Σύνθετος μηδενισμός ορίζεται το ελάχιστο ή μέγιστο που βρίσκεται ανάμεσα σε δύο πραγματικούς μηδενισμούς (τοπικό ελάχιστο και τοπικό μέγιστο).

Η μέθοδος TESPAR αποτελείται από 3 κύριες διεργασίες: την εξαγωγή, την κωδικοποίηση και την κατηγοριοποίηση του ακουστικού κύματος. Οι χαρακτηριστικές ιδιότητες του ακουστικού κύματος αρχικά εξάγονται και κωδικοποιούνται σε μία σειρά από σύμβολα. Τα σύμβολα αυτά αποτελούν μέρος του TESPAR αλφάβητου. Έπειτα, η σειρά αυτών των συμβόλων μετατρέπεται σε ένα σύνολο πινάκων, τους TESPAR πίνακες. Οι πίνακες αυτοί θα χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων κατηγοριοποίησης του κύματος.

Διεργασία εξαγωγής και κωδικοποίησης

Η διεργασία της κωδικοποίησης της μεθόδου TESPAR βασίζεται στον εντοπισμό των πραγματικών αλλά και στον εντοπισμό των σύνθετων μηδενισμών που περιέχονται ανάμεσα σε δύο διαδοχικούς πραγματικούς μηδενισμούς. Το τμήμα του κύματος που περιέχεται ανάμεσα σε δύο διαδοχικούς πραγματικούς μηδενισμούς ονομάζεται «***Epoch***». Κάθε τμήμα «***Epoch***» του ακουστικού κύματος χαρακτηρίζεται από την διάρκεια (***D***) του αλλά και τη μορφή (***S***) του. Η παράμετρος της διάρκειας του τμήματος ορίζεται ως το χρονικό διάστημα ανάμεσα σε δύο διαδοχικούς πραγματικούς μηδενισμούς του κύματος. Η μορφή του τμήματος αναπαριστάται από έναν αριθμό ο οποίος περιέχει το πλήθος των τοπικών ελάχιστων ή μέγιστων του τμήματος αυτού.



Εικόνα 76: Η κωδικοποίηση του κύματος σε σύμβολα με την μέθοδο TESPAR [166].

Αφού ολοκληρωθεί ο προσδιορισμός των παραμέτρων ***D*** και ***S*** για κάθε διάστημα ***Epoch*** της κυματομορφής, η μέθοδος TESPAR τα χρησιμοποιεί προκειμένου να κατασκευάσει την χαρακτηριστική σειρά συμβόλων του κύματος.

Αλφάβητο της μεθόδου TESPAR

Ο ρόλος του αλφάβητου είναι καθοριστικός στην αποτελεσματικότητα της μεθόδου TESPAR. Αυτό το ειδικό αλφάβητο αποτελεί έναν πίνακα συμβόλων και χρησιμοποιείται για την αντιστοίχηση των δύο παραμέτρων (***D*** και ***S***) του κάθε ***Epoch*** σε ένα μοναδικό σύμβολο. Όπως είναι φανερό το μέγεθος του αλφαβήτου παίζει μεγάλο ρόλο στην αποτελεσματικότητα της αντιστοίχησης. Για τις περισσότερες εφαρμογές ένα αλφάβητο μεγέθους 28 συμβόλων είναι αρκετό για την αναπαράσταση της κυματομορφής ομιλίας. [166]

Παρόλα αυτά, επειδή τα ακουστικά κύματα των οχημάτων έχουν διαφορετικά χαρακτηριστικά από αυτά της ομιλίας, η χρήση ενός αλφάβητου μεγέθους 28 συμβόλων δεν αποτελεί την βέλτιστη λύση. Πλήθος μελετών περιγράφουν τρόπους για τον υπολογισμό του κατάλληλου μεγέθους της αλφάβητου σε συνάρτηση με τα χαρακτηριστικά των ακουστικών κυμάτων που χρειάζεται να κατηγοριοποιήσουν. Στην συγκεκριμένη μελέτη θα χρησιμοποιήσουμε ένα έτοιμο αλφάβητο το οποίο προέκυψε από την μελέτη της ομάδας του Μαζαράκη [8].

	S = 0	S = 1	S = 2	S = 3	S = 4	S = 5
D = 1	1					
D = 2	2	2				
D = 3	3	3	3			
D = 4	4	4	4	4		
D = 5	5	5	5	5		
D = 6	6	6	6	6	6	
D = 7	6	6	6	6	6	
D = 8	7	8	8	8	8	8
D = 9	7	8	8	8	8	8
D = 10	7	8	8	8	8	8
D = 11	9	10	10	10	10	10
D = 12	9	10	10	10	10	10
D = 13	9	10	10	10	10	10
D = 14	11	12	13	13	13	13
D = 15	11	12	13	13	13	13
D = 16	11	12	13	13	13	13
D = 17	11	12	13	13	13	13
D = 18	11	12	13	13	13	13
D = 19	14	15	16	17	17	17
D = 20	14	15	16	17	17	17
D = 21	14	15	16	17	17	17
D = 22	14	15	16	17	17	17
D = 23	14	15	16	17	17	17
D = 24	18	19	20	21	22	22
D = 25	18	19	20	21	22	22
D = 26	18	19	20	21	22	22
D = 27	18	19	20	21	22	22
D = 28	18	19	20	21	22	22
D = 29	18	19	20	21	22	22
D = 30	18	19	20	21	22	22
D = 31	23	24	25	26	27	28
D = 32	23	24	25	26	27	28
D = 33	23	24	25	26	27	28
D = 34	23	24	25	26	27	28
D = 35	23	24	25	26	27	28
D = 36	23	24	25	26	27	28
D = 37	23	24	25	26	27	28

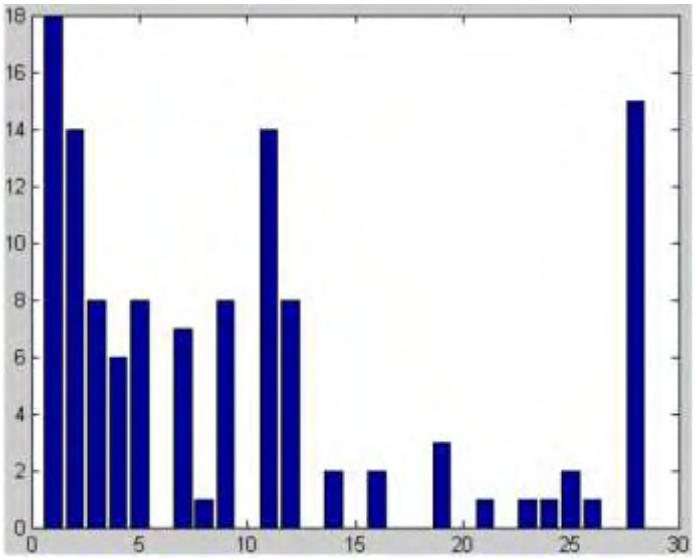
Εικόνα 77: Ένα παράδειγμα αλφάβητου της μεθόδου TESPAR.

Ο πίνακας – S

Όπως αναφέραμε παραπάνω, κάθε ακουστικό κύμα κωδικοποιείται σε μια σειρά από σύμβολα τα οποία βασίζονται στις παραμέτρους ***D*** και ***S*** του κάθε ***Epoch*** τμήματος. Στην περίπτωση όπου ο αριθμός των ***Epoch*** τμημάτων μιας κυματομορφής είναι μεγάλος, θα δημιουργηθεί ένα αντίστοιχα μεγάλο πλήθος συμβόλων το οποίο θα είναι δύσκολα επεξεργάσιμο.

Ένας έξυπνος τρόπος διαχείρισης αυτού του μεγάλου πλήθους συμβόλων, είναι η τοποθέτησή τους μέσα σε ειδικούς πίνακες, με αντιπροσωπευτικό παράδειγμα τον πίνακα S. Πρόκειται για έναν μονοδιάστατο πίνακα, μεγέθους ίσο με το μέγεθος του αλφάβητου που χρησιμοποιήθηκε για την δημιουργία των συμβόλων. Στο πίνακα αυτόν αποθηκεύεται το πλήθος των επαναλήψεων όπου εμφανίζεται κάθε σύμβολο του αλφάβητου στο ακουστικό κύμα.

Παρακάτω φαίνεται ένα παράδειγμα ενός πίνακα τύπου S.



Εικόνα 78: Ο πίνακας-S της μεθόδους TESPAR.

7.3 Υλοποίηση

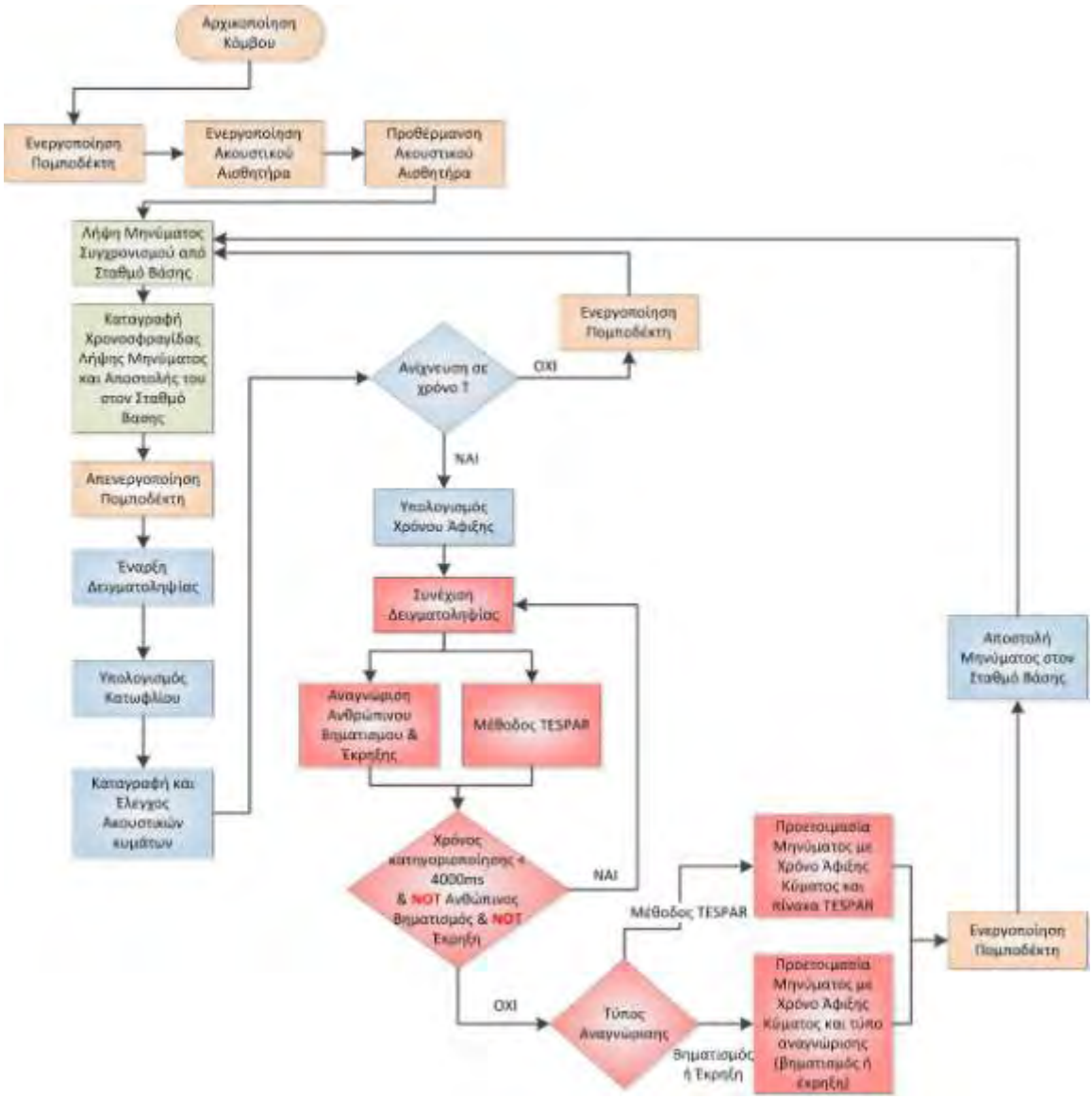
Η κατηγοριοποίηση των απειλών επαφίεται στην χρήση των παραπάνω τριών μεθόδων. Στην χρήση δηλαδή των

- δύο ευρετικών μεθόδων για την αναγνώριση ανθρώπινου βαδίσματος και έκρηξης
- στην χρήση της μεθόδου TESPAR για την αναγνώριση πιο πολύπλοκων ακουστικών κυμάτων, όπως είναι αυτά των οχημάτων.

Η αποτελεσματική εκτέλεση αυτών των τριών μεθόδων επιτυγχάνεται μέσω της ενσωμάτωσής τους σε ένα γενικότερο πλαίσιο λειτουργικότητας του ασύρματου κόμβου. Αυτό το γενικό πλαίσιο λειτουργικότητας αναλαμβάνει να συνδυάσει την λειτουργίες της κατηγοριοποίησης των απειλών με αυτές της μεθόδου εντοπισμού και συγχρονισμού των κόμβων που περιγράφτηκαν σε προηγούμενο κεφάλαιο. Με αυτό τον τρόπο επιτυγχάνεται η εκτέλεση της επιθυμητής λειτουργικότητας για τους κόμβους παρέχοντας παράλληλα την βέλτιστη ενεργειακά διαχείριση των πόρων τους.

7.3.1 Γενικό πλαίσιο λειτουργικότητας

Οι λειτουργίες της κατηγοριοποίησης των απειλών ενσωματώνονται μέσα στο γενικότερο πλαίσιο λειτουργικότητας του κόμβο με την μορφή νέων καταστάσεων λειτουργιάς. Όπως βλέπουμε και την παρακάτω εικόνα, στον κόμβο προστίθενται νέες καταστάσεις λειτουργίας (χρώμα κόκκινο). Αυτές οι καταστάσεις αναλαμβάνουν να εκτελέσουν τις μεθόδους κατηγοριοποίησης των απειλών. Λεπτομέρειες σχετικά με την υλοποίηση των καταστάσεων αυτών υπάρχουν στις επόμενες ενότητες.



Εικόνα 79: Το γενικό πλαίσιο λειτουργικότητας των κόμβων για την εκτέλεση εντοπισμού και κατηγοριοποίησης των απειλών.

Ο κόμβος αφού κατά την διάρκεια εκτέλεσης της μεθόδου εντοπισμού του κύματος καταγράφει τα ακουστικά κύματα. Κάθε τιμή του κύματος που καταγράφεται ελέγχεται προκειμένου να διαπιστωθεί αν υπερβαίνει την στάθμη του κατωφλίου. Στην περίπτωση όπου διαπιστωθεί ότι ένα κύμα υπερβαίνει το κατώφλι, υπολογίζεται ο χρόνος άφιξής του και στην συνέχεια μεταβαίνει στις καταστάσεις που είναι υπεύθυνες για την αναγνώριση της πηγής του συγκεκριμένου κύματος.

Με την προσθήκη των καταστάσεων κατηγοριοποίησης, ο κόμβος αφού ανιχνεύσει την ύπαρξη μίας απειλής, συνεχίζει την καταγραφή των ακουστικού κύματος για διάστημα 5 s. Κατά την διάρκεια αυτού του διαστήματος εκτελούνται οι μέθοδοι αναγνώρισης ανθρώπινου βηματισμού και εκρήξεων καθώς και η μέθοδος TESPAR.

Αυτές οι μέθοδοι αναγνώρισης εκτελούνται παράλληλα με τον παρακάτω τρόπο. Η μέθοδος αναγνώρισης εκρήξεων και ανθρώπινου βηματισμού απαιτούν διάρκεια

εκτέλεσης 3 sec προκειμένου να αποφανθούν για τον τύπο της πηγής του κύματος (μπορούν αν αποφανθούν μόνο αν είναι ή όχι ανθρώπινος βηματισμός ή έκρηξη). Στην περίπτωση όπου γίνει επιτυχής αναγνώρισης ενός από τους παραπάνω τύπους στέλνεται ειδοποίηση και σταματάει η καταγραφή του κύματος νωρίτερα από τα 4 sec.

Παράλληλα με την εκτέλεσης των παραπάνω μεθόδων η μέθοδος αναγνώρισης TESPAR καταγράφει της τιμές και εκτελεί σταδιακά την επεξεργασία τους (κωδικοποίηση του κύματος σε σειρά συμβόλων). Η μέθοδος αυτή εκτελείται καθόλο το διάστημα καταγραφής του κύματος (4 sec).

Όπως είναι φανερό, η διάρκεια του διαστήματος καταγραφής του κύματος με σκοπό την κατηγοριοποίησή του εξαρτάται από τα αποτελέσματα των μεθόδων κατηγοριοποίησης. Έτσι :

- στην περίπτωση όπου γίνει αναγνώριση έκρηξης ή ανθρώπινου βηματισμού η καταγραφή διαρκεί 3 s.
- στην αντίθετη περίπτωση η καταγραφή διαρκεί το μέγιστο δυνατό, 4 s.

Επομένως, μετά την λήξη της καταγραφής του κύματος, ανάλογα με τα αποτελέσματα των μεθόδων αποστέλλεται το κατάλληλο μήνυμα στον σταθμό βάσης.

7.3.2 Πακέτα ασύρματης επικοινωνίας

Τα περιεχόμενα του μηνύματος, που αποστέλλεται στον σταθμό βάσης, εξαρτώνται από το αποτέλεσμα των μεθόδων αναγνώρισης. Έτσι στην περίπτωση όπου:

- έχει γίνει αναγνώριση της απειλής ως έκρηξη ή ανθρώπινος βηματισμός, τα περιεχόμενα του μηνύματος είναι μόνο η κλάση της κατηγοριοποίησης της απειλής.
- δεν έχει γίνει αναγνώριση των παραπάνω τύπων και έχει ολοκληρωθεί η εκτέλεση της μεθόδου TESPAR, τα περιεχόμενα του μηνύματος είναι ο ειδικός πίνακας-S της μεθόδου, ο οποίος περιέχει το πλήθος εμφανίσεων κάθε συμβόλου του αλφάβητου στο καταγεγραμμένο κύμα.

Για λόγους μείωσης της κατανάλωσης ενέργειας, τα παραπάνω δεδομένα δεν θα αποσταλούν μέσω ενός νέου μηνύματος, αλλά θα ενσωματωθούν μέσα στο μήνυμα EventMsg. Το μήνυμα EventMsg ήταν υπεύθυνο για την μεταφορά στον σταθμό βάσης του χρόνου άφιξης του κύματος της απειλής στον κάθε κόμβο. Πλέον με την ενσωμάτωση των αποτελεσμάτων κατηγοριοποίησης το μήνυμα αποκτάει δύο εκδώσεις (ανάλογα με το αποτέλεσμα).

- Το μήνυμα **EventHeuristicMsg** είναι υπεύθυνο για την μεταφορά της κλάσης κατηγοριοποίησης στην περίπτωση όπου έχει αναγνωριστεί επιτυχώς μία έκρηξη ή ένα ανθρώπινο βάδισμα. Τα επιπλέον δεδομένα που προστίθενται σε αυτά του EventMsg είναι η μεταβλητή: ***uint8 detectClass*** που περιέχει τον τύπο της κατηγοριοποίησης της απειλής.
- Το μήνυμα **EventTesparMsg** είναι υπεύθυνο για την αποστολή του πίνακα-S της κλάσης TESPAR. Τα επιπλέον δεδομένα που προστίθενται σε αυτά του EventMsg είναι ο πίνακας ***uint16 arrayS[40]***. Το μέγεθος του πίνακα εξαρτάται από το μέγεθος του αλφάβητου που χρησιμοποιείται από την μέθοδο. Στην περίπτωσή μας, το μέγεθος είναι 40.

Εικόνα 80: Οι δύο εκδώσεις του μηνύματος EventMsg.

7.3.3 Υλοποίηση στο επίπεδο των ασύρματων κόμβων

Η υλοποίηση των μεθόδων αποτελείται από 2 επίπεδα. Οι λειτουργίες των δύο αυτών επιπέδων εξαρτώνται από την μορφολογία του ασύρματου δικτύου. Έτσι το 1^{ο} επίπεδο υπολογισμών λαμβάνει χώρα στο επίπεδο των ασύρματων κόμβων, ενώ το 2^{ο} επίπεδο υπολογισμών εκτελείται στο επίπεδο του σταθμού βάσης.

Οι ενέργειας που εκτελούνται στο επίπεδο των ασύρματων κόμβων αφορούν τον έλεγχο των ακουστικών κυμάτων και την επεξεργασία τους προκειμένου να εξαχθούν τα χαρακτηριστικά διανύσματα. Στην περίπτωση αναγνώρισης ανθρώπινου βηματισμού ή έκρηξης, ο κόμβος αποστέλλει στον σταθμό βάσης ένα μήνυμα με την κλάση της κατηγοριοποίησης της απειλής. Στην περίπτωση εκτέλεσης της μεθόδου TESPAR, ο κόμβος δημιουργεί ένα πίνακα-S τον οποίο και αποστέλλει στον σταθμό βάσης. Τα δεδομένα αυτά αφού ληφθούν από τον σταθμό βάσης, επεξεργάζονται και συγκρίνονται με τα δεδομένα των υπόλοιπων κόμβων του δικτύου προκειμένου να γίνει η αναγνώριση της απειλής.

Παρατηρώντας το σύνολο των στοιχείων που χρησιμοποιούνται για την υλοποίηση των μεθόδων κατηγοριοποίησης γίνεται εύκολα αντιληπτό ότι μεγάλο μέρος αυτών αποτελεί κομμάτι της υλοποίησης της μεθόδου ανίχνευσης των απειλών (όπως περιγράφτηκε στην Ενότητα 6.4.1). Το κοινό αυτό σύνολο των στοιχείων οφείλεται στο γεγονός ότι οι μέθοδοι εντοπισμού και χαρακτηρισμού των απειλών λειτουργούν κάτω από ένα ευρύτερο κοινό πλαίσιο λειτουργικότητας.

7.3.3.1 Μέθοδος αναγνώρισης ανθρώπινου βηματισμού - εκρήξεων

Η υλοποίηση της μεθόδου για χρήσης της στους κόμβους Mica2 έγινε με την γλώσσα προγραμματισμού nesC και το λειτουργικό σύστημα TinyOS 2. Η εφαρμογή αποτελείται από βασικό (configuration) αρχείο SurveilAppC, το οποίο ορίζει τις συνδέσεις (wirings) μεταξύ των διάφορων στοιχείων και των διεπαφών τους. Τα στοιχεία που χρησιμοποιούνται είναι:

- **MainC:** αποτελεί το βασικό στοιχείο κάθε TinyOS εφαρμογής
- **LedsC:** παρέχει πρόσβαση στα leds του κόμβου (χρήσιμα για την απασφαλμάτωση του προγράμματος).
- **LocalTime:** πρόκειται για έναν 32-bit μετρητή ο οποίος περιέχει κάθε φορά την τρέχων χρονική στιγμή του κόμβου.

- **ActiveMessageC:** προσφέρει τις βασικές λειτουργίες για την ασύρματη επικοινωνία του κόμβου.
- **MicrophoneC:** ενεργοποιεί τον ακουστικό αισθητήρα, τον προθερμαίνει, ρυθμίζει διάφορα χαρακτηριστικά της λειτουργίας του (π.χ. gain) και δειγματοληπτεί τον αισθητήρα
- **DetectC:** αναλαμβάνει την χρήση των ακουστικών δεδομένων για τον υπολογισμό του κατωφλίου, τον έλεγχο ενός ακουστικού κύματος για την υπέρβασή του καθώς και τον εντοπισμό του μηδενικού του σημείου για τον υπολογισμό του χρόνου άφιξης του κύματος.
- **HeuristicCharactC:** αναλαμβάνει τον έλεγχο της «συμπεριφοράς» του ακουστικού κύματος με σκοπό την αναγνώριση της κλάσης του σε ανθρώπινο βηματισμού ή έκρηξη.
- **SurveilC:** πρόκειται για το κεντρικό αρχείο του προγράμματος, το οποίο αναλαμβάνει να διαχειριστεί όλα τα υπόλοιπα στοιχεία και διεπαφές ώστε ο κόμβος να εκτελεί σωστά τις διάφορες λειτουργίες και μεθόδους του καθώς και να μεταβαίνει στις αντίστοιχες κάθε φορά καταστάσεις λειτουργίας του.

Με την εκκίνηση του κόμβου, το πρόγραμμα ξεκινάει με την εκτέλεση του LocateC και συγκεκριμένα με την μέθοδο ***Boot.booted()***. Η συγκεκριμένη μέθοδος αρχικοποιεί κατά σειρά τα υποσυστήματα των leds, του πομποδέκτη (***ActiveMessageC.start()***) και του ακουστικού αισθητήρα (***MicrophoneC.start()***).

Στην συνέχεια εκτελούνται βήματα που περιγράφηκαν στην Ενότητα 6.4.1 και αφορούν την αρχικοποίηση του κόμβου και του ακουστικού αισθητήρα, την εκτέλεση των λειτουργιών συγχρονισμού, τον υπολογισμό της στάθμης του κατωφλίου καθώς και την εκτέλεση λειτουργιών για την καταγραφή και τον έλεγχο του κατωφλίου των ακουστικών κυμάτων. Ο έλεγχος του κάθε στιγμιότυπου του κύματος με την στάθμη του κατωφλίου εκτελείται μέσα στο αρχείο DetectC.

Στην περίπτωση όπου ανιχνευτεί ένα κύμα το οποίο υπερβαίνει την στάθμη του κατωφλίου, υπολογίζεται ο χρόνος άφιξης του κύματος και στην συνέχει καλείται το αρχείο HeuristicCharactC προκειμένου να κάνει τους απαραίτητους υπολογισμούς για την κατηγοριοποίησή του.

HeuristicCharactC

Το αρχείο HeuristicCharactC καλείται αμέσως μετά την ανίχνευση ενός κύματος-απειλής. Ο συγκεκριμένος κώδικας λαμβάνει μέσω της κλήσης της συνάρτησης ***HeuristicCharactC.getThreshSignal(uint16 signal)*** κάθε καταγραφή του κύματος η οποία υπερβαίνει το κατώφλι. Η συνάρτηση αυτή αφού λάβει την πρώτη καταγραφή, ενεργοποιεί έναν timer ο οποίος θα παράγει μια διακοπή μετά από 150 ms. Το χρονικό αυτό διάστημα που μεσολαβεί μέχρι την διακοπή του timer, η μέθοδος αγνοεί τις καταγραφές που δέχεται. Ο σκοπός αυτού του χρονικού διαστήματος αναμονής είναι η αγνόηση του διαστήματος απόσβεσης του ακουστικού κύματος. Αφού ενεργοποιηθεί η διακοπή του timer, η μέθοδος αναμένει την ύπαρξη μίας νέας καταγραφής με τιμή υψηλότερη αυτής του κατωφλίου.

Στην περίπτωση όπου αυτή η καταγραφή δεν φτάσει σε διάστημα από 300 - 1000 ms , η μέθοδος αποκλείει την περίπτωση ύπαρξης ανθρώπινου βηματισμού. Οπότε συνεχίζει

την αναμονή νέας τιμής για περίπου 2s. Στην περίπτωση όπου δεν λάβει μια νέα τιμή σε αυτό το διάστημα, η μέθοδος αναγνωρίζει το κύμα ως έκρηξη και στέλνει την κατάλληλη ειδοποίηση στο κεντρικό αρχείο ελέγχου SurveiC μέσω της συνάρτησης ***SurveilC.detectExplosion()***. .

Εναλλακτικά, στην περίπτωση όπου ένα στιγμιότυπο του κύματος με τιμή μεγαλύτερη του κατωφλίου φτάσει σε χρονικό διάστημα 300-1000ms μετά την ενεργοποίηση της διακοπής του timer, το κύμα αναγνωρίζεται ως εν δυνάμει ανθρώπινος βηματισμός, και επαναλαμβάνει την εκτέλεσή του 2 ακόμα φορές. Αν και στις 12 επόμενες επαναλήψεις, το κύμα αναγνωριστεί ως ανθρώπινος βηματισμός, η μέθοδος στέλνει μια ειδοποίηση αναγνώρισης στο κεντρικό αρχείο ελέγχου SurveiC μέσω της συνάρτησης ***SurveilC.detectFootestps()***.

Αναλυτικά τα βήματα που εκτελούνται στην κύρια συνάρτηση **getThreshSignal()** του αρχείου HeuristicChatactC είναι:

```
cur_state = STATE_1;
count_footsteps;                    //περιέχει το πλήθος συνεχόμενων βημάτων που έχει εντοπίσει η μέθοδος

void HeuristicCharactC.getThreshSignal(uint16 signal){      //καλείται κάθε φορά που εντοπίζεται ένα σήμα
                                                            //με τιμή μεγαλύτερη του κατωφλίου

        if(cur_state == STATE_1){
                count_footsteps = 0;        //μηδενισμός του πλήθους συνεχόμενων βημάτων καθώς
                                            //ξεκινάει ανάλυση νέου κύματος
                cur_state = STATE_2;
                call Timer.startOneShot(150);       //καλούμε τον timer ώστε να ενεργοποιήσει μια
                                                    //διακοπή μετά από 150 ms
        }

        if(cur_state == STATE_2 && έχει ενεργοποιηθεί η διακοπή του timer){
                if(334 < χρόνος από την προηγούμενη κλίση < 1000){      //εντοπισμός ενός βήματος
                        count_footsteps++;

                        if(count_footsteps == 3){                   //εντοπισμός 3 συνεχόμενων βημάτων

                                cur_state = STATE_3;
                                //ενημέρωση του κεντρικού αρχείου SurveilC για τον αναγνώριση του
                                //κύματος ως ανθρώπινος βηματισμός
                                SurveilC.detectFootestps();
                        }
                }
                if( χρόνος από την προηγούμενη κλίση < 3000){
                        //αν έρθει κάποιο σήμα σε χρόνο  από την προηγούμενη κλήση όπου ισχύει:
                        //1000 < χρόνος < 3000 , δεν υπάρχει καμία αναγνώριση από την συγκεκριμένη
                        //μέθοδο.

                        cur_state = STATE_1;   //επιστροφή της μεθόδου στην αρχική της κατάσταση
                }
        }

        if( χρόνος από την προηγούμενη κλίση >= 3000
                && δεν έχει καταγραφεί άλλο στιγμιότυπο με τιμή μεγαλύτερη από το κατώφλι){

                cur_state = STATE_4;
                //ενημέρωση του κεντρικού αρχείου SurveilC για τον αναγνώριση του
                //κύματος ως έκρηξη.
                SurveilC.detectExplosion();

        }
}
```

Το αρχείο SurveiC με την σειρά του, αφού λάβει μία από της παραπάνω κλήσης συναρτήσεων σταματάει την καταγραφή των ακουστικών κυμάτων (ακόμα και την καταγραφή που προοριζόταν για την μέθοδο TESPAR) , ενεργοποιεί τον πομποδέκτη και ετοιμάσει το μήνυμα που θα σταλεί στον σταθμό βάσης. Το μήνυμα που θα σταλεί είναι του τύπου EventHeuristicMsg και μέσα ενσωματώνει την κλάση που αναγνωριστικέ, βάση της συνάρτηση του SurveiC που κλήθηκε.

7.3.3.2 Μέθοδος αναγνώρισης με την χρήση της μεθόδου TESPAR

Η υλοποίηση της μεθόδου TESPAR βασίζεται στην υλοποίηση που περιγράφεται στα πλαίσια της έρευνας του Μαζαράκη [8]. Στην συγκεκριμένη διατριβή, γίνεται μια πλήρη έρευνα της μεθόδου TESPAR και μελετάται η καταλληλότητα της για χρήση στα ακουστικά και σεισμικά κύματα με σκοπό την κατηγοριοποίηση της πηγής των κυμάτων αυτών. Η υλοποίηση της μεθόδου, που περιγράφεται, επιτυγχάνει πολύ καλά αποτελέσματα τόσο στην ακρίβεια της κατηγοριοποίησης όσο και στην διαχείριση των ενεργειακών πόρων των κόμβων.

Για την υλοποίηση της μεθόδου, που περιγράφουμε στην συγκεκριμένη διατριβή, χρησιμοποιήθηκε η γλώσσα προγραμματισμού nesC και το λειτουργικό σύστημα TinyOS 2. Η ανάπτυξη της μεθόδου έγινε στα πλαίσια των απαιτήσεων και των περιορισμών που εισάγουν οι ασύρματοι κόμβοι Mica2. Η εφαρμογή αποτελείται από βασικό (configuration) αρχείο SurveilAppC, το οποίο ορίζει τις συνδέσεις (wirings) μεταξύ των διάφορων στοιχείων και των διεπαφών τους. Τα στοιχεία που χρησιμοποιούνται είναι:

- **MainC:** αποτελεί το βασικό στοιχείο κάθε TinyOS εφαρμογής
- **LedsC:** παρέχει πρόσβαση στα leds του κόμβου (χρήσιμα για την απασφαλμάτωση του προγράμματος).
- **LocalTime:** πρόκειται για έναν 32-bit μετρητή ο οποίος περιέχει κάθε φορά την τρέχων χρονική στιγμή του κόμβου.
- **ActiveMessageC:** προσφέρει τις βασικές λειτουργίες για την ασύρματη επικοινωνία του κόμβου.
- **MicrophoneC:** ενεργοποιεί τον ακουστικό αισθητήρα, τον προθερμαίνει, ρυθμίζει διάφορα χαρακτηριστικά της λειτουργίας του (π.χ. gain) και δειγματοληπτεί τον αισθητήρα
- **DetectC:** αναλαμβάνει την χρήση των ακουστικών δεδομένων για τον υπολογισμό του κατωφλίου, τον έλεγχο ενός ακουστικού κύματος για την υπέρβασή του καθώς και τον εντοπισμό του μηδενικού του σημείου για τον υπολογισμό του χρόνου άφιξης του κύματος.
- **TESPARCharactC:** αναλαμβάνει την εκτέλεση των υπολογισμών που απαιτούνται από την μέθοδο κατηγοριοποίησης TESPAR.
- **SurveilC:** πρόκειται για το κεντρικό αρχείο του προγράμματος, το οποίο αναλαμβάνει να διαχειριστεί όλα τα υπόλοιπα στοιχεία και διεπαφές ώστε ο κόμβος να εκτελεί σωστά τις διάφορες λειτουργίες και μεθόδους του καθώς και να μεταβαίνει στις αντίστοιχες κάθε φορά καταστάσεις λειτουργίας του.

Η εκτέλεση της μεθόδου TESPAR λειτουργεί με παρόμοιο τρόπο με αυτόν των ευρετικών μεθόδων που περιγράφτηκε παραπάνω. Το γενικό αρχείο ελέγχου SurveiC αναλαμβάνει την διαχείριση όλων των επιμέρους υποπρογραμμάτων. Έτσι αρχικά

γίνονται οι απαραίτητες ενέργειας για την αρχικοποίηση του κόμβου, την εκτέλεση των λειτουργιών συγχρονισμού καθώς και τον υπολογισμό της στάθμης του κατωφλίου του. Στην συνέχεια και αφού ξεκινήσει η καταγραφή των ακουστικών αισθητήρων μέσω του αρχείου DetectC γίνεται ο έλεγχος για την ύπαρξη κάποιου στιγμιότυπου του κύματος το οποίο ξεπερνάει την στάθμη κατωφλίου.

Στην περίπτωση όπου βρεθεί κάποιο τέτοιο στιγμιότυπο, υπολογίζεται ο χρόνος άφιξης του στον κόμβο και στην συνέχεια καλείται η συνάρτηση ***TESPARCharactC.getThreshSignal(uint16 signal)*** του αρχείου TESPARCharactC. Η συγκεκριμένη συνάρτηση καλείται για κάθε τιμή που καταγράφει η DetectC για ένα χρονικό διάστημα 4sec μετά ανίχνευση ενός κύματος που υπερβαίνει το κατώφλι. Το χρονικό αυτό διάστημα των 4sec απαιτείται από την μέθοδο ώστε να πάρει έναν αντιπροσωπευτικό δείγματα καταγραφών του κύματος με σκοπό να εξάγει συμπέρασμα για την κλάση του με όσο το δυνατό μεγαλύτερη ακρίβεια και αξιοπιστία.

Για κάθε κλήση της η συνάρτηση εκτελεί της παρακάτω ενέργειες:

```
πίνακα-S          //γίνεται αρχικοποίηση του ειδικού πίνακα-S της μεθόδου TESPAR. Το μέγεθος του
                  //πίνακα είναι ίσο με το μέγεθος του αλφάβητου που χρησιμοποιείται. Στην
                  //συγκεκριμένη περίπτωση είναι 40.

void TESPARCharactC.getThreshSignal(uint16 signal){      //καλείται για πρώτη φορά μόλις
        //εντοπιστεί ένα σήμα με τιμή μεγαλύτερη του κατωφλίου.
        //Επειτα καλείται για κάθε καταγραφή για διάστημα 4s.

        if( signal ανήκει στο τρέχον διάστημα Epoch){
                Υπολογισμός των χαρακτηριστικών του τρέχοντος διαστήματος Epoch.
        }
        else if( signal σηματοδοτεί δημιουργία νέου διαστήματος Epoch ){
                Μετατροπή των χαρακτηριστικών D & S του προηγούμενου Epoch στο
                αντίστοιχο σύμβολο του αλφάβητου.

                Προσθήκη του συμβόλου στην αντίστοιχη θέση του πίνακα-S.
        }

        if( χρόνος από την πρώτη κλήση της συνάρτηση >= 4s){
                //ενημέρωση του κεντρικού αρχείου SurveilC για την ολοκλήρωση της μεθόδου
                //TESPAR και αποστολή του πίνακα S
                SurveilC.detectTESPAR(πινακαsS);
        }
}
```

Μετά την ολοκλήρωση του χρονικού διαστήματος των 4sec, η μέθοδος ολοκληρώνει την εκτέλεσή της μέσω της κλήσης της συνάρτησης ***SurveilC.detectTESPAR(πινακαsS)*** του αρχείου SurveiC. Η συγκεκριμένη συνάρτηση χρησιμοποιείται προκειμένου να σηματοδοτείται την ολοκλήρωση της μεθόδου στο αρχείο SurveiC, αλλά και να προωθήσει σε αυτό τον πίνακαS, με τα αποτελέσματα των υπολογισμών της. Στην συνέχεια το αρχείο SurveiC, ολοκληρώνει την καταγραφή του ακουστικού κύματος, ενεργοποιεί τον ασύρματο πομποδέκτη του κόμβου και προετοιμάζει ένα μήνυμα τύπου

EventTESPARMSG και στέλνεται στον σταθμό βάσης. Στο συγκεκριμένο μήνυμα περιέχεται ο χρόνος άφιξης του μηνύματος στον κόμβο και ο πίνακαςS της μεθόδους κατηγοριοποίησης TESPAR.

Αλφάβητο TESPAR

Το αλφάβητο που χρησιμοποιήθηκε, αποτελεί αποτέλεσμα της έρευνας της ομάδας των Μαζαράκη και Αβαριτσιώτη [8]. Στην συγκεκριμένη έρευνα μελετήθηκε διεξοδικά η επίδραση του μεγέθους του αλφάβητου στην αποτελεσματικότητα της μεθόδου TESPAR. Έγιναν μελέτες τόσο σε περιβάλλοντα προσωμείωσης όσο και σε πραγματικές συνθήκες με σκοπό την εύρεση του βέλτιστου αλφάβητου για την κατηγοριοποίηση διάφορων τύπων οχημάτων, όπως αυτοκίνητα, λεοφωρεία, φορτηγά και μοτοσυκλέτες. Το αλφάβητο που προέκυψε είναι μεγέθους 40 συμβόλων και επιτυγχάνει ποσοστό, σωστής αναγνώρισης του τύπου του οχήματος, της τάξης του 80%. Το αλφάβητο που χρησιμοποιήθηκε είναι:

TinyOS TESPAR Alphabet						
D↓ S→	0	1	2	3	4	5
1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	3	3	3
4	4	5	5	5	5	5
5	6	7	7	7	7	7
6	8	9	9	9	9	9
7	10	11	11	11	11	11
8	12	13	13	13	13	13
9	14	15	15	15	15	15
10	14	15	15	15	15	15
11	16	17	18	18	18	18
12	16	17	18	18	18	18
13	19	20	21	21	21	21
14	19	20	21	21	21	21
15	22	22	23	23	23	23
16	22	22	23	23	23	23
17	22	22	23	23	23	23
18	24	24	25	25	26	26
19	24	24	25	25	26	26
20	24	24	25	25	26	26
21	24	24	25	25	26	26
22	27	27	28	28	29	29
23	27	27	28	28	29	29
24	27	27	28	28	29	29
25	27	27	28	28	29	29
26	27	27	28	28	29	29
27	30	30	31	31	32	33
28	30	30	31	31	32	33
29	30	30	31	31	32	33
30	30	30	31	31	32	33
31	30	30	31	31	32	33
32	30	30	31	31	32	33
33	30	30	31	31	32	33
34	34	34	35	35	36	36
35	34	34	35	35	36	36
36	34	34	35	35	36	36
37	34	34	35	35	36	36
38	34	34	35	35	36	36
39	34	34	35	35	36	36
40	34	34	35	35	36	36

Εικόνα 81: Το αλφάβητο που χρησιμοποιήθηκε από την μέθοδο κατηγοριοποίησης TESPAR [8].

7.3.4 Υλοποίηση στο επίπεδο του σταθμού βάσης

Στα πλαίσια της κατηγοριοποίησης των απειλών, ο σταθμός βάσης είναι υπεύθυνος για την συλλογή των μηνυμάτων κατηγοριοποίησης από τους ασύρματους κόμβους και την εκτέλεση συσχετίσεων. Ουσιαστικά ο ρόλος του σταθμού βάσης είναι να εκτελέσει τις απαραίτητες ενέργειες προκειμένου να εξάγει μια κλάση κατηγοριοποίηση για την κάθε απειλή, η οποία συνάδει με το σύνολο των αποτελεσμάτων κατηγοριοποίησης κάθε κόμβου ξεχωριστά.

Έτσι στην περίπτωση λήψης αποτελεσμάτων από τις ευρετικές μεθόδους κατηγοριοποίησης, ο σταθμός βάσης εξάγει το τελικό αποτέλεσμα βάση πλειοψηφίας. Συλλέγει δηλαδή τα μηνύματα τύπου EventHeureticMsg από το σύνολο των κόμβων και βρίσκει ποια από τις 2 κλάσεις (ανθρώπινο βάδισμα ή έκρηξη) αναγνωρίστηκε από τους περισσότερους κόμβους.

Στην περίπτωση λήψης μηνυμάτων τύπου EventTESPARMsg, ο σταθμός βάσης αναλαμβάνει να εξάγει το αποτέλεσμα της κατηγοριοποίησης χρησιμοποιώντας τους πίνακεςS που λαμβάνει από το σύνολο των ασύρματων κόμβων του δικτύου. Τα περιεχόμενα των πινάκωνS συγκρίνονται με μία βιβλιοθήκη γνωστών αποτελεσμάτων που κατέχει ο σταθμό βάσης. Το αποτέλεσμα της σύγκρισης είναι και το αποτέλεσμα της κατηγοριοποίησης. Η σύγκριση γίνεται από ένα έξυπνο σύστημα ελέγχου (για παράδειγμα ένα νευρωνικό δίκτυο) που εκτελείται στον σταθμό βάσης. Η βιβλιοθήκη των γνωστών αποτελεσμάτων έχει δημιουργηθεί στον σταθμό βάσης κατά την περίοδο αρχικοποίησης του συστήματος. Πριν την εκκίνηση της κανονικής λειτουργίας του, ο σταθμό βάσης μέσω των ασύρματων κόμβων καταγράφει ένα σύνολο γνωστών τύπων απειλών, εκτελείται η μέθοδος TESPAR για το σύνολο αυτών των καταγραφών και οι τελικοί πίνακεςS που δημιουργούνται αποθηκεύονται στον ίδιο τον σταθμό βάσης. Στην ουσία αυτό το σύνολο των αποθηκευμένων πινάκωνS αποτελεί το σύνολο εκπαίδευσης του νευρωνικού δικτύου που χρησιμοποιείται. Η υλοποίηση του νευρωνικού δικτύου είναι εκτός πλαισίων της συγκεκριμένης διατριβής, οπότε και δεν αναλύεται περεταίρω.

Στην περίπτωση όπου ο σταθμό βάσης λάβει μηνύματα και από τις 2 παραπάνω περιπτώσεις, επιλέγει να εκτελέσει την επιλέξει αυτή με τις περισσότερες εμφανίσεις.

7.4 Ενεργειακή Ανάλυση

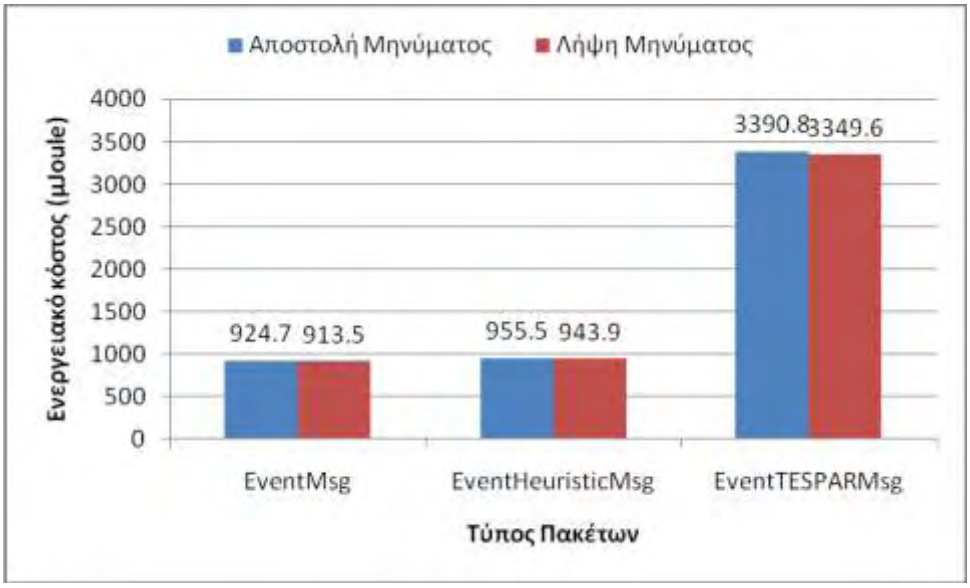
Παρακάτω ακολουθεί ανάλυση του ενεργειακού κόστους των μεθόδων κατηγοριοποίησης των απειλών. Ο υπολογισμός του ενεργειακού κόστους βασίστηκε στο περιβάλλον προσομοίωσης Avrora [95]. Ακολουθούν οι μετρήσεις:

7.4.1.1 <u>Ασύρματη λήψη – αποστολή πακέτων.</u>

Τα πακέτα μηνυμάτων χρησιμοποιούνται από τις μεθόδους κατηγοριοποίησης αφορούν δύο διαφορετικές εκδώσεις/επεκτάσεις του αρχικού τύπου μηνύματος EventMsg. Ο ακόλουθος πίνακας παρουσιάζει την κατανάλωση ενέργειας κάθε τύπου μηνύματος κατά την λήψη αλλά και την αποστολή του.

Πίνακας 24: Το ενεργειακό κόστος του μηνύματος EventMsg και των 2 επεκτάσεών του που χρησιμοποιούνται στις μεθόδους κατηγοριοποίησης.

Πακέτο	Μέγεθος Πακέτου	Ενεργειακό Κόστος Λήψης Πακέτου (μJoule)			Ενεργειακό Κόστος Αποστολής Πακέτου (μJoule)		
		Μικρο-ελεγκτή	Πομποδέκτης	Σύνολο	Μικρο-ελεγκτή	Πομποδέκτης	Σύνολο
EventMsg	30 byte (22 βοηθητικά + 8 δεδομένων)	284.544	628.992	913.53	284.544	640.224	924.76
EventHeuristicMsg	31 byte (22 βοηθητικά + 9 δεδομένων)	294.02	649.95	943.98	294.02	661.56	955.59
EventTESPARMsg	110 byte (22 βοηθητικά + 88 δεδομένων)	1043.32	2306.30	3349.63	1043.32	2347.48	3390.81



Εικόνα 82: Το συνολικό ενεργειακό κόστος που απαιτείται για την λήψη και την αποστολή των μηνυμάτων EventMsg, EventHeuristicMsg και EventTESPARMsg.

Όπως αναφέραμε παραπάνω, οι μεθόδου κατηγοριοποίησης ενσωματώνουν τα αποτελέσματά τους στο αρχικό τύπο μηνύματος EventMsg, δημιουργώντας έτσι δύο νέα μηνύματα το EventHeuristicMsg και το EventTESPARMsg. Η αιτία αυτής της ενσωμάτωσης είναι η εξοικονόμηση πόρων. Με αυτό τον τρόπο δηλαδή, ο ασύρματος κόμβος θα στείλει χρησιμοποιώντας μόνο ένα μήνυμα τις πληροφορίες που περιέχει κατεξοχήν το EventMsg μαζί με τα αποτελέσματα της κατηγοριοποίησης. Ουσιαστικά αυτή η εξοικονόμηση ενέργειας πηγάζει από το γεγονός ότι θα στείλουμε ένα πακέτο

αντί για 2, άρα θα έχουμε σημαντική μείωση του αριθμού των εκπεμπόμενων byte από τον κόμβο.

Πίνακας 25: Κατανάλωση ενέργειας των κόμβων στην περίπτωση χρήση ενός απλού EventMsg καιτ των δύο βελτιωμένων εκδόσεών του για την αποστολή των αποτελεσμάτων κατηγοριοποίησης των απειλών.

				Ενεργειακό κόστος χρήσης διαφορετικού τύπου μηνυμάτων			
				Χρήση απλής έκδοσης του EventMsg και ξεχωριστών μηνυμάτων για αποτελέσματα κατηγοριοποίησης.		**Χρήση βελτιωμένων εκδόσεων του EventMsg**	
Μήνυμα	**Λειτουργία**	**Μέγεθος μηνύματος**	**Ενεργειακό Κόστος (μJoule)**	**EventMsg + HeuristicMsg**	**EventMsg + TESPARMsg**	**EventHeuristicMsg**	**EventTESTPARMsg**
EventMsg	Αποστολή	30 byte (22βοηθητικά + 8 δεδομένων)	924.76	1* 924.76	1* 924.76		
	Λήψη		913.53				
HeuristicMsg	Αποστολή	27 byte (22βοηθητικά + 5 δεδομένων)	832.29	1*832.29			
	Λήψη		822.18				
TESPARMsg	Αποστολή	106 byte (22βοηθητικά + 84 δεδομένων)	3267.51		1*3267.51		
	Λήψη		3227.82				
EventHeuristicMsg	Αποστολή	31 byte (22 βοηθητικά + 9 δεδομένων)	955.59			1*955,59	
	Λήψη		943.98				
EventTESPARMsg	Αποστολή	110 byte (22 βοηθητικά + 88 δεδομένων)	3390.81				1*3390,81
	Λήψη		3349.63				
			Σύνολο bytes	30 + 27= **57**	30 + 106= **136**	**31**	**110**
			Σύνολο ενεργειακού κόστους (μJoule)	**1757**	**4192.27**	**955.59**	**3390.81**

Στην περίπτωση αποστολής δύο ξεχωριστών αρχείων παρατηρούμε ότι απαιτείται συνολικά:

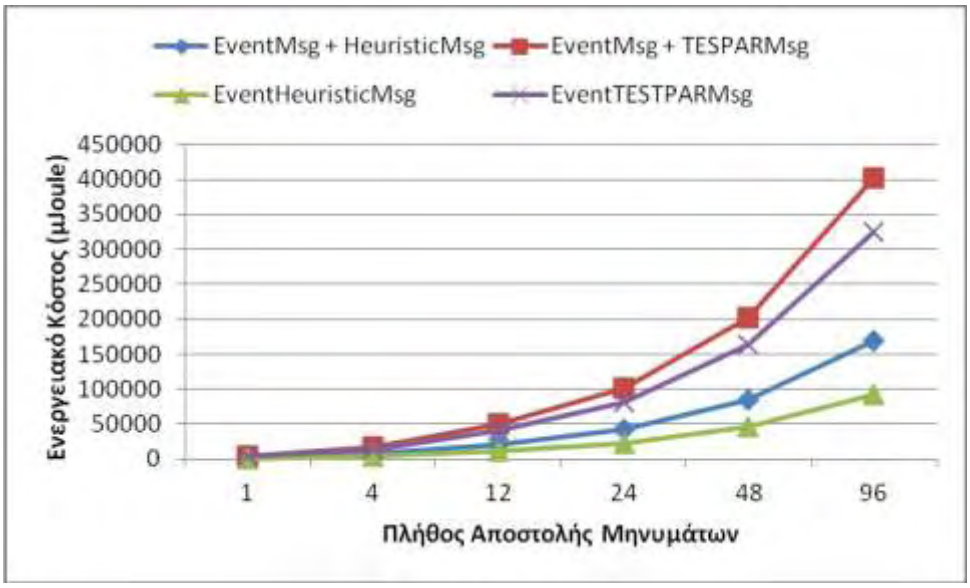
- αποστολή 57 bytes στην περίπτωση αποστολής των αποτελεσμάτων των ευρετικών μεθόδων για έναν γύρο εκτέλεσης.
- αποστολή 136 bytes στην περίπτωση αποστολής των αποτελεσμάτων της μεθόδου TESPAR για έναν γύρο εκτέλεσης.

Αντίστοιχα περίπτωση χρήσης των βελτιωμένων εκδόσεων του EventMsg οι οποίες ενσωματώνουν τα αποτελέσματα κατηγοριοποίησης απαιτείται συνολικά:

- αποστολή 31 bytes στην περίπτωση αποστολής των αποτελεσμάτων των ευρετικών μεθόδων για έναν γύρο εκτέλεσης.
- αποστολή 110 bytes στην περίπτωση αποστολής των αποτελεσμάτων της μεθόδου TESPAR για έναν γύρο εκτέλεσης.

Παρατηρούμε δηλαδή, ότι έχουμε μια μείωση του πλήθους των αποσταλμένων bytes της τάξης του 45% για την περίπτωση αποστολής των αποτελεσμάτων των ευρετικών μεθόδων και 20% για την περίπτωση αποστολής των αποτελεσμάτων της μεθόδου TESPAR.

Αντίστοιχα, η μείωση του ενεργειακού κόστους για τις παραπάνω περιπτώσεις κυμαίνεται στα ίδια επίπεδα.



Εικόνα 83:Το ενεργειακό κόστος της χρήσης ή μη, κοινού μηνύματος για την αποστολή των αποτελεσμάτων κατηγοριοποίησης.

7.4.1.2 Ευρετικοί Μέθοδοι Κατηγοριοποίησης

Η μέτρηση του ενεργειακού κόστους για κάθε μέθοδο κατηγοριοποίησης που χρησιμοποιούν οι κόμβοι θα γίνει από κοινού. Το μέγιστο χρονικό διάστημα κατηγοριοποίησης για κάθε κόμβο ανά κύκλο εκτέλεσης είναι 4sec. Σε ποσοστό 75% αυτού του διάστημα (3 sec) αυτοί οι μέθοδοι κατηγοριοποίησης εκτελούνται παράλληλα

(Στην πραγματικότητα δεν είναι παράλληλα, αλλά σειριακά.). Η πραγματική σειρά εκτέλεσης των ενεργειών είναι:

```
Καταγραφή του κύματος.

Έλεγχος της τιμής του για υπέρβαση του κατωφλίου

if( υπάρχει υπέρβαση ){

        if( 1η υπέρβαση κατά την διάρκεια του τρέχοντος κύκλου εκτέλεσης ){

                Υπολογίζεται ο χρόνος άφιξης του κύματος

        }

        Καλείται η μέθοδος για την αναγνώρισης του βηματισμού και της έκρηξης,
}

if( NOT 1η υπέρβαση κατά την διάρκεια του τρέχοντος κύκλου εκτέλεσης ){

        Καλείται η μέθοδος TESPAR
}
```

Στην παραπάνω σειρά εκτέλεσης των εντολών βλέπουμε ότι ο χρόνος άφιξης υπολογίζεται μόνο για το πρώτο κύμα που θα καταγραφεί, στην διάρκεια ενός κύκλου εκτέλεσης, και το οποίο έχει τιμή μεγαλύτερη της στάθμης του κατωφλίου. Αντίθετα βλέπουμε ότι μέθοδος TESPAR καλείται για όλες τις καταγραφές που διαδέχονται αυτή που υπερέβη $1^{η}$ το κατώφλι. Αυτό οφείλεται στον περιορισμένο διαθέσιμο χρόνο που υπάρχει ανάμεσα σε δύο διαδοχικές καταγραφές. Ο χρόνος που μεσολαβεί ανάμεσα σε δύο διαδοχικές καταγραφές είναι 100μs (συχνότητα δειγματοληψίας 10kHz.). Σε αυτό το διάστημα των 100μs θα πρέπει να εκτελεστούν όλες οι απαραίτητες ενέργειες.

Ο παρακάτω πίνακα παρουσιάζει τους χρόνους εκτέλεσης κάθε μεθόδου.

Πίνακας 26: Χρόνοι εκτέλεσης μεθόδων κατηγοριοποίησης

Εντολή	Χρόνος εκτέλεσης (μsec)
Καταγραφή κύματος	28
Έλεγχος υπέρβασης κατωφλίου	15
Υπολογισμός χρόνου άφιξης	30
Ευρετική Μέθοδος	17
Μέθοδος TESPAR	35

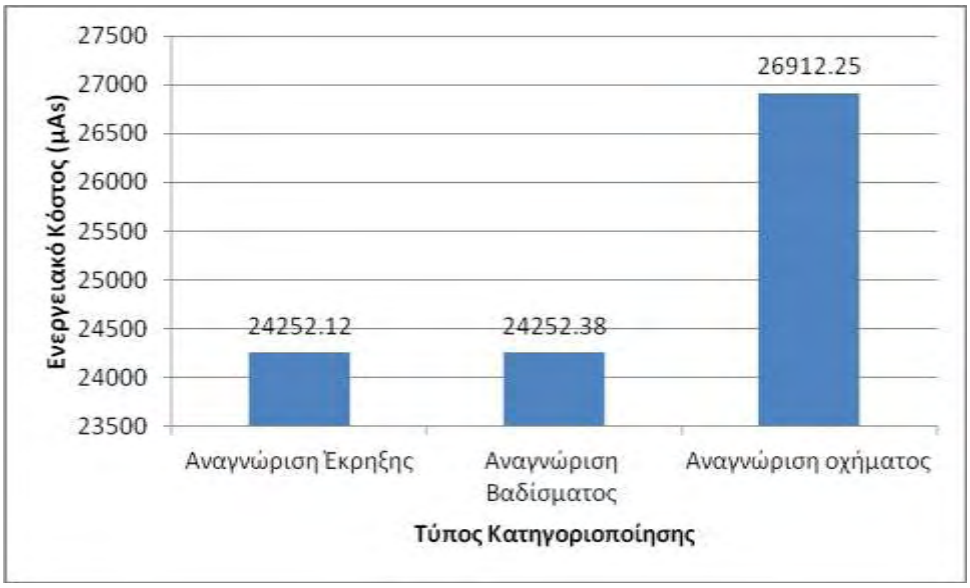
Ο συνολικός χρόνος εκτέλεσης των εντολών στην περίπτωση ύπαρξης μιας καταγραφής που υπερβαίνει το κατώφλι είναι 125μsec, αρκετά μεγαλύτερος δηλαδή από τον διαθέσιμο. Η λύση σε αυτό το πρόβλημα είναι να αποφύγουμε την «ταυτόχρονη» εκτέλεση ανάμεσα σε δύο διαδοχικές καταγραφές των δύο πιο «ακριβών» χρονικά εντολών. Αυτές οι εντολές είναι ο "Υπολογισμός του χρόνου άφιξης" και η "Μέθοδος TESPAR". Έτσι ο διαχωρισμός της εκτέλεσής τους, στις περιπτώσεις της $1^{ης}$ καταγραφής υπέρβασης και όλων των υπόλοιπων καταγραφών λύνει το πρόβλημα.

Ο παρακάτω πίνακα περιέχει τους χρόνοι εκτέλεσης και τα ενεργειακά κόστη των παραπάνω εντολών. Αξίζει να σημειωθεί ότι στην περίπτωση όπου η ευρετική μέθοδος αναγνωρίσει την απειλή ως έκρηξη ή ανθρώπινο βάδισμα αυτόματα σταματάει και η εκτέλεση της μεθόδου TESPAR (δηλαδή η εκτέλεση σταματάει στα 3sec αντί για τα 4.).

Πίνακας 27: Ενεργειακά κόστη εντολών κατηγοριοποίησης.

	Περίπτωση Έκρηξης (μία μόνο υπέρβαση, η αρχική)		**Περίπτωση Βαδίσματος** (τρείς υπερβάσης με συγκεκριμένο χρονικό περιθώριο μεταξύ τους)		**Περίπτωση οχήματος** (πολλές υπερβάσης με ακανόνιστά χρονικά περιθώρια μεταξύ τους)	
Λειτουργία	**Χρόνος (msec)**	**Ενεργειακό Κόστος (μAs)**	**Χρόνος (msec)**	**Ενεργειακό Κόστος (μAs)**	**Χρόνος (msec)**	**Ενεργειακό Κόστος (μAs)**
Ακουστικός αισθητήρας	**4000**	0.8 mA * 4000 ms= **3200**	**4000**	0.8 mA * 4000 ms= **3200**	**4000**	0.8 mA * 4000 ms= **3200**
Λήψη δείγματος	0.028ms * 10 (εκτελέσεις ανά msec) * 4000ms = **1120**	7.6mA * 1120 ms = **8512**	0.028ms * 10 (εκτελέσεις ανά msec) * 4000ms = **1120**	7.6mA * 1120 ms = **8512**	0.028ms * 10 (εκτελέσεις ανά msec) * 4000ms = **1120**	7.6mA * 1120 ms = **8512**

Έλεγχος υπέρβασης κατωφλίου	0.015ms * 10 (δείγματα ανά ms) * 4000ms = **600**	7.6mA * 600ms = **4560**	0.015ms * 10 (δείγματα ανά ms) * 4000ms = **600**	7.6mA * 600ms = **4560**	0.015ms * 10 (δείγματα ανά ms) * 4000ms = **600**	7.6mA * 600ms = **4560**
Ευρετική Μέθοδος	**0.017ms**	7.6mA * 0.017ms = **0.1292**	**3*0.017ms**	7.6mA * 0.051ms = **0.3876**	**2*0.017**	7.6mA * 0.034ms = **0,2584**
Μέθοδος TESPAR	0.035ms * 10 (δείγματα ανά ms) * 3000ms = **1050**	7.6mA * 1050ms = **7980**	0.035ms * 10 (δείγματα ανά ms) * 3000ms = **1050**	7.6mA * 1050ms = **7980**	0.035ms * 10 (δείγματα ανά ms) * 4000ms = **1400**	7.6mA * 1400ms = **10640**
Σύνολο		24252.12		24252.38		26912.25

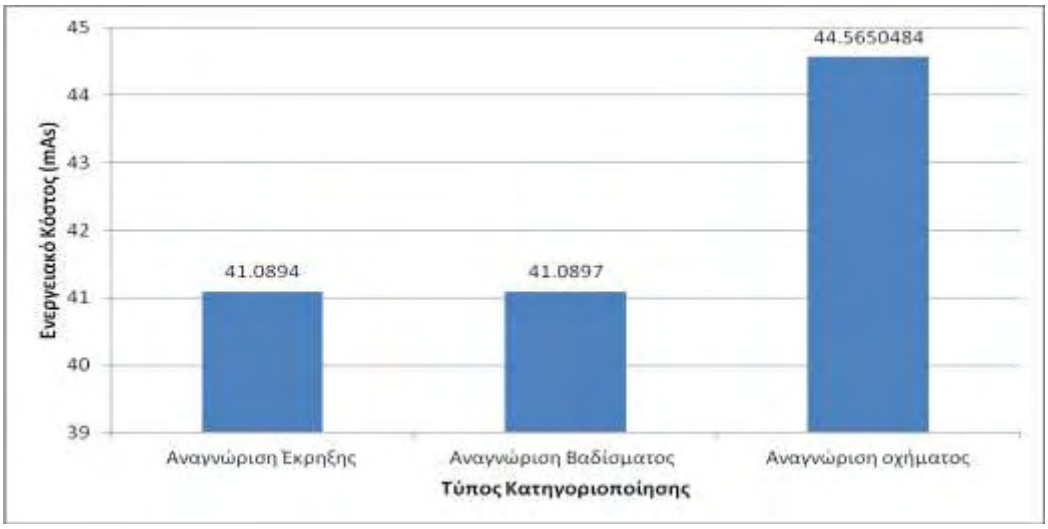


Εικόνα 84: Ενεργειακό Κόστος ανάλογα με το τύπο κατηγοριοποίησης.

Τέλος, παρακάτω παρουσιάζουμε έναν συγκριτικό πίνακα με τα ενεργειακά κόστη των λειτουργιών κατηγοριοποίησης μάζι με την ενέργεια που απαιτείται για την αποστολή των αποτελεσμάτων τους. Τα μηνύματα που χρησιμοποιούνται για την αποστολή των αποτελεσμάτων είναι τα: EventHeuristicMsg και EventTESPARMsg. Για την αποφυγή συγκρούσεων χρησιμοποιούμε ένα διάστημα 5 sec, κατά την διάρκεια του οποίου ο κάθε κόμβος εκπέμπει σε τυχαία στιγμή το μήνυμά του προς τον σταθμό βάσης (όπως σε προηγούμενα κεφάλαια). Ακόμα αξίζει να σημειωθεί ότι κατά την διάρκεια εκτέλεσης των υπολογισμών της κατηγοριοποίησης ο πομποδέκτης των κόμβων είναι απενεργοποιημένος. Ενεργοποιείται αμέσως μετά την εξαγωγή συμπεράσματος. Ο χρόνος ενεργοποίησης του είναι 1.8sec. Ο χρόνος προετοιμασίας των μηνυμάτων αποστολής EventHeuristicMsg και EventTESPARMsg είναι: 2.7ms και 3.5 αντίστοιχα.

Πίνακας 28:Συνολικό ενεργειακό κόστος κατηγοριοποίησης απειλών (συμπεριλαμβανομένου και του κόστους αποστολής των αποτελεσμάτων στον σταθμό βάσης).

	Περίπτωση Έκρηξης (μία μόνο υπέρβαση, η αρχική)	**Περίπτωση Βαδίσματος** (τρείς υπερβάσης με συγκεκριμένο χρονικό περιθώριο μεταξύ τους)	**Περίπτωση οχήματος** (πολλές υπερβάσης με ακανόνιστά χρονικά περιθώρια μεταξύ τους)
Λειτουργία	**Ενεργειακό Κόστος (mAs)**	**Ενεργειακό Κόστος (mAs)**	**Ενεργειακό Κόστος (mAs)**
Ακουστικός αισθητήρας	0.8 mA * 4 s= **3.2**	0.8 mA * 4 s= **3.2**	0.8 mA * 4 s= **3.2**
Λήψη δείγματος	7.6mA * 1.12 s = **8.512**	7.6mA * 1.12 s = **8.512**	7.6mA * 1.12 s = **8.512**
Έλεγχος υπέρβασης κατωφλίου	7.6mA * 0.6 s = **4.56**	7.6mA * 0.6 s = **4.56**	7.6mA * 0.6 s = **4.56**
Ευρετική Μέθοδος	7.6mA * 0.000017 s = **0.0001292**	7.6mA * 0.000051 s = **0.0003876**	7.6mA * 0.000034 s = **0,0002584**
Μέθοδος TESPAR	7.6mA * 1.050 s = **7.98**	7.6mA * 1.05 s = **7.98**	7.6mA * 1.4 s = **10.64**
Ενεργοποίηση πομποδέκτη	7.6mA * 0.0018s = **0.01368**	7.6mA * 0.0018s = **0.01368**	7.6mA * 0.0018s = **0.01368**
Προετοιμασία μηνύματος EventHeuristic Msg	7.6mA * 0.0027s = **0.02052**	7.6mA * 0.0027s = **0.02052**	**0**
Προετοιμασία μηνύματος EventTESPAR Msg	**0**	**0**	7.6mA * 0.0035s = **0.0266**
Κατανάλωση μικρο-ελεγκτη κατά την αναμονή αποστολής μηνύματος	(περίπτωση μέγιστης αναμονής για την αποστολή του μηνύματος) (5s - 0.0018s – 0.0027s) * 3.3mA = **16.48515**	(περίπτωση μέγιστης αναμονής για την αποστολή του μηνύματος) (5s - 0.0018s – 0.0027s) * 3.3mA = **16.48515**	(περίπτωση μέγιστης αναμονής για την αποστολή του μηνύματος) (5s - 0.0018s – 0.0035s) * 3.3mA = **16.48251**
Αποστολή μηνύματος	**0.318**	**0.318**	**1.130**
Σύνολο	**41.0894**	**41.0897**	**44.5650484**



Εικόνα 85: Συνολικό ενεργειακό κόστος κατηγοριοποίησης απειλών (συμπεριλαμβανομένου και του κόστους αποστολής των αποτελεσμάτων στον σταθμό βάσης).

8 *Ολοκληρωμένη μορφή πλαισίου λειτουργιών*

Στα προηγούμενα κεφάλαια έγινε μια αναλυτική περιγραφή ενός πλαισίου λειτουργιών το οποίο χρησιμοποιεί δεδομένα από ακουστικούς αισθητήρες προκειμένου να ανιχνεύσει την ύπαρξη απειλών σε ένα συγκεκριμένο περιβάλλον, καθώς και να αναγνωρίσει τον τύπο της. Επιπλέον, έναν από τους πολύ βασικούς τομής λειτουργικότητας που παρέχει το συγκεκριμένο πλαίσιο είναι η λειτουργίες ασφάλεια για τους ασύρματους κόμβους.

Παρακάτω θα γίνει μια περιγραφή του συνδυασμού όλων των λειτουργικοτήτων που περιλαμβάνει το συγκεκριμένο πλαίσιο καθώς και εκτίμηση του συνολικού ενεργειακού κόστους εφαρμογής του στους ασύρματους κόμβους.

Το διάγραμμα περιλαμβάνει το διάγραμμα ροής όλων των λειτουργιών που περιλαμβάνονται στο πλαίσιο λειτουργικότητας. Κάθε κατάσταση ανάλογα με την λειτουργικότητα που εκτελεί διαθέτει και διαφορετικό χρώμα. Έτσι με:

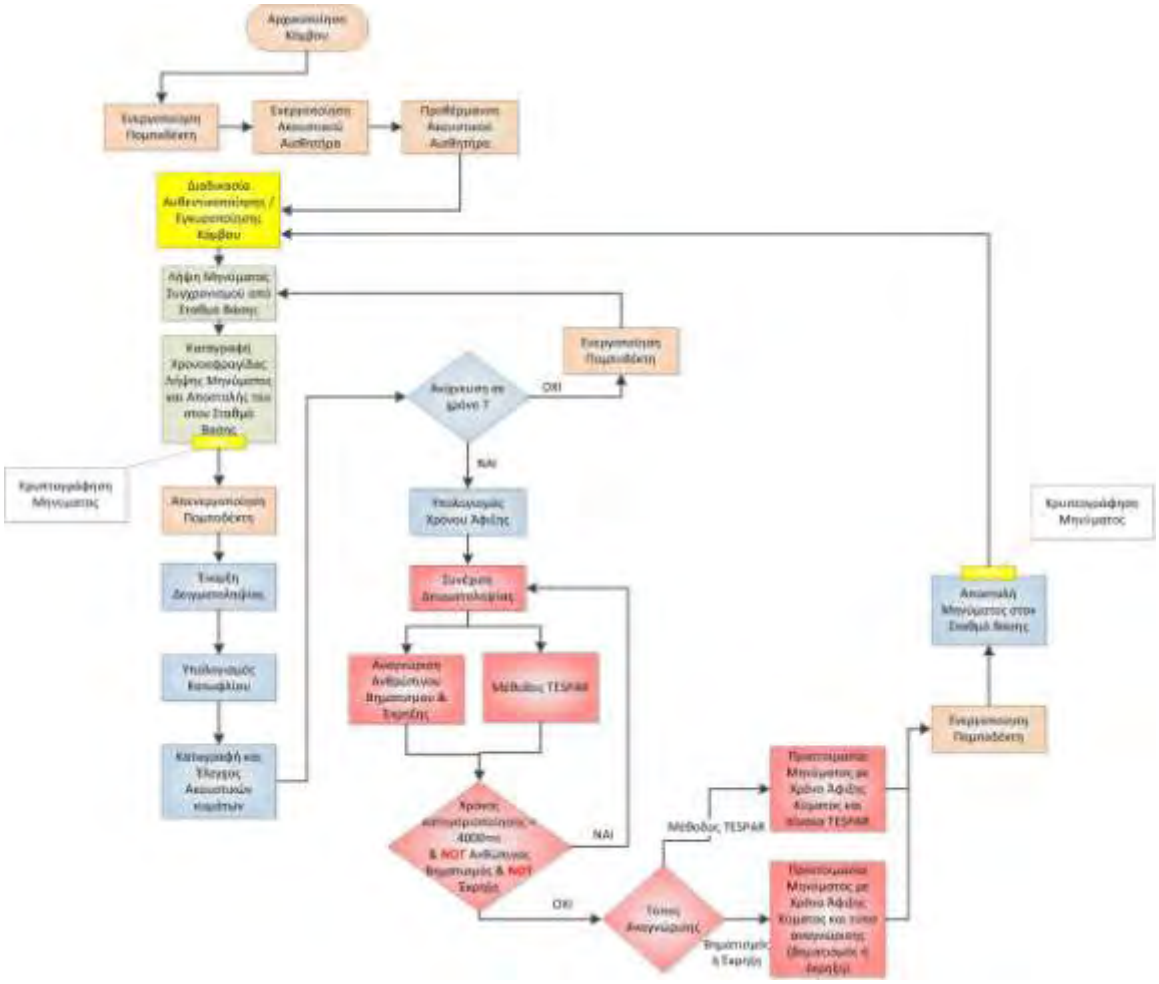
- Ροζ χρώμα απεικονίζονται οι λειτουργίες που είναι απαραίτητες για την σωστή λειτουργία του κόμβου.

- Κίτρινο χρώμα απεικονίζονται οι λειτουργίες που αφορούν την παροχή ασφάλειας στον κόμβο. Συγκεκριμένα αυτές οι λειτουργίες είναι η κρυπτογράφηση και αποκρυπτογράφηση των ασύρματων επικοινωνιών και ο έλεγχος αυθεντικοποίησης και εγκυροποίησης του κόμβου.

- Πράσινο χρώμα απεικονίζονται οι λειτουργίες που αφορούν τον συγχρονισμό του κόμβου με τον σταθμό βάσης του δικτύου.

- Μπλε χρώμα απεικονίζονται οι λειτουργίες που αφορούν την ανίχνευση απειλών. Αντιπροσωπευτικό παράδειγμα αυτών των λειτουργιών είναι η καταγραφή των ακουστικών κυμάτων, ο υπολογισμός του κατωφλίου και ο έλεγχος της ύπαρξης απειλών.

- Κόκκινο χρώμα απεικονίζονται οι λειτουργίες που αφορούν την κατηγοριοποίηση των απειλών που έχουν ανιχνευτεί.



Εικόνα 86: Ολοκληρωμένο διάγραμμα ροής του πλαισίου λειτουργικότητας ασφαλούς αναγνώρισης και κατηγοριοποίησης απειλών με την χρήση ασύρματου δικτύου αισθητήρων

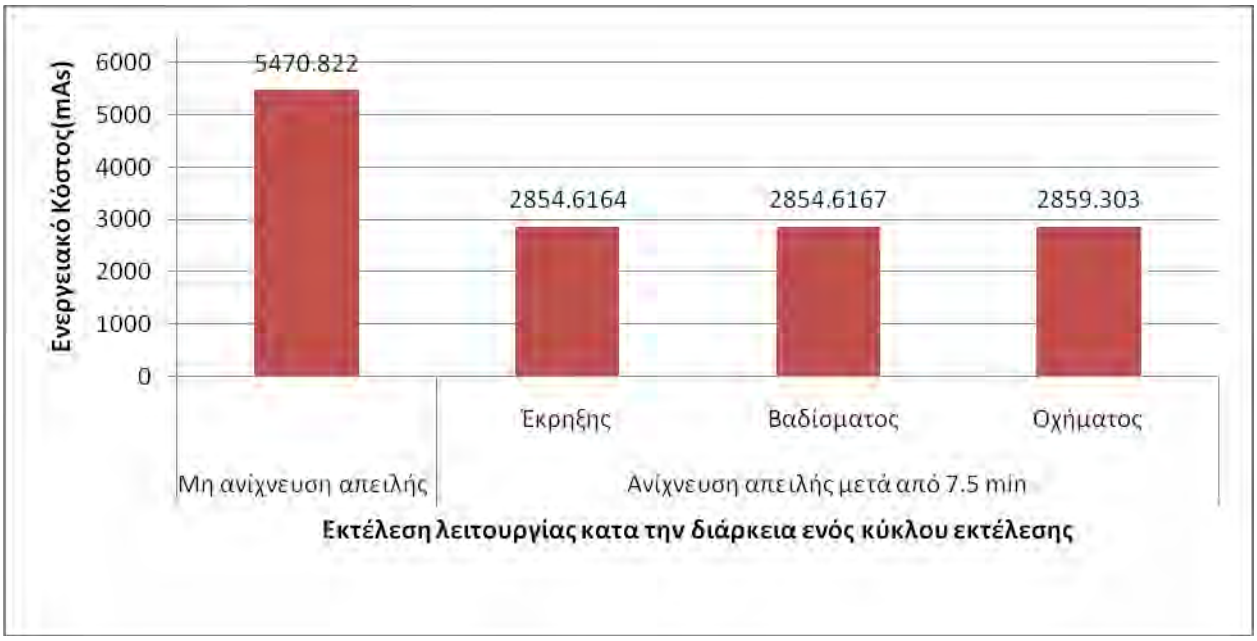
Σύμφωνα με το διάγραμμα η εκτέλεση της διαδικασίας αυθεντικοποίησης και εγκυροποίησης εκτελείται στην αρχή κάθε κύκλου εκτελέσεων των λειτουργιών του πλαισίου. Παρόλα αυτά, έχοντας υπόψη τις βέλτιστη χρήση των ενεργειακών πόρων του κόμβου, θα μπορούσαμε να μειώσουμε των ρυθμό εκτέλεσής της. Για παράδειγμα, μια πιθανή μείωση του ρυθμού εκτέλεσης της θα ήταν να εκτελείται κάθε 2 ή 3 κύκλους πλήρους εκτέλεσης του πλαισίου. Βέβαια, αυτό εξαρτάται και σε μεγάλο βαθμό από το περιβάλλον λειτουργίας του δικτύου αισθητήρων. Έτσι, στην περίπτωση όπου οι ασύρματοι κόμβοι λειτουργούν σε ένα «εχθρικό» περιβάλλον με μεγάλη πιθανότητα ύπαρξης κακόβουλων χρηστών, η διαδικασία θα πρέπει στην αρχή κάθε πλήρες κύκλου εκτέλεσης του πλαισίου. Αντίθετα, στην περίπτωση όπου η πιθανότητα ύπαρξης μη-εξουσιοδοτημένων χρηστών είναι μειωμένη, η διαδικασία θα πρέπει να εκτελείται σε μικρότερο ρυθμό.

Παρακάτω υπολογίζεται το ενεργειακό κόστος του συνόλου των λειτουργιών του πλαισίου που περιγράφεται στην συγκεκριμένη εφαρμογή. Πρέπει να σημειωθεί, ότι οι λειτουργίες που περιλαμβάνουν αποστολή μηνύματος προς τον σταθμό βάσης

χρησιμοποιούν κρυπτογράφηση των μηνυμάτων μέσω της λειτουργίας ασφαλείας που περιέχεται στο πλαίσιο.

Πίνακας 29: Το ενεργειακό κόστος ενός κύκλου εκτέλεσης με την εκτέλεση όλων των λειτουργιών που υποστηρίζει το πλαίσιο.

	Ενεργειακό Κόστος (mAs)			
Λειτουργία	**Μη ανίχνευση απειλής για T=15 min**	**Ανίχνευση απειλής μετά από 7.5 min**		
		Αναγνώριση Έκρηξης	**Αναγνώριση Βαδίσματος**	**Αναγνώριση Οχήματος**
Αυθεντικοποίηση / Εκγυροποίηση	28.02	28.02	28.02	28.02
Λήψη μηνύματος Συγχρονισμού	0.284	0.284	0.284	0.284
Καταγραφή χρονοσφραγίδας και αποστολή στον σταθμό βάσης	18.577	18.577	18.577	18.577
Υπολογισμού του κατωφλίου	87.941	87.941	87.941	87.941
Καταγραφής ακουστικών κυμάτων και ανίχνευσης απειλών	5336	2677	2677	2677
Κατηγοριοποίηση απειλών	0	42,7944	42,7947	47,481
Σύνολο	**5470.822**	**2854.6164**	**2854.6167**	**2859.303**



Εικόνα 87: Το συνολικό ενεργειακό κόστος του πλαισίου λειτουργιών ανά κύκλο εκτέλεσης.

Το συνολικό ενεργειακό κόστος το οποίο καταναλώνει η μέθοδος ανίχνευσης κατά τη εκτέλεση ενός κύκλου εκτέλεσης είναι

- **5470.822mAs** για την περίπτωση μη ανίχνευσης απειλής
- **2854.61mAs** για τις περιπτώσεις αναγνώρισης έκρηξης και ανθρώπινου βαδίσματος (τις 2 αυτές περιπτώσεις τις θεωρούμε ίδιες, καθώς ενεργειακές τους ανάγκες έχουν πολύ μικρή διαφορά).
- **2859,3 mAs** για την περίπτωση αναγνώρισης οχήματος.

Έτσι κάνοντας την υπόθεση ότι ο κόμβος χρησιμοποιεί μια μπαταρία χωρητικότητας 2700mAh η μέγιστη διάρκεια λειτουργίας του κόμβου στις παραπάνω περιπτώσεις είναι:

<u>Περίπτωση Μη Ανίχνευσης Απειλής για χρόνο 15 min</u>

Ενεργειακό κόστος ανά κύκλο εκτέλεσης :

$$5470.822\text{mAs} = 1.519\,\text{mAh}$$

Μέγιστος δυνατός αριθμός κύκλων εκτέλεσης :

$$\frac{2700mAh}{1.519mAh} = 1777 \text{ αριθμός κύκλων εκτέλεσης}$$

Μέγιστη χρονική διάρκεια εκτέλεσης μεθόδου εντοπισμού απειλών (Λαμβάνοντας υπόψη ότι η διάρκεια εκτέλεσης ενός κύκλου εκτέλεσης χωρίς την ύπαρξη απειλών είναι ~15.5min + χρόνος εκτέλεσης των διαδικασιών αυθεντικοποίησης και εγκυροποίησης = 15.7 min**):**

$$\frac{1777 * 15.7}{60 * 24} = 19.37 \text{ ημέρες}$$

Περίπτωση Ανίχνευσης Έκρηξης ή Βαδίσματος σε χρόνο 7,5 min

Ενεργειακό κόστος ανά κύκλο εκτέλεσης :

$$2854.61\text{mAs} = 0.7929\,\text{mAh}$$

Μέγιστος δυνατός αριθμός κύκλων εκτέλεσης :

$$\frac{2700mAh}{0.7929mAh} = 3405\,\text{αριθμός κύκλων εκτέλεσης}$$

Μέγιστη χρονική διάρκεια εκτέλεσης μεθόδου εντοπισμού απειλών (Λαμβάνοντας υπόψη ότι η διάρκεια εκτέλεσης ενός κύκλου εκτέλεσης χωρίς την ύπαρξη απειλών είναι 8min+ χρόνος εκτέλεσης των διαδικασιών αυθεντικοποίησης και εγκυροποίησης + χρόνος κατηγοριοποίησης = 8.4 min**):**

$$\frac{3405 * 8.4}{60 * 24} = 19.86\,\text{ημέρες}$$

Περίπτωση Ανίχνευσης Οχήματος σε για χρόνο 7,5 min

Ενεργειακό κόστος ανά κύκλο εκτέλεσης :

$$2859.3\text{mAs} = 0.7942\,\text{mAh}$$

Μέγιστος δυνατός αριθμός κύκλων εκτέλεσης :

$$\frac{2700mAh}{0.7942mAh} = 3399\,\text{αριθμός κύκλων εκτέλεσης}$$

Μέγιστη χρονική διάρκεια εκτέλεσης μεθόδου εντοπισμού απειλών (Λαμβάνοντας υπόψη ότι η διάρκεια εκτέλεσης ενός κύκλου εκτέλεσης χωρίς την ύπαρξη απειλών είναι 8min+ χρόνος εκτέλεσης των διαδικασιών αυθεντικοποίησης και εγκυροποίησης + χρόνος κατηγοριοποίησης = 8.4 min**):**

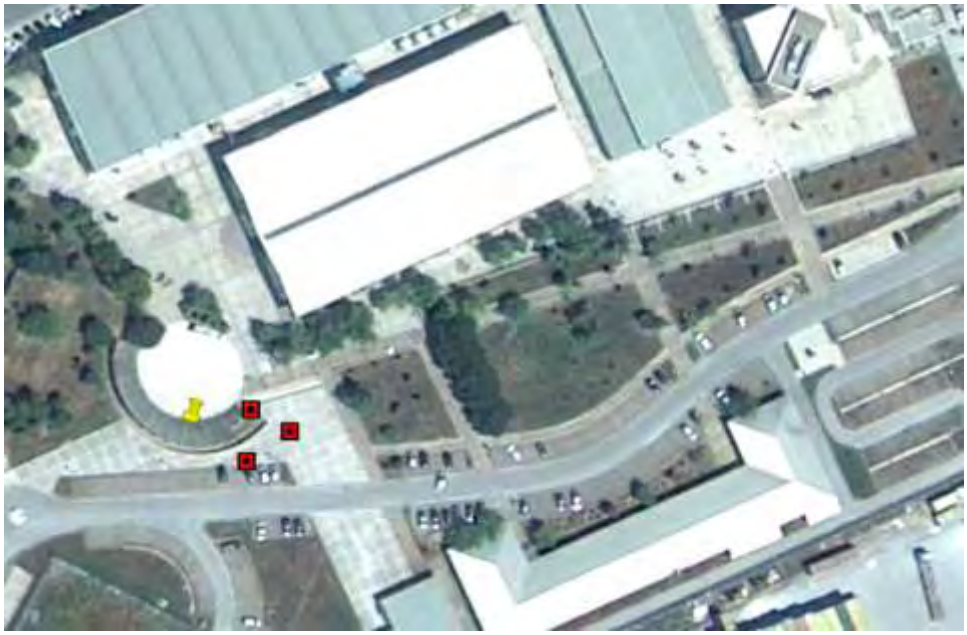
$$\frac{3399 * 8.4}{60 * 24} = 19.83\,\text{ημέρες}$$

8.1 Περιγραφή πραγματικών σεναρίων χρήσης του πλαισίου λειτουργιών

Στα πλαίσια της δοκιμής του πλαισίου λειτουργιών σε πραγματικές συνθήκες έγινε υλοποίηση του και εφαρμογή του σε ασύρματους κόμβους τύπου Mica2. Χρησιμοποιήθηκαν 3 ασύρματοι κόμβοι και ένας σταθμό βάσης και έγιναν μετρήσεις τόσο της ακρίβειας εντοπισμού μιας απειλής όσο και της ικανότητας αναγνώρισης του τύπου της απειλής. Οι δοκιμές έγιναν στον Βόλο στο προαύλιο χώρο του Πανεπιστημίου Θεσσαλίας. Οι καιρικές συνθήκες που επικρατούσαν κατά την διάρκεια των δοκιμών ήταν:

- θερμοκρασία 19-22 ^{o}C
- σχετική υγρασία 65%.-75%.
- Ατμοσφαιρική πίεση 1010mbar.
- Ταχύτητα ανέμου 0 km (άπνοια).

Εικόνα 88: Περιοχή εκτέλεσης των δοκιμών. Προαύλιος χώρος Πανεπιστημίου Θεσσαλίας.

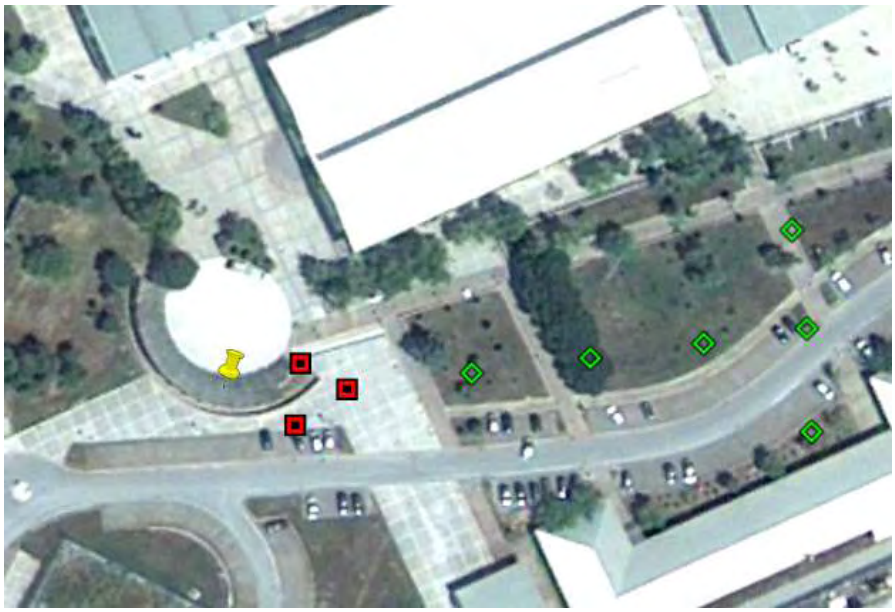


Εικόνα 89: Η θέση του σταθμού βάσης (κίτρινο χρώμα) και των τριών ασύρματων κόμβων Mica2 (κόκκινο χρώμα).

Στα πλαίσια των δοκιμών επιλέξαμε να τοποθετήσουμε τους κόμβους σε σταθερά σημεία. Έτσι η απόσταση ανάμεσα τους είναι 5 μέτρα και η απόστασή τους από τον σταθμό βάσης ~10 μέτρα (Κάθε κόμβος έχει διαφορετική απόσταση από τον σταθμό βάσης. Ο μέσος όρος των αποστάσεων αυτών είναι στα 10μ, χωρίς όμως να παίζει κανέναν ουσιαστικό ρόλο στην απόδοση του συστήματος.).

Αφού τοποθετήθηκαν ο σταθμό βάσης και οι τρις ασύρματοι κόμβοι του δικτύου εκτελεστήκαν δομικές σχετικά με την εξακρίβωση της ακρίβειας εντοπισμού μιας απειλής. Για την μέτρηση της ακρίβειας χρησιμοποιήθηκαν τεχνικές έκρηξης μικρού μεγέθους (δυναμιτάκια), τα οποία τα «σκάσαμε» σε διαφορετικές χρονικές στιγμές, διαφορετικές αποστάσεις αλλά πάνω στην ίδια ευθεία από τους κόμβους. Οι εκρήξεις έγινα σε απόσταση 20, 40, 60, 70 μέτρων από τους ασύρματους κόμβους. Επιπλέον έγιναν και μερικές δοκιμές αριστερά και δεξιά από την γενική ευθεία των δοκιμών, στην απόσταση των 100 μέτρων προκειμένου να δοκιμάσουμε περαιτέρω την ακρίβειά του.

Τα αποτελέσματα σχετικά με την ακρίβεια εντοπισμού του σημείου της απειλής είναι περίπου στα 10 μέτρα. Το μεγάλο εύρος της ακρίβειας οφείλεται κυρίως στον μικρό αριθμό ασύρματων κόμβων που χρησιμοποιήσαμε και στην μικρή σχετικά απόσταση μεταξύ τους. Σύμφωνα με εκτιμήσεις, η αύξηση αυτών των δύο παραμέτρων μπορεί να δώσει αρκετά μεγάλη ακρίβεια στην εκτίμηση της θέσης της απειλής. Η ακρίβεια αυτή μπορεί να φτάσει ακόμα και τα 2 μέτρα.



Εικόνα 90: Εκτέλεση δοκιμών μέτρησης ακρίβειας εντοπισμού των κόμβων. Με πράσινο χρώμα είναι τα σημεία εντοπισμού της απειλής. (στα 20μ ,40μ ,60μ ,70μ).

Στην συνέχεια εκτελέστηκε πλήθος δοκιμών σχετικά με την δυνατότητα αναγνώρισης του τύπου των απειλών. Χρησιμοποιήθηκαν 4 διαφορετικές κατηγορίες απειλών:

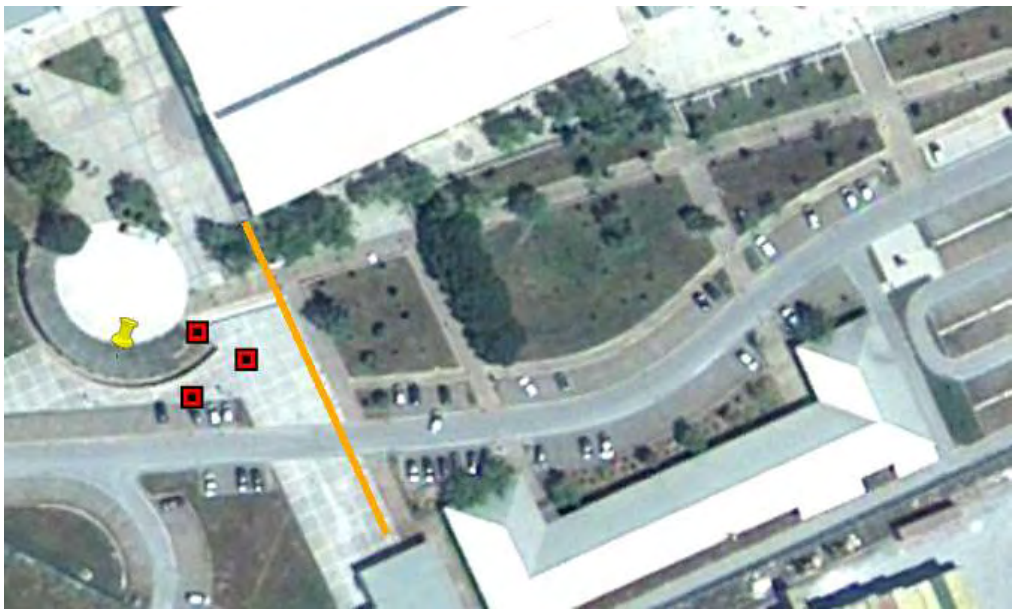
1. Κατηγορία έκρηξης (δυναμιτάκια).
2. Κατηγορία ανθρώπινου βηματισμού.
3. Κατηγορία οχήματος_1 (αυτοκίνητο).
4. Κατηγορία οχήματος_2 (μοτοσυκλέτα).

Οι θέσης των απειλών βρισκόντουσαν σε σταθερά σημεία (Εικόνες 91 & 92). Το ποσοστό σωστής αναγνώρισης των παραπάνω κατηγοριών φαίνεται στον παρακάτω πίνακα.

Πίνακας 30:Ποσοστό επιτυχούς αναγνώρισης τύπου απειλών

Τύπος απειλής	% Ποσοστό επιτυχούς αναγνώρισης
Κατηγορία Έκρηξης (δυναμιτάκια)	98 %
Κατηγορία Ανθρώπινου Βηματισμού	95 %
Κατηγορία οχήματος_1 (αυτοκίνητο).	85 %
Κατηγορία οχήματος_2 (μοτοσυκλέτα).	75 %

Εικόνα 91: Ανίχνευση και αναγνώριση οχήματος.



Εικόνα 92: Ανίχνευση και αναγνώρισης ανθρώπινου βηματισμού.

9 ΕΠΙΛΟΓΟΣ

9.1 Συμπεράσματα

Η διατριβή αυτή εκπονήθηκε έχοντας ως άξονα κίνησης της την αναζήτηση λύσης για ένα ιδιαίτερα απαιτητικό πρόβλημα , όπως αυτό της επιτήρησης ενός χώρου. Προτείνεται ένα πλαίσιο λειτουργιών το οποίο βασίζεται στην καταγραφή και επεξεργασία των ακουστικών κυμάτων που διαδίδονται στον ως προς επιτήρησης χώρο. Βασικό στοιχείο της λειτουργικότητας που περιγράφεται αποτελούν τα Ασύρματα Δίκτυα Αισθητήρων.

Η ταχύτατη ανάπτυξη της μικροηλεκτρονικής και των υλικών επέτρεψε την κατασκευή πολύ μικρών αισθητήρων, οι οποίοι έχουν την ικανότητα να μετρούν και να καταγράφουν μια κυριολεκτικά ατέλειωτη σειρά από περιβαλλοντολογικά ή βιολογικά μεγέθη. Οι αισθητήρες αυτοί έχουν την δυνατότητα επικοινωνίας και αυτοωργάνωσης δημιουργώντας έτσι ένα ασύρματο δίκτυο από κόμβους ικανούς να εκτελέσουν συνδυαστικούς υπολογισμούς στον χώρο.

Οι ασύρματοι κόμβοι που συγκροτούν ένα Ασύρματο Δίκτυο Αισθητήρων συνήθως έχουν χαμηλή επεξεργαστική ισχύ και χαμηλή ενεργειακή διαθεσιμότητα, καθιστώντας τους ακατάλληλους για την εκτέλεση πολύπλοκων αλγορίθμων. Το περιεχόμενο της συγκεκριμένης διατριβής είναι:

1. η μελέτη των περιορισμών που εισάγει η χρήση αυτών των ασύρματων κόμβων
2. η ανάπτυξη τεχνικών και αλγορίθμων χαμηλών ενεργειακών και επεξεργαστικών απαιτήσεων για την ανίχνευση και κατηγοριοποίηση απειλών.
3. η ανάπτυξη ενός πλαισίου λειτουργιών ασφαλείας το οποίο εγγυάται για την αυθεντικοποίηση και εγκυροποίηση των ίδιων των κόμβων καθώς και την ασφαλή ασύρματη μετάδοση των δεδομένων τους μέσω της χρήση αλγορίθμων κρυπτογράφησης.

Διαρθρωτικά διδόμενη, στο πρώτο μέρος της τέθηκαν οι βάσεις σχετικά με το θεωρητικό και τεχνολογικό υπόβαθρο του αντικείμενου μελέτης. Αναλυτικά, μελετήθηκε η φυσιολογία των ακουστικών κυμάτων καθώς και η επίδραση που έχουν οι περιβαλλοντικές συνθήκες στον τρόπο διάδοσης τους. Ακόμα έγινε μια περιγραφή των απαιτήσεων και περιορισμών που παρουσιάζουν τα Ασύρματα Δίκτυα Αισθητήρων. Τέλος έγινε μια αναλυτική μελέτη των ασύρματων κόμβων που χρησιμοποιήθηκαν στα πλαίσια της συγκεκριμένης διατριβής. Παρουσιάστηκαν πληροφορίες σχετικά με

ικανότητες των κόμβων, ενώ ιδιαίτερη σημασία δόθηκε στην παρουσίαση των αισθητήριων οργάνων που φέρουν αυτά καθώς και της ακρίβειας των μετρήσεων τους.

Το δεύτερο μέρος της διατριβής περιλαμβάνει την διαδικασία ανάπτυξης και υλοποίησης των λειτουργιών του πλαισίου. Αρχικά, περιγράφεται η ανάπτυξη των λειτουργιών ασφάλειας των κόμβων. Οι λειτουργίες αυτές περιλαμβάνουν την αυθεντικοποίηση και εγκυροποίηση των κόμβων καθώς και την κρυπτογράφηση των δεδομένων τους. Στην συνέχεια παρουσιάζονται οι λειτουργίες εντοπισμού των απειλών χρησιμοποιώντας τα ακουστικά τους κύματα. Τέλος γίνεται παρουσίαση των τεχνικών αναγνώρισης της κατηγορίας τους. Οι παραπάνω τεχνικές αναπτύχθηκαν λαμβάνοντας υπόψη τους περιορισμούς που εισάγουν οι ασύρματοι κόμβοι. Γίνεται εκτέλεση αυτών σε ειδικό περιβάλλον προσομοίωσης, υπολογίζονται με ακρίβεια οι ενεργειακές τους απαιτήσεις ενώ παράλληλα γίνεται περιγραφή διάφορων ενεργειακών πολιτικών που αποσκοπούν στην βελτίωση της χρήσης των πόρων τους.

Το τρίτο και τελευταίο μέρος της διατριβής αφορά την εφαρμογή του πλαισίου λειτουργιών σε πραγματικούς ασύρματους κόμβους, τους Mica2. Γίνεται δοκιμή αυτών σε πραγματικές συνθήκες όπου και γίνεται μέτρηση της αποδοτικότητας των λειτουργιών του πλαισίου καθώς και εκτίμηση της ακρίβειας των αποτελεσμάτων τους.

9.2 Μελλοντικές δυνατότητες επέκτασης

Φυσική συνέχεια της εργασίας, αποτελεί η βελτίωση των λειτουργιών εντοπισμού και κατηγοριοποίησης. Οι λειτουργίες αυτές έχουν την δυνατότητα βελτίωσης τόσο στο πεδίο της ενεργειακής κατανάλωσής τους, όσο και στο πεδίο της ακρίβειας των αποτελεσμάτων τους. Ακόμα, η ενσωμάτωση σε έναν κοινό ασύρματο κόμβο των ακουστικών αισθητήρων και των αισθητήριων οργάνων που εκτελούν καταγραφή των περιβαλλοντικών συνθηκών θα βελτιώσει σε μεγάλο βαθμό την φορητότητα και την ευκολία διαχείρισης των ίδιων των κόμβων αλλά και των λειτουργιών τους. Τέλος, η ανάπτυξη κατάλληλων γραφικών διεπαφών για την παρουσίαση των αποτελεσμάτων αλλά και την διαχείριση του δικτύου θα μπορούσε να μετατρέψει το πλαίσιο αυτό σε ένα χρήσιμο εργαλείο των στρατιωτών στο πεδίο της μάχης.

10 ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]. Mark Weiser, ***"The Computer for the Twenty-First Century"***, Scientific American, pp.94-10, September 1991.

[2]. "The Internet of Things", ITU, November 2005.

[3]. H. Sundmaeker, P. Guillemin, S. Antipolis,P. Friess, S. Woelfflé, "Vision and Challenges for Realising the Internet of Things", Cluster of European Research Projects on the Internet of Things (CERPIoT), March 2010

[4]. O. Vermesan et al., "Internet of Things Strategic Research Roadmap", European Research Cluster on the Internet of Things, Cluster Strategic Research Agenda 2011.

[5]. A. Dunkels Adam and J.P. Vasseur, "IP for Smart Objects", Internet Protocol for Smart Objects (IPSO) Alliance, Sepember 2008.

[6]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. 2002. Wireless sensor networks: a survey. Computer Networks, vol. 38, no. 4, March 2002, pp. 393-422, doi=10.1016/S1389-1286(01)00302-4

[7]. Ν. Λαρίσης, "Σύστημα διαχείρισης στάθμευσης με χρήση ασύρματου δικτύου αισθητήρων σε πραγματικό περιβάλλον", Διπλωματική εργασία, Πανεπιστήμιο Θεσσαλίας, Βόλος, Ιούλιος 2011

[8]. G. Mazarakis, ***"Seismic personnel detection and seismic and acoustic vehicle recognition and classification in Wireless Sensor Networks with emphasis on energy efficiency and low power consumption"***, Ph.D. Thesis, National Technical University of Athens, October 2007.

[9]. Λ. Περλεπές, "Ανάπτυξη συστήματος διαχείρισης αγροτικών εφαρμογών με τη χρήση δικτύου ασύρματων αισθητήρων", Μεταπτυχιακή Διπλωματική εργασία, Πανεπιστήμιο Θεσσαλίας, Βόλος, 2009

[10]. http://www.xbow.com (Accessed 10 April 2011).

[11]. http://commonsense.epfl.ch/COMMONSense/description.htm

[12]. http://www2.enthesis.net/index.php?news=645

[13]. P. Kikiras and J. Avaritsiotis, ***"Unattended Ground Sensor Network for Force Protection"***, Journal of Battlefield Technology, vol. 7, no.3, Nov. 2004.

[14]. A. Arora et al., ***"A line in the sand: A wireless sensor network for target detection, classification, and tracking"***, Computer Networks Journal, vol. 46, no. 5, pp. 605–634, 2004.

[15]. M. Caruso, L. Withanawasam, ***"Vehicle Detection and Compass Applications using AMR Magnetic Sensors"***, Honeywell, SSEC, 12001 State Highway 55, Plymouth, MN USA 55441 http://www.ssec.honeywell.com

[16]. The Vehicle Detector Clearinghouse, Southwest Technology Development Institute (SWTDI), ***"A Summary of Vehicle Detection and Surveillance Technologies used in Intelligent Transportation Systems",*** 2000.

[17]. A. Arora et al., ***"ExScal: Elements of an Extreme Scale Wireless Sensor Network"***, Proc. of the 11th IEEE Int. Conf. on Embedded and Real-Time Computing Systems and Applications, pp. 102 – 108, 17-19 Aug, 2005.

[18]. G. Succi, T. Pedersen, R. Gampert, G. Prado, ***"Acoustic Target Tracking and Target Identification - Recent Results"***, Proceedings of the SPIE, vol. 3713, p. 10, 1999.

[19]. J. Ding, ***"Vehicle detection by sensor network nodes",*** MS thesis, Department of Electrical Engineering and Computer Science, University of California, Berkeley, CA, 2003.

[20]. M. Duarte and Y. Hu, ***"Vehicle Classification in Distributed Sensor Networks"***, Journal of Parallel and Distributed Computing, Vol. 64 No. 7, pp. 826-838, 2004.

[21]. M. Pauli, M. C. Ertem and E. Heidhausen , "Quick Response Airborne Deployment of Viper Muzzle Flash Detection and Location System During DC Sniper Attacks," Proceedings of the 32nd Applied Imagery Pattern Recognition Workshop (AIPR'03), pp.221-228, October 2003.

[22]. Tan Kok Sin Stephen, "Source Localization Using Wireless Sensor Networks", Ph.D. Thesis, Naval Postgraduate School, Monterey, California, June 2006

[23]. J. B´edard and S. Par´e, "Ferret, a small arms' fire detection system: localization concepts," in *Sensors, and Command, Control, Communications, and Intelligence (C31) Technologies for Homeland Defense and Law Enforcement II*, vol. 5071 of *Proceedings of SPIE*, pp. 497–509, 2003.

[24]. D. Crane, "Ears-MM soldier-wearable gun-shot/sniper detection and location system," Defence Review, 2008.

[25]. "PILAR Sniper Countermeasure System", November 2009, http://www.canberra.com

[26]. "SADS - Small-Arms Detection System", January 2011, http://defense-update.com/products/s/sads.htm

[27]. J. A. Mazurek, J. E. Barger, M. Brinn et al., "Boomerang mobile counter shooter detection system," in *Sensors, and C3I Technologies for Homeland Security and Homeland Defense IV*, vol. 5778 of *Proceedings of SPIE*, pp. 264–282, Bellingham, Wash, USA, 2005.

[28]. "Artillery Location Acoustic System - ARTILOC", January 2010, http://www.rafael.co.il/Marketing/401-1180-en/Marketing.aspx

[29]. "Hostile Artillery Locating System - HALO", February 2011, http://www.baesystems.com/Newsroom/NewsReleases/2005/press_11022005.html

[30]. "Remotely Monitored Battlefield Sensor System-II – (REMBASS-II)", March 2004, http://www2.l-3com.com/cs-east/pdf/rembassii.pdf

[31]. C. Stubbs, M. Brenner, L. Bildsten, P. Dimotakis, S. Flatt´e, J. Goodman, B. Hearing, C. Max, R. Schwitters, J. Tonry, "Tactical Infrasound", Report of JASON Defense Advisory Panel, May 2005

[32]. P. Volgyesi, G. Balogh, A. Nadas, et al., "Shooter localization and weapon classification with soldier-wearable networked sensors", in Proceedings of the 5th International Conference on Mobile Systems, Applications, and Services (Mobisys '07), san Juan, Puerto Rice, 2007

[33]. G. Simon, M. Maróti, Á. Lédeczi, G. Balogh, B. Kusy, A. Nádas, G. Pap, J. Sallai, and K. Frampton. 2004. Sensor network-based countersniper system. In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (SenSys '04). ACM, New York, NY, USA, 1-12.

[34]. David Lindgren, Olof Wilsson, Fredrik Gustafsson, and Hans Habberstad. 2010. Shooter localization in wireless microphone networks. *EURASIP J. Adv. Signal Process* 2010, Article 6 (February 2010), 25 pages.

[35]. A. Yang, S. Iyengar, S. S. Sastry, R. Bajcsy, P. Kuryloski, and R. Jafari. Distributed Segmentation and Classi_cation of Human Actions Using a Wearable Motion Sensor Network. In Proc. of IEEE Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW '08), Anchorage, AK, USA, June 2008.

[36]. Georg Wittenburg, Norman Dziengel, Christian Wartenburger, and Jochen Schiller. 2010. A system for distributed event detection in wireless sensor networks. In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks* (IPSN '10). ACM, New York, NY, USA, 94-104.

[37]. A. Mayoral, I. McCool, R. Gramann, ***"Detection and Classification of Time-Critical Targets Using Seismic Sensors"***, Proceedings of the SPIE, vol. 4743, p. 80, 2002.

[38]. R. Gramannm M. Bennett, T. O'Brien, "Vehicle and personnel detection using seismic sensors", Proc. SPIE, vol. 3577, 1998

[39]. "Εγκύκλιος Παιδεία – Διάδοση του Ήχου", Φεβρουάριος 2009, http://egpaid.blogspot.com/2009/02/blog-post_8875.html

[40]. Tony F. W. Embleton, "Tutorial on sound propagation outdoors",J. Acoust. Soc. Am. 100, 31 (1996)

[41]. P. G. Hewitt, "*Conceptual Physics* 9th edition", Addison Wesley Longman, July 2002

[42]. Σ. Γεωργακαράκος, "Θεωρία και πρακτική εφαρμογή της Υδροακουστικής Τεχνολογίας στη Βιολογία", Τμήμα Επιστημών Θάλασσας, Πανεπιστήμιο Αιγαίου, Μυτιλήνη, 2004

[43]. X. Li, R. Logan, R. Pastore, ***"Perception of acoustic source characteristics: Walking sounds"***, Journal of the Acoustical Society of America, v. 90, no. 6, pp. 3036-3049, December 1991.

[44]. K. Houston, D. McGaffigan, ***"Spectrum Analysis Techniques for Personnel Detection Using Seismic Sensors"***, Proc. SPIE, vol. 5090, p. 162, 2003.

[45]. H. Wu, M. Siegel and P. Khosla "Vehicle sound signature recognition by frequency vector principal component analysis", IEEE Trans. Instrum. Meas., vol. 48, pp. 1005-1009, 1999.

[46]. N. Bhave and P. Rao, "Vehicle engine sound analysis applied to traffic congestion Estimation", Proc. of International Symposium on Computer Music Modeling and Retrieval (CMMR) and Frontiers of Research on Speech and Music (FRSM), March 2011, Bhubaneswar, India

[47]. Rahim, N.A.; Paulraj, M.P.; Adom, A.H.; Sundararaj, S.; "Moving vehicle noise classification using backpropagation algorithm", 6th International Colloquium on Signal Processing and Its Applications (CSPA), 21-23 May 2010, Malaysia

[48]. G. Prado, ***"Acoustic-seismic sensors: past experiences and future prospects"***, Proceedings of the SPIE, vol. 5611, p. 117, 2004.

[49]. C. Buschmann and D. Pfisterer, "iSense: A modular hardware and software platform for wireless sensor networks," 6. Fachgesprach Drahtlose Sensornetze ¨ der GI/ITG-Fachgruppe Kommunikation und Verteilte Systeme, Tech. Rep., 2007. [Online]. Available: http://ds.informatik.rwth-aachen.de/events/fgsn07

[50]. "ΗΧΟΛΗΨΙΑ", Εκπαιδευτικό υλικό, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Εργαστήριο Ηλεκτροακουστικής και Τηλεοπτικών Συστημάτων

[51]. Chee-yee Chong, Srikanta P. Kumar. 2003. "*Sensor Networks: Evolution, Opportunities and Challenges*". Proceedings of IEEE.

[52]. http://www.globalsecurity.org/intell/systems/sosus.htm

[53]. Ε. Βουμβουράκης, "Ολοκληρωμένο Σύστημα Δικτύου Αισθητήρων για την Παρακολούθηση Περιβαλλοντικών Συνθηκών και την Απεικόνισή τους σε GIS", Διπλωματική εργασία, Πανεπιστήμιο Θεσσαλίας, Βόλος, Ιούλιος 2011

[54]. http://en.wikipedia.org/wiki/Smartdust

[55]. Romer K., Mattern F.,"The Design Space of Wireless Sensor Networks", *IEEE Wireless Communications*, ETH Zurich, Switzerland , Dec 2004

[56]. Λ. Περλεπές, "Καταγραφή και απεικόνιση δεδομένων δικτύου αύρματων αισθητήρων σε πραγματικό χρόνο", Διπλωματική εργασία, Πανεπιστήμιο Θεσσαλίας, Βόλος, 2007

[57]. Holger Karl, Andreas Willig, "*Protocols and Architectures for WSN*", John Wiley & Sons, Ltd., 2005, p. 7-10,31-32.

[58]. P. Kikiras, ***"Sensor Networks for Pervasive Computing"***, PhD Thesis, National Technical University of Athens, 2005.

[59]. I. Mohammad and I. Mahgoub, ***Handbook of sensor networks: compact wireless and wired sensing systems***, CRC Press, 2005.

[60]. Warneke, B. Atwood, B. Pister, K.S.J., 2001 Smart Dust Mote Forerunners, Fourteenth Annual International Conference on Micro-electromechanical Systems (MEMS 2001), Interlaken, Switzerland, Jan. 21-25, 2001.

[61]. Randall, J. F. On ambient energy sources for powering indoor electronic devices, Ph.D Thesis, Ecole Polytechnique Federale de Lausanne, Switzerland, May 2003.

[62]. Shad Roundy, Dan Steingart, Luc Frechette, Paul Wright, Jan Rabaey, "Power Sources for Wireless Sensor Networks" , *Wireless Sensor Networks* (2004), pp. 1-17

[63]. J. Bautel, ***"Design and Deployment of Wireless Networked Embedded Systems"***, Ph.D Thesis, ETH Zurich, 2005

[64]. http://www.coalesenses.com/index.php?page=core-module-3 (Προσπελάστηκε στις 04/04/2012)

[65]. Crossbow Technology Inc. Revision B, June 2006. "*MPR-MIB Users Manual*".

[66]. Crossbow Technology Inc. Revision A, June 2007. "*MTS/MDA Sensor Board Users Manual".*

[67]. David Gay, Philip Levis, David Culler, Eric Brewer. 2005. "*nesC 1.2 Language Reference Manual*".

[68]. Official TinyOS Project Web Page: www.tinyos.net (προσπελάστηκε στις 2-Φεβρουαρίου 2012)

[69]. D. Culler, ***"TinyOS: Operating System Design for Wireless Sensor Networks"***, Sensors Weekly, www.sensorsmag.com, May 1, 2006.

[70]. P. Levis, S.Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A.Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, ***"Ambient Intelligence, chapter TinyOS: An Operating System for Sensor Networks"***, pages 115–148. Springer, Berlin, 2005.

[71]. IEEE Computer Society, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf

[72]. Preliminary Data Sheet – JN5148, online available at http://www.jennic.com/support/datasheets/jn5148_wireless_microcontroller_datasheet (προσπελάστηκε στις 2-Φεβρουαρίου 2012)

[73]. iSense Core Module 2 DataSheet, online available at http://www.coalesenses.com/download/data_sheets/DS_CM20X_1v0.pdf (προσπελάστηκε στις 2-Φεβρουαρίου 2012)

[74]. R. Anderson and M. Kuhn, Tamper Resistance—A Cautionary Note, *Proc. Second USENIX Workshop Electronic Commerce*, 1996, pp. 1-11.

[75]. D. W. Carman, P. S. Kruus, and B. J. Matt, Constraints and Approaches for Distributed Sensor Network Security, *NAI Labs Technical Report*, Vol. 00, No. 010, Sept. 2000.

[76]. R. Anderson, Why Cryptosystems Fail, *Comm. ACM*, Vol. 37, No. 11, Nov. 1994.

[77]. S. Blythe, B. Fraboni, S. Lall, H. Ahmed, and U. Riu, Layout Reconstruction of Complex Silicon Chips, *IEEE J. Solid-State Circuits*, Vol. 28, No. 2, Feb. 1993, pp. 138-145.

[78]. C. Collberg, C. Thomborson, and D. Low, Breaking Abstractions and Unstructuring Data Structures, *Proc. IEEE Int'l Conf. Computer Languages (ICCL '98)* , May 1998, pp. 28-38.

[79]. C. Wang, J. Hill, J. Knight, and J. Davidson, Software Tamper Resistance: Obstructing Static Analysis of Programs, technical report, *Dept. of Computer Science, Univ. of Virginia*, 2000.

[80]. C. Wang, J. Hill, J. Knight, and J. Davidson, Protection of Software-Based Survivability Mechanisms, *Proc. Int'l Conf. Dependable Systems and Networks*, July 2001, pp. 193-202.

[81]. G. Wroblewski, General Method of Program Code Obfuscation, *Proc. Int'l Conf. Software Eng. Research and Practice (SERP)*, June 2002.

[82]. M. Blum and S. Kannan, Designing Programs that Check Their Work, *J. ACM*, Vol. 42, No. 1, 1995, pp. 269-291.

[83]. H. Wasserman and M. Blum, Software Reliability via Run-Time Result-Checking, *J. ACM*, Vol. 44, No. 6, 1997, pp. 826-849.

[84]. F. Ergun, S. Kannan, S. R. Kumar, R. Rubinfeld, and M. Vishwanathan, Spot-Checkers, *Proc. ACM Symp. Theory of Computing (STOC '98)*, May 1998, pp. 717-751.

[85]. D. Aucsmith, Tamper Resistant Software: An Implementation, Information Hiding, *Springer-Verlag*, 1996, pp. 317-333.

[86]. C. S. Collberg and C. Thomborson, Watermarking, Tamper-Proofing, and Obfuscation—Tools for Software Protection, *IEEE, Trans. Software Eng.*, Vol. 28, No. 8, Aug. 2002, pp. 735-746.

[87]. B. Horne, L. Matheson, C. Sheehan, and R. E. Tarjan, Dynamic Self-Checking Techniques for Improved Tamper Resistance, *Proc. First ACM Workshop Digital Rights Management (DRM)*, London, UK, 2002, pp. 141-159.

[88]. H. Chang and M. J. Atallah, Protecting Software Code by Guards, *Proc. Second ACM Workshop Digital Rights Management (DRM)* , 2002, pp. 160-175.

[89]. Taejoon Park, Kang G. Shin, Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks, *IEEE Transactions on mobile computing*, Vol. 4, No. 3, May/June 2005, pp. 297-309.

[90]. Squawk Project, http://labs.oracle.com/projects/squawk/ (Accessed 4 April 2011).

[91]. A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. SWATT: Software-based ATTestation for Embedded Devices, *In IEEE Symposium on Security and Privacy*, May 2004, pp. 272-282.

[92]. M. Shaneck, K. Mahadevan, V. Kher, and Y. Kim, Remote software-based attestation for wireless sensors. *In Proceedings of the 2nd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks*, 2005, pp. 27-41.

[93]. Y. Yang, X. Wang, S. Zhu, and G. Cao, Distributed softwarebased attestation for node compromise detection in sensor networks, *In Proceedings of the 26th IEEE International Symposium on Reliable Distributed Systems*, 2007, pp. 219-230.

[94]. O. Landsiedel, K. Wehrle, and S. Gotz, Accurate prediction of power consumption in sensor networks, *in Proc. 2nd IEEE Workshop on Embedded Networked Sensors (EmNetS-II). IEEE Computer Society*, 2005, pp. 37–44.

[95]. B. L. Titzer, D. K. Lee, and J. Palsberg, Avrora: scalable sensor network simulation with precise timing, *in Proc. 4th Int'l Conf. Information Processing Sensor Networks (IPSN '05),* 2005, p. 67.

[96]. L. Gu, D. Jia, P. Vicaire, T. Yan, L. Luo, A. Tirumala, Q. Cao, T. He, J. A. Stankovic, T. Abdelzaher, and B. H. Krogh. "Lightweight Detection and Classification for Wireless Sensor Networks in Realistic Environments." In Proc. of 3rd Intl. Conf. on Embedded Networked Sensor Systems (SenSys '05), San Diego, CA, USA, Nov. 2005.

[97]. NIST, Digital hash standard, *Federal Information Processing Standards Publication,* 180-1, April 1995.

[98]. L. Foley, S. Wilson, Analysis of an On-line Random Number Generator, *Trinity College Dublin*, http://www.random.org (Accessed 8 April 2011).

[99]. A. Zaharis, A. I. Martini, L. Perlepes, G. Stamoulis, and P. Kikiras, Live forensics framework for wireless sensor nodes using sandboxing. In *Proceedings of the 6th ACM workshop on QoS and security for wireless and mobile networks (Q2SWinet '10),* 2010, pp. 70-77.

[100]. D. Wheeler and R. Needham., TEA, a Tiny Encryption Algorithm, *Springer-Verlag*, 1995.

[101]. S. Hong, D. Hong, Y. Ko, D. Chang, W. Lee, and S. Lee., Differential cryptanalysis of TEA and XTEA., In *Proceedings of ICISC 2003*, 2003b, pp. 402-417.

[102]. E. Yarrkov, Cryptanalysis of xxtea. Cryptology ePrint Archive, Report 2010/254, 2010, http://eprint.iacr.org/ (Accessed 27 May 2011).

[103]. Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, Margaretha Mazura, Mark Harrison, Markus Eisenhauer, Pat Doody, Internet of Things Strategic Research Roadmap, European Research Cluster on the Internet of Things, *Cluster Strategic Research Agenda,* 2011.

[104]. Feistel H., Cryptography and Computer Privacy, *Scientific American,* Vol. 228, 1973, No. 5, pp. 15-23.

[105]. García Villalba, Luis J., Sandoval Orozco, Ana L., Triviño Cabrera, Alicia, Barenco Abbas, Cláudia J., Routing Protocols in Wireless Sensor Networks., *Sensors,* 9, No. 11, 2009, pp. 8399-8421.

[106]. Victor Shnayder, Mark Hempstead, Bor-rong Chen, Geoff Werner Allen, and Matt Welsh, Simulating the Power Consumption of Large-Scale Sensor Network Applications, In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (SenSys '04), New York, USA, 2004, pp.188-200.

[107]. Ray Hunt, Network Security: The Principles of Threats, Attacks and Intrusions, part1 and part 2, *APRICOT*, 2004.

[108]. Ehab Al-Shaer, Network Security Attacks I: DDOS, *DePaul University*, 2007.

[109]. A. D. Wood and J. A. Stankovic, Denial of service in sensor networks, *Computer*, Vol. 35, No. 10, 2002, pp. 54–62.

[110]. Chien-Chun Ni, Tien-Ruey Hsiang J. D. Tygar, A Power-Preserving Broadcast Protocol for WSNs With DoS Resistance, In *Proceedings of ICCCN'200*8, pp.777-782

[111]. M. Maimour, H. Zeghilet, F. Lepage, Cluster-based Routing Protocols for Energy Efficiency in Wireless Sensor Networks, CRAN laboratory, *Nancy University*, CNRS, France.

[112]. P. K. Kikiras, J. N. Avaritsiotis, Unattended Ground Sensor Network for Force Protection, *Journal of Battlefield Technology,* Vol. 7, No. 3, November 2004.

[113]. L. Perlepes, A. Zaharis, G. Stamoulis and P. Kikiras, "A Framework for Secure Data Delivery in Wireless Sensor Networks**",** Sensors & Transducers Journal, Vol. 14-2, Special Issue, March 2012, pp.125-149

[114]. A. Tavakoli, J. Zhang, and S. H. Son. Group-Based Event Detection in Undersea Sensor Networks. In Proc. of 2nd Intl. Workshop on Networked Sensing Systems (INSS '05), San Diego, CA, USA, June 2005.

[115]. H. Wang, J. Elson, L. Girod, D. Estrin, and K. Yao., "Target Classi_cation and Localization in Habitat Monitoring.", In Proc. of IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing (ICASSP '03), Hong Kong, China, Apr. 2003.

[116]. Georg Wittenburg, Norman Dziengel, Christian Wartenburger, and Jochen Schiller. “A system for distributed event detection in wireless sensor networks.”, In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks* (IPSN '10). ACM, New York, NY, USA, 2010, 94-104.

[117]. Tian He, Sudha Krishnamurthy, John A. Stankovic, Tarek Abdelzaher, Liqian Luo, Radu Stoleru, Ting Yan, Lin Gu, Gang Zhou, Jonathan Hui, Bruce Krogh, “VigilNet: An Integrated Sensor Network System for Energy-Efficient Surveillance”, ACM Transactions on Sensor Networks, 2004.

[118]. Yu Liu, Wei Zhang, “Static Worst-Case Lifetime Estimation of Vigil Net”, IEEE/ACM International Conference on Green Computing and Communications (GreenCom), Sichuan , 4-5 Aug. 2011

[119]. Q. Wang, W. Chen, R. Zheng, K. Lee, and L. Sha. Acoustic target tracking using tiny wireless sensor devices. In *Proc. Of 2nd Intl. Conf. on Information Processing in Sensor Networks (IPSN’03)*, 2003.

[120]. David Lindgren,1 OlofWilsson,2 Fredrik Gustafsson (EURASIPMember),2 and Hans Habberstad1, “Shooter Localization inWirelessMicrophone Networks”, EURASIP Journal on Advances in Signal Processing, Volume 2010,

[121]. J. Millet and B. Balingand, “Latest achievements in gunfire detection systems,” in *Proceedings of the of the RTO-MP-SET-107 Battlefield Acoustic Sensing for ISR Applications*, Neuillysur-Seine, France, 2006.

[122]. R. Szewczyk, A. Mainwaring, J. Polastre, and D. Culler. An analysis of a large scale habitat monitoring application. In *Proc. of the 2nd ACM Intl. Conf. on Embedded Networked Sensor Systems (SenSys’04)*.

[123]. P. Zhang, C. Sadler, S. Lyon, and M. Martonosi. Hardware design experiences in zebranet. In *Proc. of the 2nd ACM Intl. Conf. on Embedded Networked Sensor Systems (SenSys’04)*, Nov. 2004.

[124]. W. S. Conner, J. Chhabra, M. Yarvis, and L. Krishnamurthy, “Experimental evaluation of synchronization and topology control for in-building sensor network applications,” in *Proceedings of the 2nd ACM InternationalWorkshop onWireless Sensor Networks and Applications (WSNA ’03)*, pp. 38–49, San Diego, Calif, USA, September 2003.

[125]. O. Younis and S. Fahmy, “A scalable framework for distributed time synchronization in multi-hop sensor networks,” in *Proceedings of the 2nd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON ’05)*, pp. 13–23, Santa Clara, Calif, USA, September 2005.

[126]. J. Elson and D. Estrin, “Time synchronization for wireless sensor networks,” in *Proceedings of the International Parallel and Distributed Processing Symposium*, 2001.

[127]. G. T. Whipps, L. M. Kaplan, and R. Damarla, “Analysis of sniper localization for mobile, asynchronous sensors,” in *Signal Processing, Sensor Fusion, and Target Recognition XVIII*, vol. 7336 of *Proceedings of SPIE*, 2009.

[128]. L. M. Kaplan, T. Damarla, and T. Pham, "Qol for passive acoustic gunfire localization," in *Proceedings of the 5th IEEE International Conference onMobile Ad-Hoc and Sensor Systems (MASS '08)*, pp. 754–759, Atlanta, Ga, USA, 2008.

[129]. J. DiBiase, H. Silverman and M. Brandstein, "Robust localization in reverberant rooms," Microphone Arrays: Signal Processing Techniques and Applications, Ch. 8, pp. 157-180, Springer, 2001.

[130]. J. M. Peterson and C. Kyriakakis, "Hybrid Algorithm for Robust, Real-time Source Localization in Reverberant Environments," International Conference on Acoustics, Speech and Signal Processing, Vol. 4, pp. 1053-1056, March 2005. 78

[131]. C. H. Knapp and G. C. Carter, "The generalized correlation method for estimation of time delay," IEEE Transaction on Acoustics, Speech, and Signal Processing, Vol. ASSP-24, No. 4, pp. 320-327, August 1976.

[132]. Benjamin Croker, Navinda Kottege,"Using feature vectors to detect frog calls in wireless sensor networks",J. Acoust. Soc. Am. Volume 131, Issue 5, pp. EL400-EL405 (2012)

[133]. Majdi Mansouri, Ouachani Ilham, Hichem Snoussi, and Cédric Richard. 2011. Adaptive quantized target tracking in wireless sensor networks. *Wirel. Netw.* 17, 7 (October 2011)

[134]. Zhou Yanm, Li JianXun, Wang DongLi, "Target tracking in wireless sensor networks using adaptive measurement quantization", SCIENCE CHINA Information Sciences, 2012

[135]. Luo, X., & Giannakis, G. "Energy-constrained optimal quantization for wireless sensor networks." EURASIP Journal on Advances in Signal Processing, 1–12, 2008

[136]. Mansouri, M., Ouchani, I., Snoussi, H., & Richard, C. "Cramer–Rao bound-based adaptive quantization for target tracking in wireless sensor networks.", In IEEE/SP workshop on statistical signal processing, 2009. SSP'09, 2009

[137]. Κοσσυβάκης Θεόφιλος, Δήμου Μαρία, "Προσομοίωση ασύρματων αισθητήρων και μέτρησης μεγεθών σε πραγματικό χρόνο", Ανώτατο Τεχνολογικό Εκπαιδευτικό Ιδρυμα Λάρισας, Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, Λάρισα 2011

[138]. Miklós Maróti, Branislav Kusy, Gyula Simon, and Ákos Lédeczi. 2004. The flooding time synchronization protocol. In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (SenSys '04). ACM, New York, NY, USA, 39-49. DOI=10.1145/1031495.1031501 http://doi.acm.org/10.1145/1031495.1031501

[139]. Hui Dai and Richard Han. 2004., " TSync: a lightweight bidirectional time synchronization service for wireless sensor networks.", *SIGMOBILE Mob. Comput. Commun. Rev.* 8, 1 (January 2004), 125-139. DOI=10.1145/980159.980173 http://doi.acm.org/10.1145/980159.980173

[140]. A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson: "Wireless Sensor Networks for Habitat Monitoring", First ACMWorkshop onWireless Sensor Networks and Applications (WSNA) 2002, pp. 88-97

[141]. Q. Li, D. Rus.,"Global Clock Synchronization in Sensor Networks.", IEEE Trans. on Computers, 55(2), 2006.

[142]. K. Rmer., "Time Synchronization in Ad hoc Networks.", MobiHoc '01.

[143]. S. Ganeriwal, R. Kumar, and M.B. Srivastava. "Timing-sync Protocol for Sensor Networks.", SenSys '03.

[144]. T. Schmid, P. Dutta, M. B. Srivastava., "High-Resolution, Low-Power Time Synchronization an Oxymoron No More.", IPSN '10.

[145]. J. Elson and K. Rmer, "Wireless Sensor Networks: A New Regime for Time Synchronization", Proceedings of the First Workshop on Hot Topics In Networks (HotNets-I), Princeton, New Jersey. October 28- 29 2002.

[146]. J. Elson, L. Girod and D. Estrin, "Fine-Grained Network Time Synchronization using Reference Broadcasts.", Proceedings of the Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), Boston, MA. December 2002

[147]. R. Karp, J. Elson, D. Estrin, and S. Shenker: "Optimal and Global Time Synchronization in Sensornets", Technical Report CENS Technical Report 0012, Center for Embedded Networked Sensing, University of California, Los Angeles, April 2003.

[148]. C. Lenzen, P. Sommer and R. Wattenhofer, "Optimal Clock Synchronization in Networks.", SenSys '09.

[149]. S. Kim, S. Pakzad, D. Culler, J. Demmel, et al.,"Health Monitoring of Civil Infrastructures using Wireless Sensor Networks.", IPSN '07.

[150]. M. Pajic and R. Mangharam, "Anti-jamming for Embedded Wireless Networks.", IPSN '09.

[151]. Z. Zhong, P. Chen, and T. He, "On-demand time synchronization with predictable accuracy", in Proc. INFOCOM, 2011, pp.2480-2488.

[152]. Amit Nayyer, Meenakshi Nayyer, Lalit Kr. Awasthi, "A Comparative study of Time Synchronization Protocols in Wireless Sensor Network", International Journal of Computer Applications, Volume 36– No.11, December 2011

[153]. E. Mangas and A. Bilas, *"FLASH*: Fine-grained Localization in Wireless Sensor Networks using Acoustic Sound Transmissions and High Precision Clock Synchronization*",* 29th IEEE International Conference on Distributed Computing Systems, 2009

[154]. T. Alhmiedat, A. A. Taleb, M. Bsoul, " A Study on Threats Detection and Tracking Systems for Military Applications using WSNs", International Journal of Computer Applications (0975 – 8887), Volume 40– No.15, February 2012

[155]. T. Pham, "Advanced Concepts of Acoustic and Seismic Technology for Military Applications", NATO Research and Technology Organisation, Technical Report, July 2010

[156]. O. Cramer, "The variation of the specific heat ratio and the speed of sound in air with temperature, pressure, humidity, and CO2 concentration", The Journal of the Acoustical Society of America (JASA), J. Acoust. Soc. Am. 93(5) p. 2510-2516; formula at p. 2514.

[157]. K. Rasmussen, "Calculation methods for the physical properties of air used in the calibration of microphones", Department of Acoustic Technology, Technical University of Denmark, technical report PL-11b, May 1997

[158]. F. Martincic and L. Schwiebert., "Distributed Event Detection in Sensor Networks.", In Proc. of Intl. Conf. on Systems and Networks Communications (ICSNC '06), Tahiti, French Polynesia, Oct. 2006.

[159]. M. Li, Y. Liu, and L. Chen., "Non-Threshold based Event Detection for 3D Environment Monitoring in Sensor Networks.", In Proc. of 27th Intl. Conf. on Distributed Computing Systems (ICDCS '07), Toronto, Canada, June 2007.

[160]. H. Niemann. ,"Klassiffokation von Mustern.", Springer, 1st edition, July 1983.

[161]. R. King, ***"TESPAR/FANN: An effective new capability for voice verification in the defense environment"***, Royal Aeronautical Society Conf. on the Role of Intelligent Systems in Defense, pp. 5.1-5.8, London, March 1995.

[162]. G Succi, D. Clapp, R. Gampert, G. Prado, "Footstep Detection and Tracking"

[163]. A. Ekimov, J. Sabatier, "Vibration and Sound Signatures of Human Footsteps in Buildings", Journal of the Acoustical Society of America, v. 120, no. 2, pp. 762-768, August 2006

[164]. J. Scholl, J. agre, L. Clare, M. Gill, "A Low Power Impulse Signal Classifier using the Haar Wavelet Transform", Proc. SPIE, vol. 3577, pp. 136, 1999

[165]. J.C.R.Licklidder, I. Pollack, "Effects of Differentiation, Integration and Infinite Peak Clipping upon the Intelligibility of Speech", journal of the Acoustical society of America, Vol. 20, no. 1, pp42-51, Jan 1948.

[166]. R.A. King and T.C Phipps, "Shannon, TESPAR and Approximation Strategies", ICSPAT 98, Vol. 18, pp 445-453, Great Britain 1999