ΑΝΙΧΝΕΥΣΗ ΕΠΙΘΕΣΕΩΝ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Εκπόνηση Διπλωματικής Εργασίας Από:

Βασιλική Χατζή

Επιβλέπων Καθηγητής

Δρ. Ιορδάνης Κουτσόπουλος

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Η/Υ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΟΚΤΩΒΡΙΟΣ 2008

Περιεχόμενα

Περίληψη 4

1.Εισαγωγή 5

1.1 Γενικά **5**

1.2 Υπόβαθρο..... 6

1.3 Η δική μας συνεισφορά..... 11

1.4 Γενική επισκόπηση γύρω από θέματα εντοπισμού..... 11

1.5 Κακόβουλη συμπεριφορά στο IEEE 802.11 MAC πρωτόκολλο.... 19

1.6 Οργάνωση της εργασίας..... 23

2.Εντοπισμός κακόβουλης συμπεριφοράς με χρήση πολλών παρατηρητών-Αλγόριθμος 1. **24**

2.1 Αλγόριθμος 1..... 24

2.2 Παραλλαγή του Αλγορίθμου 1..... 30

3.Εντοπισμός κακόβουλης συμπεριφοράς με χρήση πολλών παρατηρητών-Αλγόριθμος 2. **31**

3.1 Αλγόριθμος 2..... 31

3.2 Επιλογή των βαρών w_n του αλγορίθμου 2..... 35

4.Εντοπισμός κακόβουλης συμπεριφοράς με χρήση πολλών παρατηρητών-Αλγόριθμος 3. **39**

4.1 Αλγόριθμος 3..... 39

4.2 Επέκταση του Αλγορίθμου 3..... 42

5.Προσομοίωση. **46**

5.1 Σύγκριση των προτεινόμενων αλγορίθμων ως προς την ενέργεια..... 46

5.2 Επιλογή Της Παραμέτρου g..... 51

6.Εύρεση του απαιτούμενου πλήθους παρατηρήσεων. **53**

6.1 Πρόβλημα για την εύρεση του πλήθους των παρατηρήσεων των κόμβων ενός δικτύου..... 53

Σύνοψη **59**

Βιβλιογραφία **60**

Περίληψη

Σε αυτή την εργασία θα αναλύσουμε το πρόβλημα εντοπισμού κακόβουλης συμπεριφοράς σε ασύρματα δίκτυα. Είναι ένα από τα σημαντικότερα προβλήματα που εμφανίζεται σε δίκτυα αυτής της μορφής και η επίλυσή του έχει απασχολήσει πολλούς ερευνητές. Εμείς, αρχικά, θα κάνουμε μια γενική επισκόπηση σε έρευνες διαφόρων επιστημόνων πάνω στο συγκεκριμένο θέμα κι έπειτα, θα προσπαθήσουμε να συνεισφέρουμε στη λύση του προβλήματος προτείνοντας τρείς νέους αλγορίθμους. Επίσης, θα προσπαθήσουμε να βρούμε εκείνες τις τιμές των παραμέτρων των αλγορίθμων που μεγιστοποιούν την απόδοσή τους και τέλος, θα εξετάσουμε την αποδοτικότητα τους μέσω προσομοίωσης. Μας ενδιαφέρει η αποδοτικότητα των αλγορίθμων να μετρηθεί ως προς την ακρίβεια και την κατανάλωση ενέργειας.

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1 Γενικά

Τα ασύρματα δίκτυα διαφέρουν από τα αντίστοιχα ενσύρματα στο ότι χρησιμοποιούν διαφορετικό μέσο για την μετάδοση των δεδομένων τους. Αυτός είναι και ο λόγος που τα ασύρματα δίκτυα είναι πιο ευάλωτα σε επιθέσεις. Οι επιθέσεις στις οποίες υπόκεινται χωρίζονται σε δύο κατηγορίες: *παθητικές* και *ενεργητικές*. Στις παθητικές, η οντότητα που πραγματοποιεί την επίθεση απλά παρατηρεί (κρυφακούει) την συνεχιζόμενη επικοινωνία των άλλων οντοτήτων του δικτύου έχοντας ως στόχο να παραβιάσει την ιδιωτικότητα τους, ενώ στις ενεργητικές η επιτιθέμενη οντότητα εμπλέκεται κανονικά στην μετάδοση. Στην περίπτωση, τώρα, που ο επιτιθέμενος δεν υπακούει στο πρωτόκολλο του δικτύου, λόγω του ότι έχει ως στόχο να επιτύχει καλύτερη απόδοση σε σχέση με τις άλλες οντότητες, η επίθεση ονομάζεται *κακόβουλη συμπεριφορά*.

Οι οντότητες των ασύρματων δικτυών εμφανίζουν κακόβουλη συμπεριφορά έχοντας ως στόχο να βελτιώσουν τη δική τους χρησιμότητα έναντι της απόδοσης των άλλων οντοτήτων. Με τον όρο "χρησιμότητα" αναφερόμαστε, για παράδειγμα, στο ποσό καταναλώμενης ενέργειας ή μεταδιδόμενης

πληροφορίας. Τον στόχο τους αυτό μπορούν να τον επιτύχουν είτε μη προωθώντας μηνύματα άλλων οντοτήτων ώστε να φυλάξουν ενέργεια για τις δικές τους μεταδόσεις είτε εμποδίζοντας άλλες οντότητες από το να αποκτήσουν πρόσβαση στο κανάλι. Επιπλέον, οι οντότητες των ασύρματων δικτύων έχουν γίνει εύκολα προγραμματίσιμες λόγω των ευέλικτων πρωτοκόλλων και αυτό έχει ως αποτέλεσμα, ένα μέλος του δικτύου να μπορεί να "σκαλίσει" το λογισμικό και τελικά να καταφέρει να κάνει κατάχρηση του πρωτοκόλλου.

Η λύση στο πρόβλημα είναι η έγκαιρη και αξιόπιστη ανίχνευση τέτοιων περιπτώσεων κακόβουλης συμπεριφοράς, η οποία τελικά θα πρέπει να οδηγήσει σε άμυνα από την πλευρά του δικτύου και απομόνωση του κακόβουλου μέλους.

1.2 Υπόβαθρο

Έχουν γίνει πολλές μελέτες πάνω στο πρόβλημα εντοπισμού κακόβουλων συμπεριφορών. Στην εργασία [1], οι συγγραφείς Mingyan Li, Ιορδάνης Κουτσόπουλος και Radha Poovendran αναλύουν την περίπτωση επίθεσης σε ασύρματο δίκτυο που χρησιμοποιεί ένα μόνο κανάλι τυχαίας πρόσβασης. Γίνεται υπόθεση ότι ο επιτιθέμενος έχει τη δυνατότητα να ελέγχει την πιθανότητα επίθεσής του και την ακτίνα μετάδοσης (του σήματος του), έχοντας ως στόχο να προκαλέσει την μέγιστη δυνατή "ζημιά" στο δίκτυο. Περιπτώσεις επιθέσεων σαν κι αυτή είναι δύσκολο να εντοπιστούν και να αντιμετωπιστούν. Μέσα από τις λύσεις των προβλημάτων βελτιστοποίησης που θέτονται στην [1], ο επιτιθέμενος από τη μία προσπαθεί να βρεί τη βέλτιστη ισορροπία ανάμεσα στην ένταση της επίθεσης και στο βαθμό στον οποίο γίνεται αντιληπτός από το

σύστημα, και το δίκτυο από την άλλη προσπαθεί να ελαττώσει την επίδραση της επίθεσης μέσω του εντοπισμού του επιτιθέμενου.

Στην εργασία [2], οι συγγραφείς Ιορδάνης Κουτσόπουλος, Svetlana Radosavac και John Baras μελετούν το πρόβλημα εντοπισμού κακόβουλης συμπεριφοράς στο IEEE 802.11 MAC πρωτόκολλο. Οι συγγραφείς χαρακτηρίζουν την κακόβουλη συμπεριφορά με την μεγαλύτερη επίπτωση στο δίκτυο και δείχνουν ότι σε αυτή την περίπτωση ο βέλτιστος ακολουθιακός κανόνας εντοπισμού είναι ο SPRT. Επίσης, δίνουν μερικές λύσεις για το πρόβλημα ειδοποίησης του υπόλοιπου δικτύου σχετικά με την επίθεση.

Δίκτυα που βασίζονται σε CSMA/CA, όπως αυτά που χρησιμοποιούν το IEEE 802.11 DCF πρωτόκολλο, έχουν χρησιμοποιηθεί ευρέως εξαιτίας της εύκολης εφαρμογής τους. Οι συγγραφείς Alberto Lopez Toledo και Xiaodong Wang, στην εργασία [3], προτείνουν μια μέθοδο εντοπισμού εκείνων των επιθέσεων που έχουν στόχο να παρεμποδίζουν τη σωστή λειτουργία του δικτύου (DoS) σε επίπεδο MAC. Αυτή βασίζεται στον υπολογισμό της πιθανότητας οι συγκρούσεις του δικτύου να μπορούν να εξηγηθούν-προβλεφθούν μέσω της απλής παρατήρησης των γεγονότων που συμβαίνουν στο δίκτυο.

Στην εργασία [5] παρουσιάζονται, από τους συγγραφείς Ramanarayanan Viswanathan και Pramod K. Varshney, βασικά θέματα γύρω από την ανίχνευση επιθέσεων με τη βοήθεια ενός συνόλου κατανεμημένων αισθητήρων. Επίσης, εξετάζονται δύο βασικές τοπολογίες δικτύου αισθητήρων, η "παράλληλη" και η "εν σειρά", και δύο βασικά κριτήρια βελτιστοποίησης που χρησιμοποιούνται στην εξαγωγή κανόνων απόφασης.

Οι Antony D.Wood και John A. Stankovic στην εργασία [6], αναλύουν δύο αποτελεσματικά πρωτόκολλα δικτύων αισθητήρων τα οποία δεν συμπεριέλαβαν αρχικά το θέμα της ασφάλειας. Αυτό γίνεται για να δείξουν ότι εάν δεν υπάρχει επαρκής προστασία από επιθέσεις, τα δίκτυα αισθητήρων δεν μπορούν να εφαρμοστούν σε πολλές περιοχές παρά μόνο σε περιορισμένα και ελεγχόμενα περιβάλλοντα. Επίσης, εξηγούν ότι για να επιτευχθεί επιτυχής εφαρμογή ενός δικτύου θα πρέπει η ασφάλεια να ληφθεί υπόψη την ώρα του σχεδιασμού του πρωτοκόλλου.

Στην εργασία [7], οι Pradeep Kyasanur και Nitin H. Vaidya παρουσιάζουν κάποιες μετατροπές του IEEE 802.11 πρωτοκόλλου οι οποίες διευκολύνουν την ανίχνευση κακόβουλων συμπεριφορών σε ένα δίκτυο. Προτείνουν, επίσης, έναν αποτελεσματικό τρόπο ώστε η κακόβουλη οντότητα να συμπεριφέρεται δίκαια.

Οι Venugopal V. Veeravalli, Tamer Başar και H. Vincent Poor στην εργασία [8] εξετάζουν ένα πρόβλημα αποκεντρωμένου ακολουθιακού εντοπισμού στο οποίο κάθε ένας από ένα σύνολο αισθητήρων λαμβάνει μια ακολουθία παρατηρήσεων σχετικά με την υπόθεση. Κάθε αισθητήρας, έπειτα, στέλνει μια ακολουθία μηνυμάτων στο fusion center όπου διεξάγεται ένα ακολουθιακό τεστ για να καθοριστεί η πραγματική απόφαση.

Στην εργασία [9], οι Svetlana Radosavac και John S. Baras ορίζουν ένα σύνολο εγγυήσεων ασφαλείας για ένα σύστημα εντοπισμού κακόβουλης συμπεριφοράς κι επίσης ορίζουν με ακρίβεια ένα μοντέλο "αντιπάλου". Έπειτα, εφαρμόζουν το προτεινόμενο μοντέλο για να ορίσουν αρχικά κάποια

όρια απόδοσης για την χειρότερη περίπτωση "αντιπάλου" και στη συνέχεια το γρηγορότερο σύστημα εντοπισμού κακόβουλης συμπεριφοράς στο IEEE 802.11 MAC πρωτόκολλο. Τέλος, αποδεικνύουν ότι ο αλγόριθμος SPRT, όχι μόνο έχει την καλύτερη απόδοση από όλα τα ακολουθιακά και μη ακολουθιακά τεστ, αλλά είναι και υψηλά αποδοτικός. Αυτό οφείλεται στο ότι δεν απαιτείται αποθήκευση κανενός διανύσματος παρατηρήσεων.

Οι Guofei Gu, Alvaro A. Gardenas και Wenke Lee, στην εργασία [10], μελετούν πως να δημιουργήσουν μια καλή συγκεντρωτική απόφαση χρησιμοποιώντας τις αποφάσεις πολλών ανιχνευτών, με στόχο την βελτίωση της τελικής απόδοσης. Επίσης, προτείνουν μια τεχνική που βασίζεται στο LRT (likelihood ratio test). Μέσα από θεωρητικό συλλογισμό και πειράματα δείχνουν ότι η τεχνική τους είναι πιο ευέλικτη και αποδίδει καλύτερα από άλλες υπάρχουσες συγκεντρωτικές τεχνικές.

Στην εργασία [11], με τη βοήθεια των αποτελεσμάτων του [12], οι Γεώργιος Φελλούρης και Γιώργος Μουστακίδης εισάγουν ένα νέο τεστ για το πρόβλημα του αποκεντρωτικού εντοπισμού μεταβολών το οποίο είναι ασυμπτωτικά βέλτιστο. Σύμφωνα με το προτεινόμενο σχέδιο, οι αισθητήρες εφαρμόζουν τοπικά επαναληπτικούς αλγορίθμους SPRT και στέλνουν ασύγχρονα τις ενός bit αποφάσεις τους σε ένα "κέντρο συγχώνευσης" (fusion center). Το fusion center με τη σειρά του χρησιμοποιεί την ακολουθιακά αποκτούμενη πληροφορία για να εφαρμόσει ένα CUSUM τεστ και να αποφασίσει εαν υπήρξε ή όχι μια μεταβολή.

Στην εργασία [13], οι Bruno M. Jedynak και Sanjeev Khudanpur προτείνουν

μια νέα μέθοδο για την εκτίμηση της συσσωρευτικής συνάρτησης πιθανότητας (pmf) μιας διακριτής και πεπερασμένης τυχαίας μεταβλητής από ένα μικρό δείγμα. Ορίζουν ως σύνολο μέγιστης πιθανοφάνειας (MLS) το σύνολο των pmfs που δίνουν μεγαλύτερο βάρος στις παρατηρούμενες μετρήσεις και προτείνουν την επιλογή, από το MLS, εκείνης της pmf που είναι πιο κοντά σε μία δεδομένη pmf η οποία δηλώνει εκ των προτέρων γνώση.

Οι Alberto Lopez Toledo και Xiaodong Wang, στην εργασία [14], αναπτύσσουν έναν robust μη παραμετρικό ανιχνευτή κακόβουλης συμπεριφοράς στο IEEE 802.11 DCF, βασισμένο στο τεστ Kolmogorov-Smirnov (K-S), ο οποίος δεν απαιτεί αλλαγή στα ήδη υπάρχοντα CSMA/CA πρωτόκολλα. Επίσης, δείχνουν ότι η μέθοδός τους έχει απόδοση συγκρίσιμη με αυτή των βέλτιστων ανιχνευτών, οι οποίοι έχουν πλήρη γνώση για την πλειοψηφία των κακόβουλων συμπεριφορών.

Τέλος, στην εργασία [15], οι Alvaro A. Gardenas, Svetlana Radosavac και John S. Baras αναλύουν το πρόβλημα εντοπισμού κακόβουλων συμπεριφορών στο IEEE 802.11 MAC πρωτόκολλο εκτιμώντας την απόδοση δύο σχημάτων που είχαν προταθεί παλιότερα: του DOMINO και του SPRT. Επίσης, ορίζουν ένα ακόμη τεστ: το μη παραμετρικό CUSUM τεστ το οποίο μοιράζεται την ίδια λογική με το DOMINO αλλά έχει καλύτερη απόδοση.

1.3 Η δική μας συνεισφορά.

Σε αυτή την εργασία θα ασχοληθούμε με την περίπτωση κακόβουλης συμπεριφοράς στο IEEE 802.11 MAC πρωτόκολλο. Επίσης,

- θα μελετήσουμε τη συνεισφορά πολλών οντοτήτων του δικτύου στην διαδικασία εντοπισμού επιθέσεων
- θα αναπτύξουμε τρείς αλγορίθμους για τον εντοπισμό κακόβουλων συμπεριφορών με χρήση πολλών οντοτήτων
- θα αναλύσουμε διάφορα θέματα γύρω από τους προτεινόμενους αλγορίθμους όπως είναι η κατανάλωση ενέργειας, η επιλογή κάποιων παραμέτρων κ.ά.
- και, τέλος, θα εξάγουμε χρήσιμα αποτελέσματα μέσω της προσομοίωσης των προτεινόμενων αλγορίθμων στο πρόγραμμα Matlab.

1.4 Γενική Επισκόπηση Γύρω Από Θέματα Εντοπισμού (Detection)

Σε πολλά επιστημονικά άρθρα έχει γίνει αναφορά στον τρόπο εντοπισμού κακόβουλης συμπεριφοράς από έναν κόμβο του δικτύου κι έχουν αναπτυχθεί πολλά είδη ανίχνευσης. Για παράδειγμα, υπάρχουν διαδικασίες ανίχνευσης που χρησιμοποιούν ένα καθορισμένο αριθμό δειγμάτων (παρατηρήσεων) για να βγάλουν μια απόφαση. Συνήθως, το βασικό μοντέλο παρατήρησης σε αυτές τις διαδικασίες είναι αυτό μιας παρατηρούμενης κυματομορφής συνεχούς χρόνου η οποία αποτελείται από ένα από δύο πιθανά σήματα, το οποίο είναι αλλοιωμένο λόγω προσθετικού θορύβου. Το ζητούμενο είναι να αποφασίσουμε ποιό από τα δύο πιθανά σήματα εμφανίζεται παίρνοντας ένα πεπερασμένο αριθμό δειγμάτων από την παρατηρούμενη κυματομορφή.

Αυτό το πρόβλημα μπορεί να μοντελοποιηθεί από το ακόλουθο ζεύγος υποθέσεων για το χώρο παρατηρήσεων $(\mathbb{R}^n, \mathrm{B}^n)$:

$$H_0 : Y_k = N_k + S_{0k}, k = 1, 2, \ldots, n \tag{0.1}$$

versus

$$H_1 : Y_k = N_k + S_{1k}, k = 1, 2, \ldots, n \tag{0.2}$$

όπου $\underline{Y} = (Y_1, Y_2, \ldots, Y_n)^T$ είναι ένα διάνυσμα παρατηρήσεων που αποτελείται από τα δείγματα της παρατηρούμενης κυματομορφής, $\underline{N} = (N_1, N_2, \ldots, N_n)^T$ είναι ένα διάνυσμα δειγμάτων θορύβου, και $\underline{S}_0 = (S_{01}, S_{02}, \ldots, S_{0n})^T$ και $\underline{S}_1 = (S_{11}, S_{12}, \ldots, S_{1n})^T$ είναι διανύσματα δειγμάτων από τα δύο πιθανά σήματα. Υποθέτουμε ότι ο θόρυβος είναι ανεξάρτητος των σημάτων υπό οποιαδήποτε υπόθεση και ότι η κατανομή πιθανότητας του δεν εξαρτάται από το ποιά υπόθεση ισχύει. Επίσης, θεωρούμε ότι η κατανομή του θορύβου καθορίζεται από μία (συνεχή ή διακριτή) πυκνότητα p_N στο $\mathbb{R}^n$.

Εάν είναι γνωστή η στατιστική συμπεριφορά των S_j για $j = 0, 1$, μπορεί να υπολογιστεί ο λόγος πιθανοφάνειας για τις δύο υποθέσεις. Πιο συγκεκριμένα, δοθέντος $\underline{S}_j = \underline{s}_j \in \mathbb{R}^n$, η παρατήρηση $\underline{Y}$ έχει υπό συνθήκη πυκνότητα

$$p_{\underline{N}}(\underline{y} - \underline{s}_j), \underline{y} \in \mathbb{R}^n. \tag{0.3}$$

Από την εξίσωση (0.3) βλέπουμε ότι η πυκνότητα του $\underline{Y}$ υπό την συνθήκη H_j δίνεται από

$$p_j(\underline{y}) = E\{p_{\underline{N}}(\underline{y} - \underline{S}_j)\}, \underline{y} \in \mathbb{R}^n. \tag{0.4}$$

Ο λόγος πιθανοφάνειας τότε γίνεται:

$$L(\underline{y}) = \frac{E\{p_{\underline{N}}(\underline{y} - \underline{S}_1)\}}{E\{p_{\underline{N}}(\underline{y} - \underline{S}_0)\}}, \underline{y} \in \mathbb{R}^n. \tag{0.5}$$

Επομένως, υπολογίζοντας την εξίσωση (0.5) εξάγονται βέλτιστες διαδικασίες για το αρχικό πρόβλημα.

Μια εναλλακτική προσέγγιση, θεωρώντας δεδομενή την επιθυμητή απόδοση, επιτρέπει στον αριθμό των δειγμάτων να κυμαίνεται ώστε να επιτευχθεί η συγκεκριμένη απόδοση. Ένας ανιχνευτής που χρησιμοποιεί τυχαίο αριθμό δειγμάτων, που εξαρτάται από την ακολουθία παρατηρήσεων, είναι γενικά γνωστός ως ακολουθιακός ανιχνευτής (sequential detector).

Για να περιγράψουμε τέτοιου είδους ανιχνευτές θα χρησιμοποιήσουμε το ακόλουθο μοντέλο:
Υποθέτουμε ότι $\Gamma = \mathbb{R}^\infty$ είναι το σύνολο παρατηρήσεων και ότι οι παρατηρήσεις $Y_k; k = 1, 2, \ldots$ είναι ανεξάρτητες και ταυτοτικά κατανεμημένες σύμφωνα με

$$H_0 : Y_k \sim P_0, k = 1, 2, \ldots \tag{0.6}$$

versus

$$H_1 : Y_k \sim P_1, k = 1, 2, \ldots \tag{0.7}$$

όπου P_0 και P_1 είναι δύο πιθανές κατανομές στο $(\mathbb{R}, \mathrm{B})$, όπου B δηλώνει τη Borel σ-άλγεβρα στο $\mathbb{R}$. Ένας ακολουθιακός κανόνας απόφασης είναι ένα ζεύγος ακολουθιών $(\underline{\phi}, \underline{\delta})$ όπου $\underline{\phi} = \{\phi_j; j = 0, 1, 2, \ldots\}$ ονομάζεται *κανόνας τερματισμού* $(\phi_j : \mathbb{R}^j \to \{0, 1\})$ και $\underline{\delta} = \{\delta_j; j = 0, 1, 2, \ldots\}$ ονομάζεται *τελικός κανόνας απόφασης*, όπου δ_j είναι ένας κανόνας απόφασης στο $(\mathbb{R}^j, \mathrm{B}^j)$ για κάθε $j \geq 0$.

Ο ακολουθιακός κανόνας απόφασης $(\underline{\phi}, \underline{\delta})$ λειτουργεί ως εξής: Για μια ακολουθία παρατηρήσεων $\{y_k; k = 1, 2, \ldots\}$, ο κανόνας $(\underline{\phi}, \underline{\delta})$ παίρνει την απόφαση $\delta_N(y_1, y_2, \ldots, y_N)$, όπου N είναι ο χρόνος τερματισμού που ορίζεται από $N = \min\{n | \phi_n(y_1, y_2, \ldots, y_n) = 1\}$. Δηλαδή, ο $\underline{\phi}$ μας λέει πότε να σταματήσουμε να παίρνουμε δείγματα μέσω του εξής μηχανισμού: όταν $\phi_n(y_1, y_2, \ldots, y_n) = 0$ παίρνουμε ένα ακόμα δείγμα (το n+1-οστό) και όταν $\phi_n(y_1, y_2, \ldots, y_n) = 1$ σταματάμε να συλλέγουμε δείγματα και παίρνουμε μία απόφαση. Με αυτό τον τρόπο, ο αριθμός δειγμάτων, N, είναι τυχαίος καθώς εξαρτάται από την ακολουθία δεδομένων. Ο τελικός κανόνας απόφασης $\underline{\delta}$ μας δείχνει ποιά απόφαση να πάρουμε όταν σταματήσουμε τη συλλογή δειγμάτων.

Ένα παράδειγμα ακολουθιακού κανόνα απόφασης είναι ο SPRT (sequential probability ratio test). Στην περίπτωση που υπάρχουν δύο υποθέσεις H_0, H_1 ο SPRT συλλέγει δείγματα (παρατηρήσεις) μέχρι να υπάρξουν αρκετές αποδείξεις υπέρ μιας εκ των δύο υποθέσεων. Έπειτα από κάθε παρατήρηση στο k-οστό στάδιο, γίνεται επιλογή μεταξύ των εξής επιλογών: δεχόμαστε τη μία ή την άλλη υπόθεση και σταματούμε τη συλλογή παρατηρήσεων ή αναβάλλουμε την λήψη απόφασης για την ώρα και συλλέγουμε την k+1-οστή παρατήρηση. Στον SPRT υπάρχουν δύο κατώφλια a και b που βοηθούν στην λήψη

απόφασης. Εάν το μέτρο σύγκρισης S_k που χρησιμοποιούμε είναι $S_k \leq a$ τότε δεχόμαστε H_1, εάν $S_k < b$ τότε δεχόμαστε H_0, αλλιώς εάν $b \leq S_k < a$ τότε παίρνουμε ακόμη ένα δείγμα. Στο [4], από το θεώρημα Wald-Wolfowitz αποδεικνύεται ότι για να ένα δοθέν επίπεδο απόδοσης, ο SPRT (sequential probability ratio test) είναι ο ακολουθιακός κανόνας απόφασης με τον μικρότερο αναμενόμενο αριθμό δειγμάτων. Επίσης, αποδεικνύεται ότι ο SPRT κατά μέσο όρο χρησιμοποιεί λιγότερα από τα μισά δείγματα του FSS test για τον εντοπισμό ενός σταθερού σήματος.

Στις δύο παραπάνω προσεγγίσεις υποθέτουμε πως ξέρουμε ακριβώς την στατιστική συμπεριφορά των διαθέσιμων παρατηρήσεων. Στην πράξη όμως, δεν είναι ρεαλιστικό να υποθέσουμε κάτι τέτοιο. Χωρίς αυτή την πληροφορία είναι δύσκολο να εφαρμοστούν οι παραπάνω τεχνικές και γι' αυτό το λόγο έχουν σχεδιαστεί δύο άλλες τεχνικές:οι nonparametric και οι robust. Οι μη παραμετρικές τεχνικές προσπαθούν να λύσουν το πρόβλημα της ανίχνευσης με πολύ λίγη πληροφορία για την κατανομή των παρατηρήσεων. Οι δε robust τεχνικές εφαρμόζονται σε περιπτώσεις όπου η κατανομή των παρατηρήσεων είναι περίπου αλλά όχι ακριβώς γνωστή.

Ένας ακολουθιακός αλλά μη παραμετρικός αλγόριθμος ανίχνευσης είναι αυτός του DOMINO. Υποθέτουμε την ύπαρξη ενός κόμβου-παρατηρητή ο οποίος κάνει ένα σύνολο παρατηρήσεων για να πάρει μια απόφαση σχετικά με την ύπαρξη μιας επίθεσης στο δίκτυο. Το πρώτο βήμα του αλγορίθμου βασίζεται στον υπολογισμό της μέσης τιμής των παρατηρήσεων που συλλέγονται:

$$X_{ac} := \sum_{i=1}^{m} X_i/m. \tag{0.8}$$

Στο επόμενο βήμα, η μέση τιμή συγκρίνεται με μια δοθείσα τιμή αναφοράς:

$$X_{ac} < \gamma B, \tag{0.9}$$

όπου η παράμετρος $\gamma (0 < \gamma < 1)$ είναι ένα κατώφλι που ελέγχει το tradeoff μεταξύ του ρυθμού των εσφαλμένων συναγερμών (false alarm rate) και του ρυθμού των χαμένων ανιχνεύσεων (missed detection rate).
Ο αλγόριθμος χρησιμοποιεί μια μεταβλητή με όνομα cheat_count η οποία καταγράφει τον αριθμό των φορών που η μέση τιμή ξεπερνά το κατώφλι γB. Εάν αυτή η μεταβλητή αποκτήσει τιμή μεγαλύτερη από μια καθορισμένη σταθερά K τότε ο DOMINO δίνει σύνθημα συναγερμού. Εάν ο παρατηρούμενος κόμβος κατά την επόμενη περίοδο παρατήρησης συμπεριφέρεται φυσιολογικά, ξεχνιέται μερικώς κάνοντας $cheat\_count := cheat\_count - 1$ (όσο η cheat_count παραμένει μεγαλύτερη του μηδενός).
Πιο συγκεκριμένα, ορίζουμε ως συνθήκη την $\frac{1}{m} \sum_{i=1}^{m} X_i \leq \gamma B$ και η μεταβλητή cheat_count αρχικοποιείται με $cheat\_count := 0$. Αφού συλλεχθούν m δείγματα η ακόλουθη ρουτίνα εκτελείται:

if (συνθήκη) {
  $cheat\_count = cheat\_count + 1$
  if $(cheat\_count > K)${
    raise alarm
  }
}
elseif $cheat\_count > 0$ {
  $cheat\_count = cheat\_count - 1$
}

Είναι τώρα εύκολο να παρατηρήσουμε ότι ο DOMINO είναι ένα ακολουθιακό τεστ (N,d_N) με χρόνο τερματισμού N που ισούται με $m * N_t$ (όπου N_t αντιπροσωπεύει τον αριθμό των βημάτων που χρειάζονται για να ξεπεράσει η cheat_count το K) και ο κανόνας απόφασης κάθε φορά που ο DOMINO τερματίζει είναι $d_N = 1$. Συνήθως, $B = E_0[X_i] = \frac{W}{2}$ όπου W είναι το μέγεθος του contention παραθύρου στο IEEE 802.11 MAC πρωτόκολλο.

Στην περίπτωση που θέλουμε να βελτιώσουμε την απόδοση των συστημάτων ανίχνευσης μπορούμε να χρησιμοποιήσουμε πολλούς κόμβους-παρατηρητές. Μπορούμε να υποθέσουμε ότι αυτοί οι κόμβοι, αφού πρώτα κάνουν κάποια επεξεργασία στις μετρήσεις τους, στέλνουν την πληροφορία που εξάγουν σε άλλους κόμβους και τελικά σε έναν κεντρικό κόμβο, γνωστό ως fusion center, ο οποίος παίρνει και την τελική απόφαση. Το ζητούμενο στις περισσότερες μελέτες είναι να αναπτυχθούν αποδοτικοί αλγόριθμοι για τους κόμβους και το fusion center καθώς επίσης να παρθούν αποφάσεις για θέματα όπως η τοπολογία και η ύπαρξη επικοινωνίας μεταξύ των κόμβων και του fusion center. Στο [5] αναπτύσσονται 2 κύριες τοπολογίες που χρησιμοποιούνται για αυτό το σκοπό και είναι οι εξής: *η παράλληλη* και *η εν σειρά*.

Παράλληλη Διάταξη

Θεωρούμε την παράλληλη διάταξη N κόμβων όπως φαίνεται στο σχήμα 1. Υποθέτουμε ότι οι κόμβοι δεν επικοινωνούν μεταξύ τους και ότι δεν υπάρχει οπισθοδιάδοση (feedback) από το fusion center προς κανένα κόμβο. Έστω y_i μια απλή παρατήρηση που είναι διαθεσιμη στον i-οστό κόμβο. Αυτός ο κόμβος εφαρμόζει τον κανόνα αντιστοίχισης $u_i = \gamma_i(y_i)$ και προωθεί την κβαντισμένη

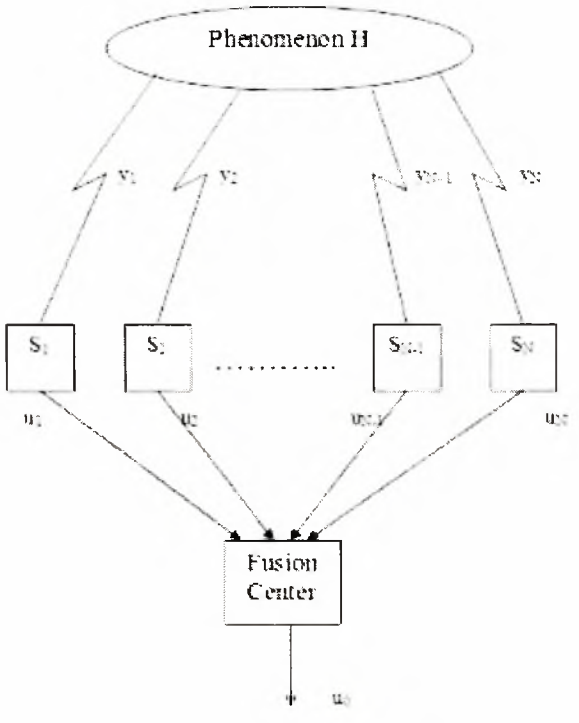

FIGURE 1. Παράλληλη Διάταξη

πληροφορία u_i στο fusion center. Με βάση τη ληφθείσα πληροφορία $u = (u_1, u_2, \ldots, u_N)$ το fusion center παίρνει την τελική απόφαση $u_0 = \gamma_0(u)$. Εάν $u_0 = 1$ τότε ισχύει H_1 ενώ εάν $u_0 = 0$ τότε ισχύει H_0.

Διάταξη Σε Σειρά

Σε μία "εν σειρά" διάταξη N κόμβων, ο (j-1)-οστός κόμβος προωθεί την κβαντισμένη πληροφορία του στον j-οστό, ο οποίος με τη σειρά του παράγει την κβαντισμένη πληροφορία του με βάση την δική του παρατήρηση και τα κβαντισμένα δεδομένα που έλαβε από τον "προηγούμενο" κόμβο (σχήμα 2). Ο πρώτος κόμβος του δικτύου χρησιμοποιεί μόνο την παρατήρησή του για να εξάγει τα κβαντισμένα δεδομένα του, τα οποία είναι για χρήση από τον

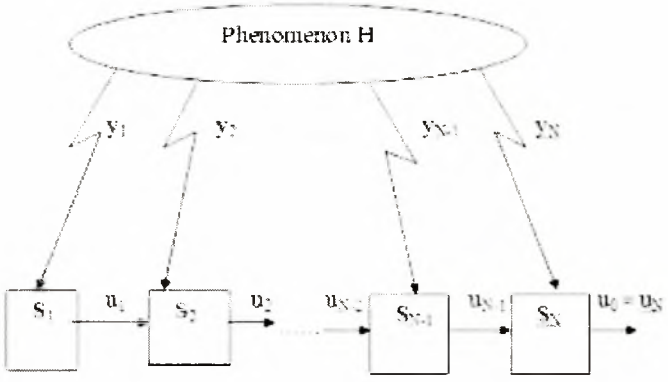

FIGURE 2. Διάταξη Σε Σειρά

"επόμενο" κόμβο. Ο τελευταίος κόμβος του δικτύου παίρνει απόφαση ως προς το ποιά από τις δύο πιθανές υποθέσεις ισχύει.

Σε αυτές τις δύο τοπολογίες θα μπορούσε να συμπεριληφθεί η περίπτωση στην οποία υπάρχει εκτεταμένη επικοινωνία μεταξύ των κόμβων ή και η περίπτωση στην οποία το fusion center στέλνει δεδομένα πίσω σε αυτούς.

1.5 Κακόβουλη Συμπεριφορά Στο IEEE 802.11 MAC Πρωτόκολλο

Στο IEEE 802.11 MAC protocol, η πρόσβαση (κόμβων) στο κανάλι επιτυγχάνεται μέσω πολλαπλής πρόσβαση με έλεγχο φέροντος και αποφυγή σύγκρουσης(CSMA/CA). Ένας κόμβος που θέλει να μεταδώσει ένα πακέτο επιλέγει μια τύχαια τιμή (back-off value) b ομοιόμορφα από το σύνολο 0,1,...,W-1, όπου W είναι το καθορισμένο μέγεθος του contention παραθύρου.Ο

χρόνος είναι χωρισμένος σε ίσα κομμάτια-διαστήματα (slots). Ο back-off μετρητής μειώνει την τιμή του κατά ένα κάθε φορά που αντιλαμβάνεται ότι σε ένα slot χρόνου δε μετέδωσε κανείς και ο κόμβος μεταδίδει ύστερα από b "ανενεργά" slots. Κάθε φορά που το κανάλι είναι απασχολημένο ο μετρητής σταματά να μειώνεται στιγμιαία. Όταν η τιμή του μετρητή γίνει μηδέν τότε ο κόμβος που θέλει να μεταδώσει μπορεί να δεσμεύσει το κανάλι και να το χρησιμοποιήσει για όσο χρόνο διαρκεί η μετάφορά των δεδομένων του. Αρχικά, στέλνει ένα πακέτο αίτησης-για-αποστολή (RTS) στον παραλήπτη, ο οποίος απαντά με ένα ελεύθερος-για-αποστολή (CTS) πακέτο. Κατ'αυτό τον τρόπο, το κανάλι δεσμεύεται για την μετάδοση. Άλλοι κόμβοι που "ακούνε" είτε το RTS είτε το CTS αναβάλλουν την μετάδοσή τους για όσο διαρκεί η μετάδοση των δεδομένων. Εάν η μετάδοση είναι επιτυχής τότε ο κόμβος που μετέδωσε διαλέγει back-off τιμή από το ίδιο σύνολο με μέγεθος W. Σε περίπτωση τώρα που η μετάδοση δεν είναι επιτυχής, λόγω σύγκρουσης ή παρεμβολής, διπλασιάζεται το μεγέθους του contention παραθύρου και ο κόμβος διαλέγει τιμή από το καινούργιο σύνολο.

Με αυτό το τρόπο, όπως καταλαβαίνουμε ,ευνοείται εκείνος ο κόμβος που επιλέγει την μικρότερη back-off τιμή. Επομένως, ένας (κακόβουλος) κόμβος που έχει ως στόχο να αποκτήσει σημαντικό πλεονέκτημα στο μοίρασμα του καναλιού έναντι των άλλων κόμβων, μπορεί να επιλέξει να μην υπακούσει στους κανόνες του πρωτοκόλλου διαλέγοντας μικρές back-off τιμές. Επιπλέον,η πιθανότητα οι "τίμιοι" κόμβοι να αποκτήσουν πρόσβαση στο κανάλι γίνεται όλο και μικρότερη αφού μετά από κάθε ανεπιτυχή μετάδοση είναι αναγκασμένοι να επιλέξουν τις back-off τιμές τους από μεγαλύτερα διαστήματα, λόγω της αύξησης του contention παραθύρου.

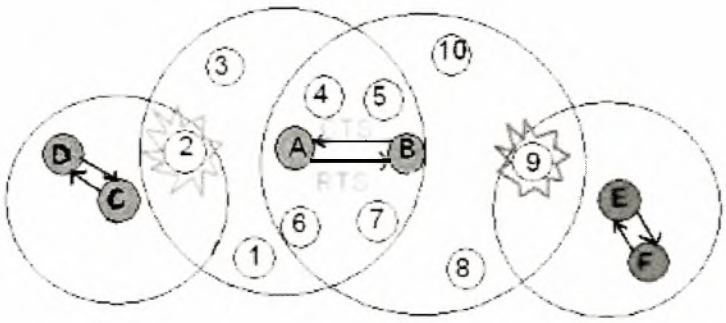

FIGURE 3. Περίπτωση ασύρματου δικτύου όπου ο κόμβος A είναι κακόβουλος

Όσοι κόμβοι είναι αναγκασμένοι να αναβάλλουν την μετάδοση τους, έχουν την δυνατότητα να "ακούν" (παρατηρούν) τις μεταδόσεις των κόμβων που μεταδίδουν, εάν βέβαια βρίσκονται στην εμβέλεια μετάδοσης τους. Το θέμα που προκύπτει είναι εάν υπάρχει δυνατότητα εκμετάλλευσης αυτής της ικανότητας παρατήρησης ώστε να εντοπίζονται περιπτώσεις κακόβουλης συμπεριφοράς και να ειδοποιείται ολόκληρο το δίκτυο.

Ο διαχωρισμός μεταξύ ενός νόμιμου αποστολέα, που τυχαίνει να διαλέγει μικρές back-off τιμές, και ενός κακόβουλου κόμβου που εσκεμένα διαλέγει μικρές back-off τιμές δεν είναι εύκολος και γι' αυτό το λόγο ο εντοπισμός μιας κακόβουλης συμπεριφοράς δεν είναι απλή υπόθεση. Επίσης, το ανοιχτό ασύρματο μέσο (μετάδοσης) και η ύπαρξη παρεμβολής λόγω ταυτόχρονων μεταδόσεων δυσκολεύουν ακόμη περισσότερο την επίλυση του προβλήματος.

Στο παραπάνω σχήμα (εικόνα 3) φαίνεται μια περίπτωση ασύρματου δικτύου

όπου μόνο ο κόμβος Α είναι κακόβουλος και κανένας άλλος κόμβος στη γειτονιά του δε μεταδίδει. (Υποθέτουμε ότι οι κόμβοι έχουν ρολόγια που είναι συγχρονισμένα). Όταν ο κόμβος Α αποκτήσει πρόσβαση στο κανάλι, επικοινωνεί με τον κόμβο Β για να στείλει δεδομένα σε αυτόν(όπως περιγράψαμε πιο πάνω). Το χρονικό διάστημα κατά το οποίο ο Α στέλνει το RTS πακέτο στον Β, όλοι οι κόμβοι (1 έως 7) που βρίσκονται μέσα στην ακτίνα μετάδοσης του "σιωπούν". Το ίδιο ισχύει και για τους κόμβους που βρίσκονται στην ακτίνα μετάδοσης του Β (4 έως 10), όταν αυτός στέλνει το CTS πακέτο. Αφού ολοκληρωθεί η "χειραψία" και η αποστολή των δεδομένων, ο Α προσπαθεί να αποκτήσει ξανά πρόσβαση στο κανάλι διαλέγοντας και πάλι μια back-off τιμή και η διαδικασία επαναλαμβάνεται. Οι κόμβοι 1 έως 10 μπορούν να "ακούσουν" τις μεταδόσεις του Α ή του Β, ή και των δύο. Ας θεωρήσουμε την i-οστή μετάδοση του Α. Ένας κόμβος, που βρίσκεται στην εμβέλεια μετάδοσης του, μπορεί να βρεί τη χρονική στιγμή t_i λήψης του RTS πακέτου από

$$t_i = T_{i-1} + T_{DIFS} + b_i, i > 1, \tag{0.10}$$

όπου T_{i-1} δηλώνει τη χρονική στιγμή που τελείωσε η λήψη των προηγούμενων δεδομένων και b_i είναι η τυχαία back-off τιμή. Επομένως, με αυτό τον τρόπο είναι πολύ εύκολο να εξάγουμε τις back-off τιμές. Μπορούμε να παρατηρήσουμε ότι η back-off τιμή πριν την πρώτη μετάδοση δεδομένων δεν μπορεί να βρεθεί καθώς δεν υπάρχει κάποιο προηγούμενο σημείο αναφοράς για να συγκριθεί. Οι κόμβοι που βρίσκονται στην ακτίνα μετάδοσης του Β μπορούν επίσης να υπολογίσουν τις back-off τιμές που χρησιμοποιούνται από τον Α χρησιμοποιώντας ως σημείο αναφοράς την χρονική στιγμή λήψης του ACK που στέλνεται από τον Β για την προηγούμενη μετάδοση δεδομένων.

Έτσι, ένας κόμβος μπορεί να μετρήσει την χρονική στιγμή t'_i λήψης του CTS πακέτου και να υπολογίσει την back-off τιμή του A από

$$t'_i = T_{ACK_{i-1}} + T_{DIFS} + b_i + T_{RTS} + T_{SIFS}, i > 1. \tag{0.11}$$

Επίσης, πρέπει να σημειωθεί ότι η ταυτότητα του κόμβου που χρησιμοποιεί τις συγκεκριμένες back-off τιμές βρίσκεται από τα αντίστοιχα πεδία των RTS και CTS μηνυμάτων.

Η ακολουθία των back-off τιμών που παρατηρούν οι κόμβοι, θα πρέπει να είναι ίδια για όλους. Εάν όμως υπάρχει παρεμβολή, λόγω ταυτόχρονων μεταδόσεων, η ορθότητα αυτών των παρατηρήσεων μπορεί να επηρεαστεί. Εάν ο κόμβος C του παραπάνω σχήματος αποκτήσει πρόσβαση στο κανάλι, ο κόμβος 2, ο οποίος βρίσκεται στην εμβέλεια μετάδοσης του C, "σιωπά". Η συνεχιζόμενη μετάδοση του C εκλαμβάνεται από τον 2 ως παρεμβολή καθώς "μπερδεύει" τις παρατηρήσεις του. Βλέπουμε ότι οι παρατηρήσεις του 2 επηρεάζονται ανάλογα με την απόστασή του από τους κόμβους A και C.

1.6 Οργάνωση της εργασίας.

Το υπόλοιπο της εργασίας χωρίζεται σε 5 ενότητες (κεφάλαια 2-6). Στα επόμενα τρία κεφάλαια παρουσιάζονται οι τρεις νέοι αλγόριθμοι και κάποια θέματα γύρω από αυτούς. Στο κεφάλαιο 5 εξετάζουμε την αποδοτικότητα των αλγορίθμων μέσω προσομοίωσης και τέλος στο κεφάλαιο 6 προσπαθούμε να επιλύσουμε ένα διαφορετικό πρόβλημα γύρω από τον αριθμό των μετρήσεων των παρατηρητών.

ΚΕΦΑΛΑΙΟ 2

ΕΝΤΟΠΙΣΜΟΣ ΚΑΚΟΒΟΥΛΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΜΕ ΧΡΗΣΗ ΠΟΛΛΩΝ ΠΑΡΑΤΗΡΗΤΩΝ-ΑΛΓΟΡΙΘΜΟΣ 1.

2.1 Αλγόριθμος 1: Αποστολή Αποφάσεων Στο Fusion Center Από Τους Παρατηρητές Και Εξαγωγή Τελικής Απόφασης Από Το Fusion Center.

Στόχος μας τώρα στον εντοπισμό κακόβουλης συμπεριφοράς είναι να εκμεταλλευτούμε τις παρατηρήσεις πολλών "παρατηρητών" για να βελτιώσουμε την απόδοση σε επίπεδο καθυστέρησης ή/και ακρίβειας. Αυτό ισοδυναμεί με την ύπαρξη πολλών παρατηρητών που στέλνουν τις μετρήσεις τους σε έναν άλλο κόμβο (fusion center), ο οποίος τις συνδιάζει κατάλληλα και εξάγει μια απόφαση ως προς την ύπαρξη ή όχι κακόβουλης συμπεριφοράς. Σε αυτό το κεφάλαιο θα δούμε ένα από τα τρία προτεινόμενα σενάρια τέτοιων περιπτώσεων. Πρίν, όμως, από αυτό θα ορίσουμε την κλάση εκείνων των κακόβουλων συμπεριφορών-επιθέσεων που έχουν σημαντικό όφελος-κέρδος.

Ας υποθέσουμε πως ένας κακόβουλος και ένας "νομοταγής" κόμβος θέλουν να αποκτήσουν πρόσβαση στο κανάλι. Έστω Y η τυχαία μεταβλητή που αντιστοιχεί στη back-off τιμή του "νομοταγούς" κόμβου και η οποία είναι ομοιόμορφα κατανεμημένη στο διάστημα [0,W]. Έστω, επίσης, η τυχαία

μεταβλητή X που αντιστοιχεί στη back-off τιμή του "επιτιθέμενου", η οποία έχει άγνωστη συνάρτηση πυκνότητας πιθανότητας (pdf) f(x) με πεδίο ορισμού στο διάστημα [0,W]. Ο επιτιθέμενος έχει πλεονέκτημα έναντι του άλλου κόμβου εάν έχει μεγαλύτερη πιθανότητα πρόσβασης στο κανάλι, εάν δηλαδή οι back-off τιμές του είναι μικρότερες. Όπως αποδεικνύεται στο [2], $Pr(X < Y) = 1 - \frac{E[X]}{W}$, όπου $E[\cdot]$ δηλώνει την μέση τιμή μιας τυχαίας μεταβλητής. Εάν και οι δύο κόμβοι λειτουργούσαν με βάση το πρωτόκολλο τότε η πιθανότητα πρόσβασης στο κανάλι θα ήταν και για τους δύο $p = 1/2$. Εάν ένας από τους δύο είναι ο επιτιθέμενος τότε για αυτόν θα ισχύει $Pr(X < Y) > 1/2$ ή ισοδύναμα $E[X] < W/2$. Αυτό υποδηλώνει μια μετακίνηση της X σε μικρότερες back-off τιμές, σε αντίθεση με την Y για την οποία ισχύει $E[Y] = W/2$. Οι επιθέσεις που έχουν μεγαλύτερο αντίκτυπο στην απόδοση του συστήματος, και στις οποίες πρέπει να επικεντρωθούμε, είναι αυτές που ορίζονται από την παρακάτω κλάση:
$F_\epsilon = \{f(x) : \int_0^W x f(x)dx \leq \frac{W}{2} - \epsilon\}$, όπου ϵ είναι ένας μικρός θετικός αριθμός. Για αυτές ισχύει $Pr(X < Y) > 1/2 + \epsilon/W$.

Παρακάτω δίνονται μερικές σημειογραφίες που θα βοηθήσουν στην περιγραφή και κατανόηση του αλγορίθμου που θα περιγράψουμε:
Αριθμός παρατηρήσεων : M
Αριθμός παρατηρητών : N
Αριθμός επαναλήψεων : Iter
Μέγεθος του contention παραθύρου : W
Τυχαία μεταβλητή που δηλώνει το αναγνωριστικό ενός κόμβου: n
Τυχαία μεταβλητή-μετρητής που μετράει τον αριθμό των επαναλήψεων στον κόμβο n: r_n

Τυχαία μεταβλητή-μετρητής του κόμβου n που μετράει πόσες φορές ισχύει μια συγκεκριμένη συνθήκη: c_n

Τυχαία μεταβλητή μέσω της οποίας καθορίζουμε ένα κατώφλι για τη μεταβλητή c_n: C

Τυχαία μεταβλητή με τιμή που κυμαίνεται μεταξύ 0 και 1: g

Η i-οστή παρατήρηση του κόμβου n : t_i^n

Διάνυσμα παρατηρήσεων του κόμβου n : $T = \{t_1^n, t_2^n, \ldots, t_M^n\}$

Διάνυσμα των back-off τιμών του επιτιθέμενου που υπολογίζονται από τον κόμβο n : $B = \{b_1^n, b_2^n, \ldots, b_M^n\}$

Η i-οστή back-off τιμή του επιτιθέμενου την οποία υπολογίζει ο κόμβος n : b_i^n

Η τυχαία μεταβλητή που αντιστοιχεί στις back-off τιμές του επιτιθέμενου : X

Η pdf της τ.μ. X την οποία υπολογίζει ο κόμβος n : $\widetilde{f}_n(x)$

Η απόφαση που στέλνει ο κόμβος n : d_n

Μέση τιμή της τ.μ. X την οποία υπολογίζει ο κόμβος n : $E_n[X]$

Υποθέτουμε πως στο σύστημα υπάρχει ένας κόμβος που συμπεριφέρεται εγωιστικά, ένα fusion center και N παρατηρητές. Οι N παρατηρητές, που βρίσκονται στην εμβέλεια μετάδοσης είτε του επιτιθέμενου-αποστολέα είτε του παραλήπτη ή και των δύο, κάνουν μετρήσεις και βρίσκουν τις back-off τιμές του επιτιθέμενου με τον τρόπο που περιγράψαμε παραπάνω. Έπειτα, χρησιμοποιώντας ένα κατάλληλο κριτήριο και με τη βοήθεια του αλγορίθμου DOMINO (τον οποίο έχουμε περιγράψει πιο πάνω), βγάζει ο καθένας μια απόφαση για το αν υπάρχει "επίθεση" ή όχι και ανάλογα με την απόφαση του στέλνει 1 bit πληροφορίας στο fusion center. Εαν αποφασίσει ότι υπάρχει κακόβουλη συμπεριφορά τότε στέλνει 1 αλλιώς 0. Όταν το fusion center συγκεντρώσει και τις N αποφάσεις, βγάζει τη δική του απόφαση, που είναι και

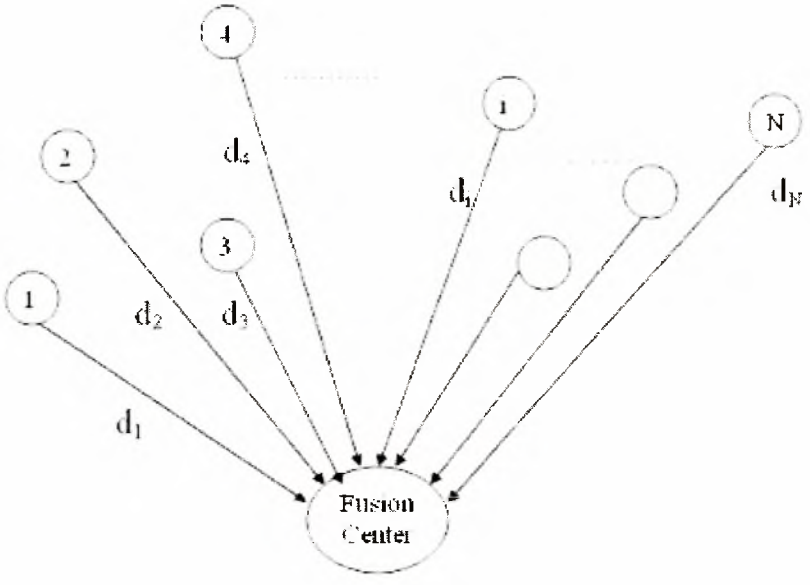

FIGURE 4. Αποστολή Αποφάσεων Στο Fusion Center Από Τους Παρατηρητές

η τελική για όλο το δίκτυο, με βάση την πλειοψηφία (περισσότερα 0 ή περισσότερα 1). Ακολουθεί ο αλγόριθμος της συγκεκριμένης μεθόδου και το αντίστοιχο βοηθητικό σχήμα (εικόνα 4).

Αλγόριθμος 1

Βήμα1: Ορίζεται ο αριθμός Iter των επαναλήψεων της παρακάτω διαδικασίας, ο αριθμός M των παρατηρήσεων που πρόκειται να κάνουν οι παρατηρητές σε κάθε επανάληψη και αρχικοποιούνται οι μετρητές r_n και c_n κάθε κόμβου με την τιμή 0.

Βήμα2: Ως $\{t_1^n, t_2^n, \ldots, t_M^n\}$ ορίζουμε τις M μετρήσεις του παρατηρητή n όπου $n \in \{1, 2, \ldots, N\}$.

Βήμα3: Κάθε παρατηρητής n, χρησιμοποιώντας τους τύπους (11) και (12), εξάγει την ακολουθία $\{b_1^n, b_2^n, \ldots, b_M^n\}$, που αντιστοιχεί στις back-off τιμές του επιτιθέμενου με $b_i^n \in \{0, 1, \ldots, W\}$ και αυξάνει την τιμή του μετρήτη r_n κατά 1.

Βήμα4: Από την παραπάνω ακολουθία ο παρατηρητής βρίσκει την πιθανότητα εμφάνισης κάθε τιμής από 0 έως W και διαμορφώνει την pdf $\widetilde{f}_n(x)$ που πιστεύει πως αντιστοιχεί στον επιτιθέμενο, όπου $X \in \{0, 1, \ldots, W\}$ η τυχαία μεταβλητή που αντιστοίχει στις back-off τιμές.

Βήμα5: Κάθε παρατηρητής βρίσκει τη μέση τιμή της τυχαίας μεταβλητής X: $E_n[X] = \int_0^W x\widetilde{f}_n(x)dx$.

Βήμα6: Εάν ισχύει $E_n[X] \leq gW$ τότε ο μετρήτης c_n αυξάνεται κατά 1 ($c_n = c_n + 1$). Εάν ισχύει $c_n > C$ τότε αποφασίζει "επίθεση", σταματά η επαναληπτική διαδικασία και τίθεται $d_n = 1$, αλλιώς εάν ισχύει $c_n \leq C$ και $r_n < Iter$ τότε επιστρέφει στο βήμα 2.

Βήμα 7: Εαν ισχύει $E_n[X] > gW$ και ισχύει $c_n > 0$ τότε $c_n = c_n - 1$. Εάν $r_n < Iter$ επιστρέφει στο βήμα 2.

Βήμα 8: Στέλνει στο fusion center απόφαση d_n με τιμή 1 εάν έχει αποφασίσει "επίθεση", διαφορετικά στέλνει απόφαση με τιμή 0.

Βήμα9: Το fusion center αφού συλλέξει και τις N αποφάσεις των παρατηρητών

ελέγχει εάν
$\sum_{n=1}^{N} d_n > N/2$. Εάν ισχύει τότε αποφασίζει "επίθεση" αλλιώς "όχι επίθεση".

Επεξήγηση βημάτων 6 έως 9: Στο βήμα 6 ο έλεγχος ($E_n[X] < gW$) γίνεται για να εντοπίσουμε επιθέσεις που είναι τόσο ισχυρές όσο επιθυμούμε εμείς. Ανάλογα με την τιμή της μεταβλητής g καθορίζουμε πόσο ισχυρές είναι οι επιθέσεις που ψάχνουμε. Όσο πιο μικρή η τιμή της g τόσο ισχυρότερες είναι οι επιθέσεις. Δηλαδή ψάχνουμε για τις εκείνες τις επιθέσεις της κλάσης F_ϵ. Μέσω της μεταβλητής c_n, όπως ακριβώς και στο DOMINO, προσπαθούμε να εντοπίσουμε εκείνο τον κόμβο που παρουσιάζει κακόβουλη συμπεριφορά για ένα παρατεταμένο διάστημα και όχι επειδή έτυχε να λάβει μικρές back-off τιμές μια φορά. Η μείωση της μεταβλητής c_n, στο βήμα 7, κάθε φορά που δεν ισχύει η συνθήκη συμβάλλει στο να μην θεωρήσουμε κακόβουλους εκείνους τους κόμβους που έτυχε να λάβουν μικρές back-off τιμές. Στο βήμα 9 ο έλεγχος $\sum_{n=1}^{N} d_n > N/2$ υποδηλώνει ότι η απόφαση λαμβάνεται με βάση την πλειοψηφία των αποφάσεων. Τέλος, η παραπάνω διαδικασία γίνεται για ένα καθορισμένο αριθμό επαναλήψεων με στόχο ο παρατηρητής να πάρει "σύντομα" κάποια απόφαση και να τη στείλει στο fusion center.

2.2 Παραλλαγή του Αλγορίθμου 1

Θα μπορούσαμε τώρα να θεωρήσουμε την περίπτωση του αλγορίθμου 1 με την εξής αλλαγή: ένας κόμβος n όταν αποφασίζει "όχι επίθεση" αντί να θέτει $d_n = 0$ θέτει $d_n = -1$ και στην περίπτωση που αποφασίζει "επίθεση" τότε $d_n = 1$ (όπως και στον αλγόριθμο 1). Επίσης, τώρα, κάθε κόμβος n χαρακτηρίζεται από ένα θετικό βάρος w_n η τιμή του οποίου εξαρτάται από το πόσο σημαντική θεωρούμε την αποφάση που παίρνει ο κόμβος. Με αυτό τον τρόπο δίνουμε συγκεκριμένη βαρύτητα στην απόφαση κάθε κόμβου. Εάν, για παράδειγμα, δύο κόμβοι i και j έχουν βάρη w_i και w_j και ο i δέχεται λιγότερη παρεμβολή απ' ότι ο j, τότε θα θέλαμε $w_i > w_j$. Έτσι, η απόφαση του i θα έχει μεγαλύτερη βαρύτητα από αυτή του j.

Το fusion center, από την πλευρά του, για να εξάγει την τελική απόφαση συλλέγει όλες τις αποφάσεις d_n που του στέλνουν οι κόμβοι , τις αθροίζει $\sum_{n=1}^{N} w_n d_n$ και ελέγχει:
Εάν $\sum_{n=1}^{N} w_n d_n > 0$ τότε απόφασίζει "επίθεση" αλλιώς "όχι επίθεση".

ΚΕΦΑΛΑΙΟ 3

ΕΝΤΟΠΙΣΜΟΣ ΚΑΚΟΒΟΥΛΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΜΕ ΧΡΗΣΗ ΠΟΛΛΩΝ ΠΑΡΑΤΗΡΗΤΩΝ-ΑΛΓΟΡΙΘΜΟΣ 2.

3.1 Αλγόριθμος 2: Αποστολή Συναρτήσεων Πυκνότητας Πιθανότητας(Pdfs) Στο Fusion Center Από Τους Παρατηρητές Και Εξαγωγή Τελικής Απόφασ Από Το Fusion Center.

Παρακάτω δίνονται μερικές σημειογραφίες που θα βοηθήσουν στην περιγραφή και κατανόηση του αλγορίθμου που θα περιγράψουμε:

Αριθμός παρατηρήσεων : M

Αριθμός παρατηρητών : N

Αριθμός επαναλήψεων : Iter

Μέγεθος του contention παραθύρου : W

Τυχαία μεταβλητή που δηλώνει το αναγνωριστικό ενός κόμβου: n

Τυχαία μεταβλητή-μετρητής που μετράει τον αριθμό των επαναλήψεων στον κόμβο n: r_n

Τυχαία μεταβλητή-μετρητής του κόμβου n που μετράει πόσες φορές ισχύει μια συγκεκριμένη συνθήκη: c_n

Τυχαία μεταβλητή μέσω της οποίας καθορίζουμε ένα κατώφλι για τη μεταβλητή c_n: C

Τυχαία μεταβλητή με τιμή που κυμαίνεται μεταξύ 0 και 1: g

Η i-οστή παρατήρηση του κόμβου n : t_i^n

Διάνυσμα παρατηρήσεων του κόμβου n : $T = \{t_1^n, t_2^n, \ldots, t_M^n\}$

Διάνυσμα των back-off τιμών του επιτιθέμενου που υπολογίζονται από τον κόμβο n : $B = \{b_1^n, b_2^n, \ldots, b_M^n\}$

Η i-οστή back-off τιμή του επιτιθέμενου την οποία υπολογίζει ο κόμβος n : b_i^n

Η τυχαία μεταβλητή που αντιστοιχεί στις back-off τιμές του επιτιθέμενου : X

Η pdf της τ.μ. X την οποία υπολογίζει ο κόμβος n : $\widetilde{f}_n(x)$

Η pdf της τ.μ. X την οποία υπολογίζει το fusion center : $f_{fusion}(x)$

Βάρος που αντιστοιχεί στον κόμβο n : w_n

Μέση τιμή της τ.μ. X την οποία υπολογίζει το fusion center : $E_{fc}[X]$

Σε αυτή την περίπτωση οι N παρατηρητές δεν στέλνουν τις αποφάσεις τους στο fusion center αλλά τις pdf που διαμορφώνουν (με τον τρόπο που περιγράψαμε στον αλγόριθμο1) μέσω των παρατηρήσεων τους. Έπειτα, το fusion center συνδιάζει κατάλληλα τις pdf που λαμβάνει και σχηματίζει τη δική του pdf (με τον τρόπο που θα περιγράψουμε παρακάτω). Μέσω ενός κατάλληλου κριτηρίου και με τη βοήθεια του DOMINO παίρνει την τελική απόφαση. Ακολουθεί ο αλγόριθμος της συγκεκριμένης μεθόδου και το αντίστοιχο βοηθητικό σχήμα (εικόνα 5).

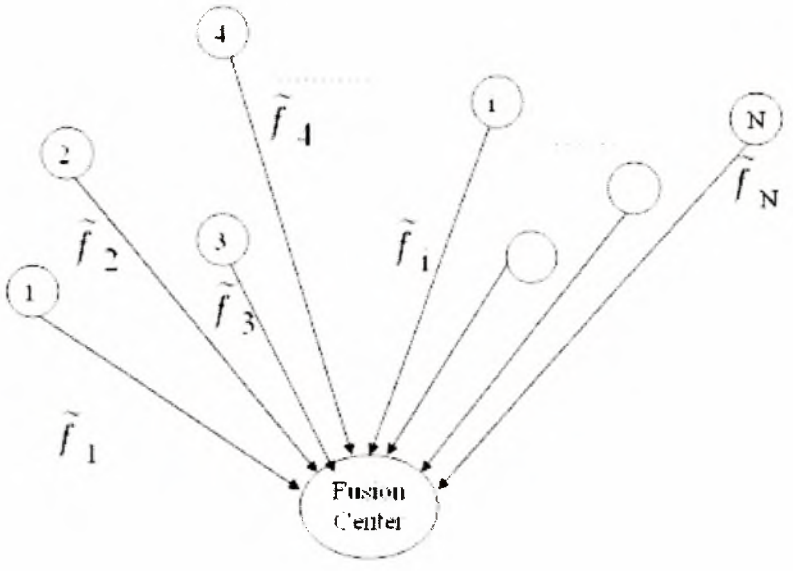

FIGURE 5. Αποστολή Συναρτήσεων Πυκνότητας Πιθανότητας Στο Fusion Center Από Τους Παρατηρητές

Αλγόριθμος 2

Τα βήματα 1 έως 4 είναι ίδια με τα 4 πρώτα του προηγούμενου αλγορίθμου, μόνο που στο βήμα 3 δεν αυξάνεται η τιμή του μετρήτη r_n κατά 1.

Βήμα5: Κάθε παρατηρητής στέλνει στο fusion center την pdf $\widetilde{f}_n(x)$ που έχει σχηματίσει.

Βήμα6: Το fusion center, αφού συλλέξει και τις N pdf των παρατηρητών, δημιουργεί την συνάρτηση $f_{fusion}(x) = \sum_{n=1}^{N} w_n \widetilde{f}_n(x)$ με $\sum_{n=1}^{N} w_n = 1$ και αυξάνει την τιμή του μετρητή του, r_{fc}, κατά 1.

Βήμα7: Έπειτα βρίσκει $E_{fc}[X] = \int_0^W x f_{fusion}(x) dx$.

Βήμα8: Εάν ισχύει $E_{fc}[X] \leq gW$ τότε ο μετρήτης c_{fc} αυξάνεται κατά 1 ($c_{fc} = c_{fc} + 1$). Εάν ισχύει $c_{fc} > C$ τότε αποφασίζει "επίθεση" και σταματά η επαναληπτική διαδικασία , αλλιώς εάν ισχύει $c_{fc} \leq C$ και $r_{fc} < Iter$ τότε

επιστρέφει στο βήμα 2.

Βήμα 9: Εαν ισχύει $E_{fc}[X] > gW$ και ισχύει $c_{fc} > 0$ τότε $c_{fc} = c_{fc} - 1$. Εάν $r_{fc} < Iter$ επιστρέφει στο βήμα 2.

Βήμα 10:Εάν κατά τη διάρκεια της επαναληπτικής διαδικασίας το fusion center δεν αποφάσισε "επίθεση", τότε αποφασίζει "όχι επίθεση".

Επεξήγηση βημάτων 5 έως 10: Στο βήμα 5, όταν λέμε ότι κάθε παρατηρητής στέλνει στο fusion center την pdf $\widetilde{f}_n(x)$ που έχει σχηματίσει, πρακτικά αυτό γίνεται στέλνοντας για κάθε back-off τιμή από 0 έως W το πλήθος των φορών που επιλέχθηκε από τον επιτιθέμενο, π.χ.εάν στις N=100 παρατηρήσεις που έγιναν η τιμή 0 επιλέχθηκε 50 φορές τότε θα σταλεί η τιμή 50 (σε δυαδική μορφή) στο fusion center. Δηλαδή, στην πραγματικότητα οι τιμές που στέλνονται είναι αυτές τις διακριτής $\widetilde{f}_n(x)$. Στο βήμα 6 το fusion center λαμβάνει αυτές τις τιμές από κάθε παρατηρητή και σχηματίζει προσεγγιστικά τις $\widetilde{f}_n(x)$ αν θέλει να είναι σε συνεχή μορφή. Έπειτα, δημιουργεί την συνάρτηση $f_{fusion}(x)$ συνδιάζοντας τις $\widetilde{f}_n(x)$ χρησιμοποιώντας βάρη w_n, τα οποία είναι στην ουσία ποσοστά (καθώς απαιτούμε $\sum_{n=1}^{N} w_n = 1$). Μεγαλύτερα βάρη-ποσοστά δίνονται σε αυτούς τους παρατηρητές που βρίσκονται πιο κοντά στον επιτιθέμενο, γιατί θεωρούμε ότι οι παρατηρήσεις τους δέχονται λιγότερη παρεμβολή. Τα βήματα 8, 9 και 10 γίνονται με την ίδια λογική που έγιναν τα βήματα 6, 7 και 8 του προηγούμενου αλγορίθμου. Στα βήματα 8 και 9, όπου όταν επιτρέπεται γίνεται επιστροφή στο βήμα 2, στην ουσία το fusion center στέλνει ένα σήμα ειδοποίησης στους παρατηρητές για να συλλέξουν και να του στείλουν τα επόμενα δεδομένα προς επεξεργασία.

3.2 Επιλογή των βαρών w_n του αλγορίθμου 2

Υπάρχουν πολλοί τρόποι να επιλέξουμε τα βάρη w_n θα θέλαμε όμως να είναι τέτοια ώστε να πληρούν κάποια κριτήρια. Για παράδειγμα, θα θέλαμε να βρούμε κατάλληλα βάρη ώστε να ελαχιστοποιείται η συνολική καταναλώμενη ενέργεια με τον περιορισμό να μην πέφτει η ακρίβεια κάτω από ένα κατώφλι. Σε αυτή την περίπτωση υποθέτουμε ότι τα βάρη είναι 0 ή 1, δηλαδή οι παρατηρητές είτε στέλνουν τα δεδομένα τους στο fusion center είτε όχι. Αυτό το πρόβλημα θα το αφήσουμε για μελέτη στον αναγνώστη και θα αναλύσουμε το σχεδόν δυαδικό του: θέλουμε να βρούμε εκείνα τα βάρη για τα οποία το μέσο τετραγωνικό σφάλμα ελαχιστοποιείται υπό τον περιορισμό το άθροισμα των βαρών να είναι ίσο με τη μονάδα. Δηλαδή θέλουμε να λύσουμε το εξής πρόβλημα βελτιστοποίησης:

$$\min \|\hat{\underline{f}} - \underline{f}\|^2 \tag{0.12}$$

$$s.t. \sum_{i=1}^{N} w_i = 1 \tag{0.13}$$

,όπου $\hat{\underline{f}} = (\hat{f}_1, \hat{f}_2, \ldots, \hat{f}_{32})$ και $\underline{f} = (f_1, f_2, \ldots, f_{32})$ είναι τα διανύσματα που περιέχουν τις διακριτές τιμές των συναρτήσεων πυκνότητας πιθανότητας $\hat{f(x)}$ και $f(x)$ αντίστοιχα, τα οποία υποθέτουμε πως είναι γνωστά (για την $f(x)$ υποθέτουμε ότι έχουμε την χειρότερη περίπτωση επίθεσης δηλαδή $f(x) = e^{-x}$ (όπως αποδεικνύεται στο [2])). Η συνάρτηση $\hat{f(x)}$ αντιστοιχεί στην $f_{fusion}(x) = \sum_{i=1}^{N} w_i \widetilde{f}_i(x)$ που υπολογίζει το fusion center (όπως δείξαμε στον

αλγόριθμο της περίπτωσης 2) και η συνάρτηση $f(x)$ αντιστοιχεί στην πραγματική συνάρτηση πυκνότητας πιθανότητας του επιτιθέμενου. Η $\hat{f(x)}$ στην ουσία αποτελεί προσέγγιση της $f(x)$. Για να βελτιώσουμε την απόδοση του αλγορίθμου, θέλουμε να ελαχιστοποιήσουμε το μέσο τετραγωνικό σφάλμα αυτών των δύο συναρτήσεων. Στην περίπτωση μας θα προσπαθήσουμε να ελαχιστοποιήσουμε την ευκλείδια νόρμα του σφάλματος:

$$\|\underline{\hat{f}} - \underline{f}\|^2 = \sum_{k=1}^{32}(\hat{f}_k - f_k)^2 = \sum_{k=1}^{32}(\sum_{i=1}^{N} w_i \tilde{f}_{ik} - f_k)^2 \tag{0.14}$$

,όπου $\hat{f}_k$ και f_k δηλώνουν τα στοιχεία των διανυσμάτων $\underline{\hat{f}}$ και $\underline{f}$ αντίστοιχα. Επίσης, όπως εξηγήσαμε παραπάνω, ισχύει:

$$\hat{f(x)} = \sum_{i=1}^{N} w_i \tilde{f}_i(x) \tag{0.15}$$

η οποία εξίσωση μπορεί να γραφεί στη μορφή διανυσμάτων:

$$\underline{\hat{f}} = \sum_{i=1}^{N} w_i \underline{\tilde{f}_i} \tag{0.16}$$

,όπου $\underline{\tilde{f}_i}$ δηλώνει το (γνωστό) διάνυσμα διακριτών τιμών της συνάρτησης πυκνότητας πιθανότητας που υπολογίζει ο παρατηρητής i. Δηλαδή

(0.17)

$$(\hat{f}_1, \hat{f}_2, \ldots, \hat{f}_{32}) = \sum_{i=1}^{N} w_i(\tilde{f}_{i1}, \tilde{f}_{i2}, \ldots, \tilde{f}_{i32}) = (\sum_{i=1}^{N} w_i \tilde{f}_{i1}, \sum_{i=1}^{N} w_i \tilde{f}_{i2}, \ldots, \sum_{i=1}^{N} w_i \tilde{f}_{i32}).$$

Επομένως,

$$\hat{f}_k = \sum_{i=1}^{N} w_i \tilde{f}_{ik} \tag{0.18}$$

κι έτσι προκύπτει η εξίσωση (0.15).

Για να λύσουμε το πρόβλημα ελαχιστοποίησης βρίσκουμε αρχικά τη

Lagrangian συνάρτηση L και έπειτα βρίσκουμε τις μερικές παραγώγους της ως προς w_i και τις θέτουμε ίσες με το 0.

$$L(\underline{w},\lambda) = \|\underline{\tilde{f}} - \underline{f}\|^2 - \lambda(\sum_{i=1}^{N} w_i - 1) = \sum_{k=1}^{32}(\sum_{i=1}^{N} w_i \tilde{f}_{ik} - f_k)^2 - \lambda(\sum_{i=1}^{N} w_i - 1) \tag{0.19}$$

.όπου λ ο πολλαπλασιαστής Lagrange που αντιστοιχεί στον περιορισμό του προβλήματος.

$$\frac{\partial L}{\partial w_j} = 0 \Rightarrow \tag{0.20}$$

$$\frac{\partial[\sum_{k=1}^{32}(\sum_{i=1}^{N} w_i \tilde{f}_{ik} - f_k)^2 - \lambda(\sum_{i=1}^{N} w_i - 1)]}{\partial w_j} = 0 \Rightarrow \tag{0.21}$$

$$\sum_{k=1}^{32} 2(\sum_{i=1}^{N} w_i \tilde{f}_{ik} - f_k)\tilde{f}_{jk} - \lambda = 0 \Rightarrow \cdots \tag{0.22}$$

$$w_j = \frac{\lambda/2 + \sum_{k=1}^{32} f_k \tilde{f}_{jk} - \sum_{i=1, i\neq j}^{N}[w_i \sum_{k=1}^{32}(\tilde{f}_{ik}\tilde{f}_{jk})]}{\sum_{k=1}^{32}(\tilde{f}_{jk})^2} \tag{0.23}$$

Στην εξίσωση (0.24) όλα τα δεδομένα είναι γνωστά εκτός από τον πολλαπλασιαστή λ και τα w_i. Λύνοντας το σύστημα των εξισώσεων που προκύπτουν λαμβάνουμε τις τιμές για όλα τα w_j. Στη συνέχεια αντικαθιστούμε αυτές τις τιμές στην εξίσωση του περιορισμού ($\sum_{j=1}^{N} w_j = 1$) ώστε να εξάγουμε την τιμή του λ.

Για παράδειγμα, ας υποθέσουμε ότι έχουμε μόνο δύο κόμβους (1 και 2) και ότι θέλουμε να βρούμε τα βάρη w_1 και w_2 που τους αντιστοιχούν. Εάν,

$\underline{\tilde{f}_1} =$

(50/100, 20/100, 10/100, 5/100, 5/100, 0, 0, 0, 0, 2/100, 0. 0, 1/100, 0, 1/100. 0, 0, 0, 0, 0, 6/100, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),

$\underline{\widetilde{f}_2} =$

$(50/100, 20/100, 10/100, 5/100, 5/100, 0, 0, 0, 5/100, 2/100, 0, 0, 1/100, 1/100, 0, 0, 0, 0, 0, 0,$
$1/100, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$

και

$\underline{f} =$

$(50/100, 20/100, 10/100, 5/100, 5/100, 5/100, 5/100, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
$0, 0, 0, 0, 0, 0)$

τότε κάνοντας την παραπάνω διαδικασία παίρνουμε: $w_1 = 0.4038$, $w_2 = 0.5962$
και $\lambda = 0.0047$.

ΚΕΦΑΛΑΙΟ 4

ΕΝΤΟΠΙΣΜΟΣ ΚΑΚΟΒΟΥΛΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΜΕ ΧΡΗΣΗ ΠΟΛΛΩΝ ΠΑΡΑΤΗΡΗΤΩΝ-ΑΛΓΟΡΙΘΜΟΣ 3.

4.1 Αλγόριθμος 3: Αποστολή Αποφάσεων Από Τους Παρατηρητές Κάθε Γειτονιάς Στους Κόμβους-Αρχηγούς, Αποστολή Ολικών Αποφάσεων Κάθε Γειτονιάς Από Τους Κόμβους-Αρχηγούς Στο Fusion Center Και Εξαγωγή Τελικής Απόφασης Από Το Fusion Center.

Παρακάτω δίνονται μερικές σημειογραφίες που θα βοηθήσουν στην περιγραφή και κατανόηση του αλγορίθμου που θα περιγράψουμε:

Αριθμός παρατηρήσεων : M

Αριθμός παρατηρητών : N

Αριθμός επαναλήψεων : Iter

Μέγεθος του contention παραθύρου : W

Τυχαία μεταβλητή που δηλώνει το αναγνωριστικό ενός κόμβου: n

Τυχαία μεταβλητή-μετρητής που μετράει τον αριθμό των επαναλήψεων στον κόμβο n: r_n

Τυχαία μεταβλητή-μετρητής του κόμβου n που μετράει πόσες φορές ισχύει μια συγκεκριμένη συνθήκη: c_n

Τυχαία μεταβλητή μέσω της οποίας καθορίζουμε ένα κατώφλι για τη

μεταβλητή c_n: C

Τυχαία μεταβλητή με τιμή που κυμαίνεται μεταξύ 0 και 1: g

Η i-οστή παρατήρηση του κόμβου n : t_i^n

Διάνυσμα παρατηρήσεων του κόμβου n : $T = \{t_1^n, t_2^n, \ldots, t_M^n\}$

Διάνυσμα των back-off τιμών του επιτιθέμενου που υπολογίζονται από τον κόμβο n : $B = \{b_1^n, b_2^n, \ldots, b_M^n\}$

Η i-οστή back-off τιμή του επιτιθέμενου την οποία υπολογίζει ο κόμβος n : b_i^n

Η τυχαία μεταβλητή που αντιστοιχεί στις back-off τιμές του επιτιθέμενου : X

Η pdf της τ.μ. X την οποία υπολογίζει ο κόμβος n : $\widetilde{f}_n(x)$

Η απόφαση που στέλνει ο κόμβος n : d_n

Μέση τιμή της τ.μ. X την οποία υπολογίζει ο κόμβος n : $E_n[X]$

Αριθμός γειτονιών : K

Σύνολο που περιέχει τους κόμβους της γειτονιάς i : U_i

Πλήθος των κόμβων της γειτονιάς i : $|U_i|$

Ολική απόφαση γειτονιάς i : z_i

Απόφαση του κόμβου m της γειτονιάς i : d_m^i

Εδώ υποθέτουμε ότι οι παρατηρητές είναι χωρισμένοι σε γειτονιές και σε κάθε γειτονιά υπάρχει περιττός αριθμός κόμβων. Και αυτή η διαδικασία μοιάζει με αυτή του αλγορίθμου 1 μόνο που τώρα υπάρχει η εξής διαφοροποίηση: αφού οι παρατηρητές κάθε γειτονιάς πάρουν απόφαση, όπως στην περίπτωση του αλγορίθμου 1, αντί να την στείλουν στο fusion center την στέλνουν στον κόμβο-αρχηγό της γειτονιάς τους. Έπειτα, αυτός με βάση την πλειοψηφία των αποφάσεων βγάζει μια τελική απόφαση την οποία και στέλνει στο fusion center. Ακολουθεί ο αλγόριθμος και το αντίστοιχο βοηθητικό σχήμα (εικόνα 6).

Αλγόριθμος 3

Τα βήματα 1 έως 7 είναι ίδια με τα αντίστοιχα του αλγορίθμου 1 μόνο που τώρα στο βήμα 1 ορίζονται και τα σύνολα $U_i, i \in 1, 2, \ldots, K$ που περιέχουν τους κόμβους κάθε γειτονιάς i.

Βήμα8: Οι κόμβοι κάθε γειτονιάς i στέλνουν τις αποφάσεις τους $d_m^i, m \in 1, 2, \ldots, |U_i| - 1$, που είναι 1 εάν έχουν αποφασίσει "επίθεση" διαφορετικά 0, στον κόμβο-αρχηγό της γειτονιάς τους.

Βήμα8: Ο κόμβος-αρχηγός κάθε γειτονιάς i αφού συλλέξει τις $|U_i| - 1$ αποφάσεις των γειτόνων του, συμπεριλαμβανομένης και της δικιάς του, ελέγχει εάν $\sum_{m=1}^{|U_i|} d_m^i > |U_i|/2$. Εάν ισχύει τότε αποφασίζει "επίθεση" (δηλαδή 1) αλλιώς "όχι επίθεση" (δηλαδή 0).

Βήμα9: Κάθε κόμβος-αρχηγός στέλνει στο fusion center την απόφαση του $z_i, i \in 1, 2, \ldots, K$.

Βήμα10: Το fusion center αφού συλλέξει και τις K αποφάσεις ελέγχει εάν $\sum_{i=1}^{K} z_i > K/2$. Εάν ισχύει τότε αποφασίζει "επίθεση" αλλιώς "όχι επίθεση".

Επεξήγηση βημάτων 8 και 10: Και στα δύο βήματα οι έλεγχοι γίνονται ώστε να παρθούν αποφάσεις με βάση την πλειοψηφία.

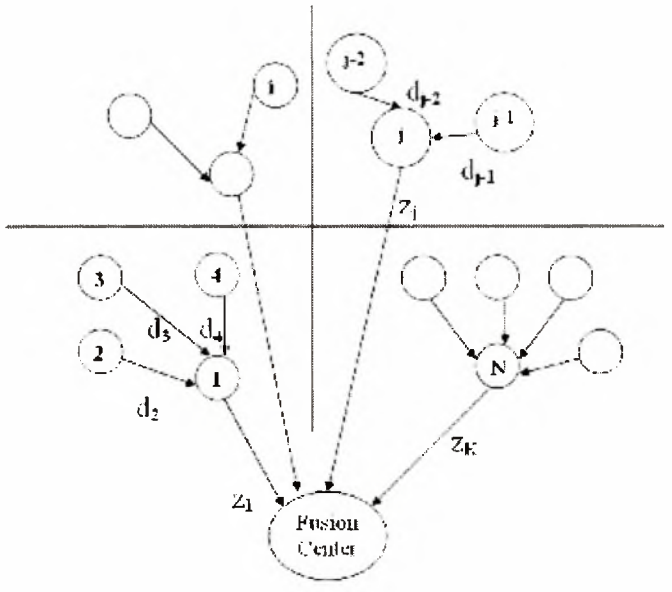

FIGURE 6. Αποστολή Αποφάσεων Στο Fusion Center Από Τους Κόμβους-Αρχηγούς

4.2 Επέκταση του Αλγορίθμου 3

Ως επέκταση-παραλαγή του αλγορίθμου 4 θα μπορούσαμε να θεωρήσουμε την περίπτωση στην οποία οι γειτονιές δεν είναι εξαρχής καθορισμένες αλλά δημιουργούνται δυναμικά από τους ίδιους τους κόμβους. Υποθέτουμε ότι ένας κόμβος i όταν δεν μεταδίδει έχει τη δυνατότητα να "ακούει" τις μετρήσεις ενός άλλου κόμβου j. Επομένως, μπορεί με βάση κάποιο κριτήριο να ελέγξει κατά πόσο σχετίζονται οι μετρήσεις τους. Εάν διαπιστώσει ότι μοιάζουν "πολύ" τότε οι δύο κόμβοι επικοινωνούν έτσι ώστε μόνο ο ένας από τους δύο να μεταδώσει τα δεδομένα του στο fusion center (π.χ. αυτός με τη περισσότερη διαθέσιμη ενέργεια). Με αυτό τον τρόπο οι παρατηρητές καθορίζουν μόνοι τους τις γειτονιές και τους κόμβους- αρχηγούς. (Στην ίδια γειτονιά ανήκουν κόμβοι των οποίων οι μετρήσεις μοιάζουν πολύ.) Με το ίδιο σκεπτικό θα μπορούσαμε

να εφαρμόσουμε την παραπάνω μέθοδο και στην περίπτωση του αλγορίθμου 2 όπου αντί να στέλνουν όλοι οι παρατηρητές τις pdf που υπολογίζουν στο fusion center, να τις στέλνουν μόνο οι κόμβοι που ορίζονται κάθε φορά ως αρχηγοί.

Ένα κριτήριο που θα μπορούσε να χρησιμοποιηθεί για τον έλεγχο ομοιότητας των παρατηρήσεων είναι η απόσταση μεταξύ δύο κατανομών p(x)και q(x):

$$D(p//q) = \sum_{x \in A} p(x) \log \frac{p(x)}{q(x)}. \tag{0.24}$$

Εάν δύο κατανομές είναι απολύτως ίδιες τότε
$D(p//q) = 0$. Στην περίπτωση μας, X είναι η τυχαία μεταβλητή των παρατηρήσεων, $A = \{1, 2, \ldots, 32\}$ είναι το πεδίο τιμών της X και p(x), q(x) είναι οι συναρτήσεις πυκνότητας πιθανότητας των παρατηρήσεων που κάνουν οι κόμβοι i και j αντίστοιχα. Θα μπορούσαμε να θέσουμε ένα λιγότερο αυστηρό κριτήριο αντί του $D(p//q) = 0$, όπως για παράδειγμα $D(p//q) < 0.1$, ανάλογα με το πόσο όμοιες θέλουμε να είναι οι παρατηρήσεις.

Ένα άλλο κριτήριο είναι η συνάρτηση τετραγωνικού σφάλματος η οποία μας δίνει στην ουσία πόσο διαφέρουν (απέχουν) τα δεδομένα που συλλέγουν οι δύο κόμβοι.

$$\sum_{k=1}^{M} (x_{ik} - x_{jk})^2, \tag{0.25}$$

όπου M ο αριθμός των παρατηρήσεων. Για να μπορούν οι κόμβοι να αποφασίσουν κατά πόσο μοιάζουν οι μετρήσεις τους θα πρέπει να οριστεί ένα κατώφλι. Αν η συγκεκριμένη συνάρτηση είναι μικρότερη από αυτό το κατώφλι τότε οι κόμβοι διαπιστώνουν ότι πράγματι οι παρατηρήσεις τους μοιάζουν πολύ.

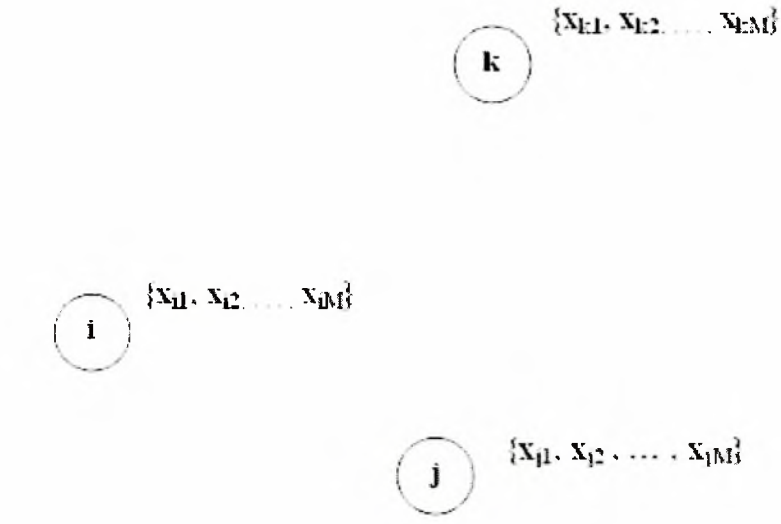

FIGURE 7. Παράδειγμα δικτύου στο οποίο εφαρμόζεται η επέκταση του αλγορίθμου 3. Έλεγχος για ομοιότητα των παρατηρήσεων.

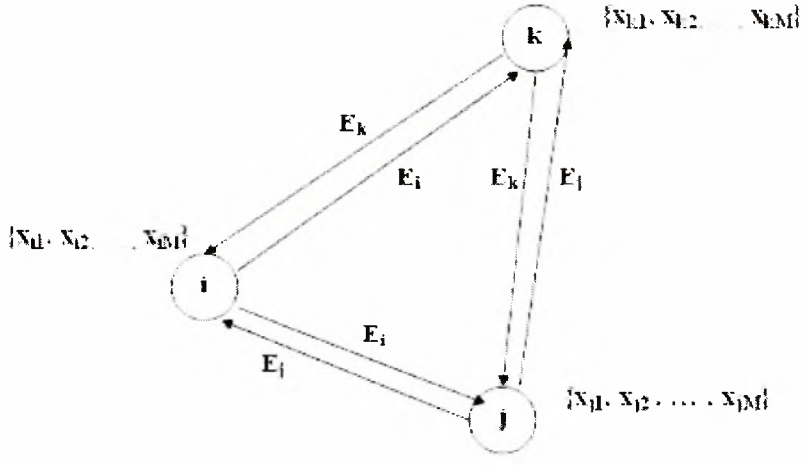

FIGURE 8. Αποστολή των ενεργειών μεταξύ των κόμβων του δικτύου.

Στο σχήμα 7 φαίνονται 3 τυχαίοι κόμβοι του δικτύου. Τα διανύσματα $\{x_{i1}, x_{i2}, \ldots, x_{iM}\}$, $\{x_{j1}, x_{j2}, \ldots, x_{jM}\}$, $\{x_{k1}, x_{k2}, \ldots, x_{kM}\}$ περιέχουν τις M

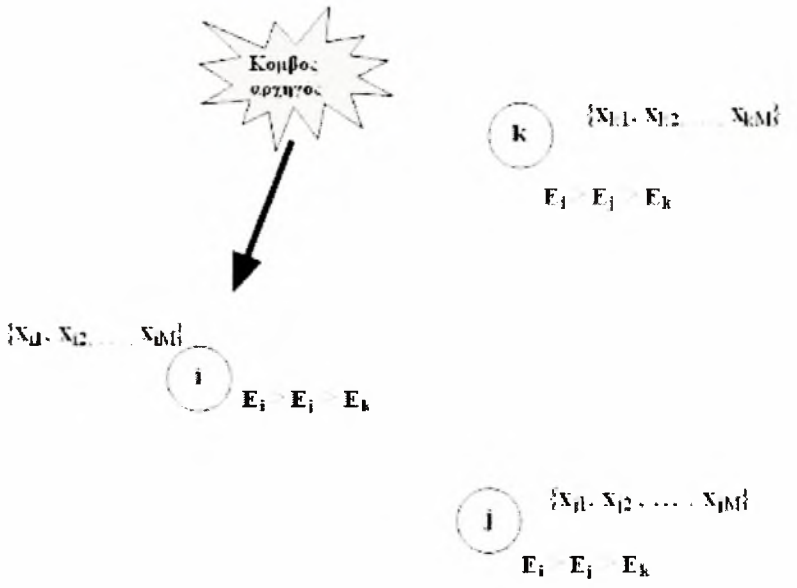

FIGURE 9. Σύγκριση των ενεργειών και εκλογή του κόμβου-αρχηγού.

παρατηρήσεις των κόμβων i,j και k αντίστοιχα. Αφότου κάθε κόμβος του δικτύου συλλέξει-ακούσει τις παρατηρήσεις των άλλων δύο, ελέγχει κατά πόσο μοιάζουν με τις δικές του (μέσω κάποιου κριτηρίου όπως αυτά που αναφέραμε παραπάνω). Ας υποθέσουμε ότι πράγματι οι μετρήσεις των τριών κόμβων μοιάζουν πάρα πολύ μεταξύ τους. Στο επόμενο βήμα κάθε κόμβος θα στείλει σε κάθε άλλο τη διαθέσιμη ενέργεια του (σχήμα 8). Όταν όλοι οι κόμβοι λάβουν τις ενέργειες των άλλων δύο, τις συγκρίνουν και αποφασίζουν τοπικά ποιος θα μεταδώσει στο fusion center (δηλαδή ποιος θα γίνει κόμβος-αρχηγός). Εάν, για παράδειγμα, η ενέργεια E_i του κόμβου i είναι μεγαλύτερη από την E_j και αυτή με τη σειρά της μεγαλύτερη από την E_k, τότε κάθε κόμβος ορίζει ως κόμβο-αρχηγό τον κόμβο i (σχήμα 9).

ΚΕΦΑΛΑΙΟ 5

ΠΡΟΣΟΜΟΙΩΣΗ

5.1 Σύγκριση των προτεινόμενων αλγορίθμων ως προς την ενέργεια.

Θα ξεκινήσουμε προσπαθώντας να συγκρίνουμε τους δύο πρώτους αλγορίθμους ως προς την ενέργεια που καταναλώνεται κατά τη διαδικασία ανίχνευσης. Μπορούμε να πούμε ότι η συνολική καταναλώμενη ενέργεια E ισούται με το άθροισμα των ενεργειών που καταναλώνουν οι κόμβοι του δικτύου. Δηλαδή,

$$E = \sum_{i=1}^{N} E_i, \tag{0.26}$$

όπου E_i η ενέργεια που καταναλώνει ο κόμβος i και N ο αριθμός των κόμβων-παρατηρητών. Η ενέργεια E_i, από την άλλη, ισούται με τον αριθμό των bits που στέλνονται στο fusion center επί την ενέργεια που καταναλώνεται για κάθε bit που στέλνεται. Δηλαδή,

$$E_i = k \cdot e_i, \tag{0.27}$$

όπου k ο αριθμός των bits που στέλνονται στο fusion center από τον κόμβο i.

Για να προσεγγίσουμε, τώρα, την ενέργεια e_i θυμόμαστε ότι ενέργεια = ισχύς × χρόνος. Οπότε, $e_i = p_i \cdot \tau$ όπου p_i είναι η ισχύς μετάδοσης του κόμβου i και

τ ο απαιτούμενος χρόνος μετάδοσης ενός bit. Επίσης, γνωρίζουμε ότι η ισχύς μετάδοσης είναι αντιστρόφως ανάλογη της απόστασης και ότι ο λόγος $\frac{p_i}{d_i^2}$, που αποτελεί την εξασθένηση της ισχύος του μεταδιδόμενου σήματος λόγω απόστασης, θα πρέπει να είναι μικρότερος από ένα κατώφλι γ, δηλαδή $\frac{p_i}{d_i^2} \leq \gamma$. Επομένως, προσεγγιστικά μπορούμε να πούμε ότι:

$$(0.28)\quad E = \sum_{i=1}^{N} E_i = \sum_{i=1}^{N} k \cdot e_i = \sum_{i=1}^{N} k \cdot p_i \cdot \tau \approx \sum_{i=1}^{N} k \cdot \gamma \cdot d_i^2 \cdot \tau = k \cdot \gamma \cdot \tau \sum_{i=1}^{N} d_i^2.$$

Η παραπάνω σχέση ισχύει και για τους δύο αλγορίθμους. Για την περίπτωση του αλγορίθμου 1 ισχύει $k = 1$, οπότε $E = \gamma \cdot \tau \sum_{i=1}^{N} d_i^2$. Από την άλλη, για την περίπτωση του αλγορίθμου 2 ισχύει: για κάθε τιμή από 1 έως 32 ο κόμβος στέλνει $\lceil \log_2 M \rceil$ bits για να παραστήσει την πιθανότητα εμφάνισης κάθε τιμής(αυτό ο ισχύει για $M \geq 3$, για M=1 απαιτείται 1 bit και για M=2 απαιτούνται 2 bits). Για παράδειγμα, εάν κάθε κόμβος κάνει $M = 100$ μετρήσεις και η back-off τιμή 1 εμφανίζεται 50 φορές (από τις 100) τότε θα πρέπει να στείλει στο fusion center τη δυαδική μορφή του 50 χρησιμοποιώντας 7 bits. Άρα, κάθε φορά που πρέπει να στείλει τα δεδομένα του στο fusion center, στέλνει $32 \cdot \lceil \log_2 M \rceil$ bits. Εάν ορίσουμε ως iter την τυχαία μεταβλητή που δηλώνει τον αριθμό των απαιτούμενων επαναλήψεων μέχρι να εξαχθεί απόφαση από το fusion center, τότε $k = iter \cdot 32 \cdot \lceil \log_2 M \rceil$ Επομένως, $E = iter \cdot 32 \cdot \lceil \log_2 M \rceil \cdot \gamma \cdot \tau \cdot \sum_{i=1}^{N} d_i^2$.

Θα προσπαθήσουμε να συγκρίνουμε τις ενέργειες που καταναλώνονται στους δύο πρώτους αλγορίθμουςς υπολογίζοντας τις τιμές τους για διάφορες τιμές του αριθμού των παρατηρητών N και των μετρήσεων M.

Στην εικόνα10 (figure 10) παριστάνονται οι τιμές που παίρνουν οι

καταναλώμενες ενέργειες στους 2 πρώτους αλγορίθμους αλλάζοντας των αριθμό των παρατηρητών ($N = 6, 9, 12, 15, 18, 21$) και κρατώντας τον αριθμό των παρατηρήσεων σταθερό($M = 10$). Είναι προφανές ότι η συνολική καταναλώμενη ενέργεια στην περίπτωση του αλγορίθμου 2 είναι πάντα κατά πολύ μεγαλύτερη από αυτή του πρώτου. Για την ακρίβεια, είναι k φορές μεγαλύτερη. Επίσης, παρατηρούμε ότι αύξηση του αριθμού των παρατηρητών N δε σημαίνει απαραίτητα και αύξηση της συνολικής ενέργειας που καταναλώνεται. Αυτό συμβαίνει διότι ακόμη κι εάν έχουμε μια μεγάλη τιμή για το N, οι αποστάσεις των παρατηρητών από το fusion center μπορεί να είναι πολύ μικρές (αφού επιλέγονται τυχαία) κι επομένως η αυτή η συνολική ενέργεια να είναι μικρότερη από μια άλλη που αντιστοιχεί σε μικρότερη τιμή του N.

Όπως βλέπουμε και από την εικόνα 11 (figure 11), στην περίπτωση που ο αριθμός των παρατηρητών είναι σταθερός ($N = 6$) και αλλάζει μόνο ο αριθμός των μετρήσεων ($M = 10, 20, 30, 40$) και πάλι η ενέργεια που καταναλώνεται στην περίπτωση του αλγορίθμου 2 είναι πάντα k φορές μεγαλύτερη από αυτή του αλγορίθμου 1 (μόνο που τώρα η τιμή του k αλλάζει κάθε φορά που αλλάζει η τιμή του M). Η ενέργεια στην περίπτωση του αλγορίθμου 1 είναι σταθερή διότι δεν εξαρτάται από των αριθμό των παρατηρήσεων M. Από την άλλη, στην περίπτωση του αλγορίθμου 2, παρατηρούμε ότι κάθε φορά που αυξάνεται ο αριθμός των παρατηρήσεων M, η συνολική ενέργεια που καταναλώνεται είναι ίση ή μεγαλύτερη από αυτή που αντιστοιχεί σε μικρότερη τιμή του M.

Οι υπολογισμοί των ενεργειών, που γίνονται με τη βοήθεια του προγράμματος MATLAB, των οποίων τα αποτελέσματα φαίνονται στις εικόνες 10 και 11, γίνονται για $\tau = 0.5msec = 5 \cdot 10^{-4}sec$ και $\gamma = 64$(καθαρός αριθμός). Επίσης,

οι ενέργειες είναι εκφρασμένες σε kilojoule και ο άξονας των ενεργειών (y) είναι σε λογαριθμική κλίμακα για να δούμε καλύτερα τις διαφορές.

Είναι επίσης προφανές ότι η κατανάλωση ενέργειας στην περίπτωση του αλγορίθμου 3 είναι μικρότερη από αυτή του αλγορίθμου 1 (άρα και του 2) αφού δεν μεταδίδουν όλοι οι κόμβοι στο fusion center. Οι κόμβοι που μεταδίδουν στους κόμβους-αρχηγούς καταναλώνουν λιγότερη ενέργεια από ότι εάν μετέδιδαν στο fusion center καθώς το σήμα που στέλνουν διανύει μικρότερη απόσταση (όπως αναφέραμε $E \sim d^2$).

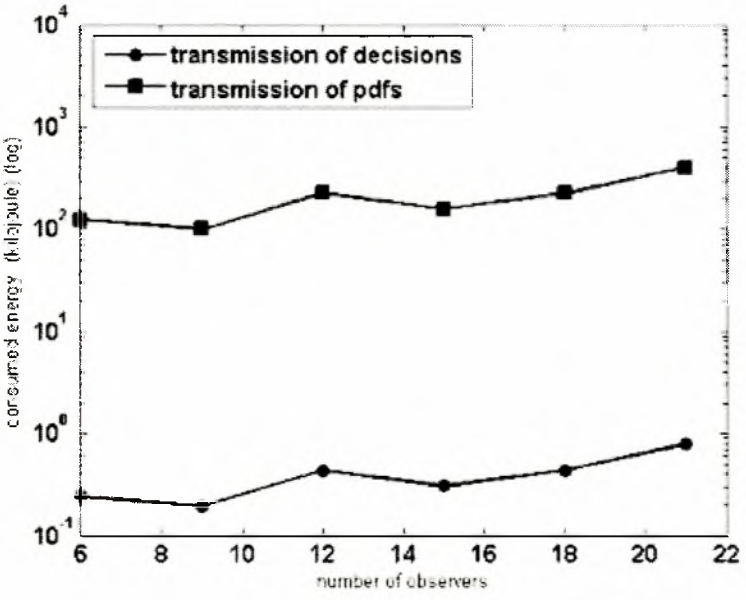

FIGURE 10. Κατανάλωση ενέργειας για N=6,9,12,15,18,21 παρατηρητές

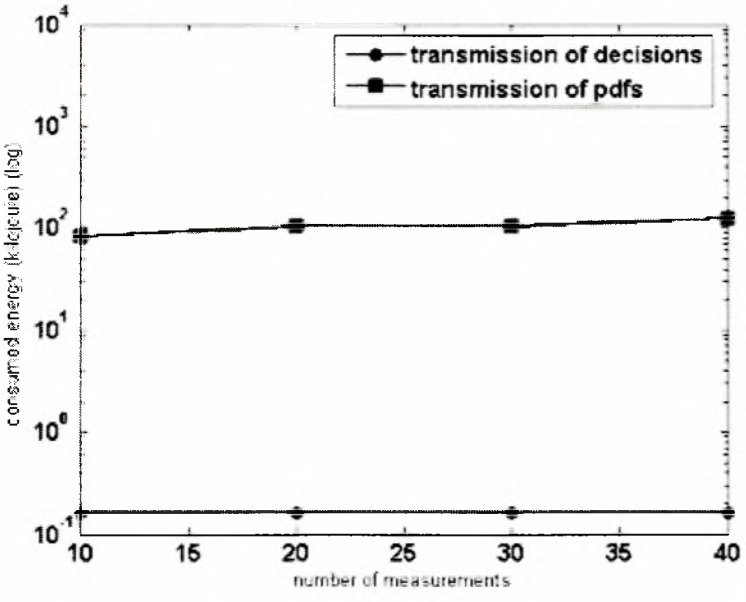

FIGURE 11. Κατανάλωση ενέργειας για M=10,20,30,40 μετρήσεις

5.2 Επιλογή Της Παραμέτρου g.

Με στόχο να επιλέξουμε εκείνη την τιμή της παράμετρου g για την οποία έχουμε μικρές πιθανότητες λανθασμένου συναγερμού (false alarm) P_{FA} και χαμένου εντοπισμού (missed detection) P_{MD} και για την οποία υπάρχει μια ισορροπία μεταξύ αυτών των δύο πιθανοτήτων κάνουμε τους κατάλληλους υπολογισμούς μέσω του MATLAB.

Για την περίπτωση του πρώτου αλγορίθμου εκτελούμε 100 πειράματα για κάθε πιθανή τιμή του g ($0 < g \leq 1$) με στόχο να υπολογίσουμε τα ποσοστά λανθασμένων συναγερμών και τα ποσοστά των χαμένων εντοπισμών που αντιστοιχούν σε κάθε μία από τις πιθανές τιμές του g. Όπως φαίνεται και από την εικόνα 12, η τιμή του g για την οποία υπάρχει μια ισορροπία μεταξύ P_{FA} και P_{MD} είναι η g=0.3. Στα παραπάνω πειράματα εκτελούμε τον αλγόριθμο 1 μεταβάλλοντας την τιμή του g και διατηρώντας όλες τις υπόλοιπες παραμέτρους σταθερές. Επίσης, παρατηρούμε ότι όσο πιο μικρή είναι η τιμή της παραμέτρου g τόσο πιο μικρή είναι η πιθανότητα false alarm και τόσο πιο μεγάλη είναι η πιθανότητα missed detection. Αυτό το αποτέλεσμα μπορούμε να πούμε πως είναι κι αυτό που περιμέναμε καθώς όσο πιο μικρή είναι η τιμή του g, άλλο τόσο μικρή είναι η τιμή του $g \cdot W$, κι έτσι είμαστε πιο αυστηροί στο τι θεωρούμε "επίθεση". Δηλαδή, δίνουμε πιο σπάνια λάθους συναγερμούς και χάνουμε πιο συχνά εντοπισμούς.

Τα ίδια ακριβώς αποτελέσματα παίρνουμε κάνοντας τα ίδια πειράματα για τους άλλους δύο αλγορίθμους. Αυτό φαίνεται και από τις εικόνες 13 και 14 που ακολουθούν.

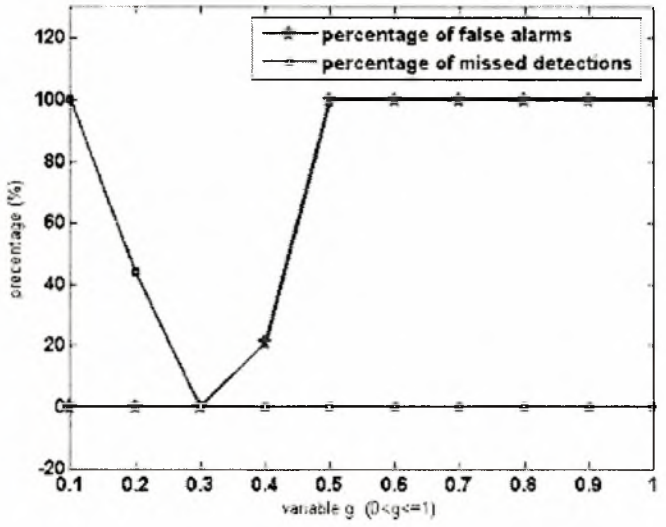

FIGURE 12. Επιλογή κατάλληλης τιμής για την παράμετρο g για τον αλγόριθμο 1.

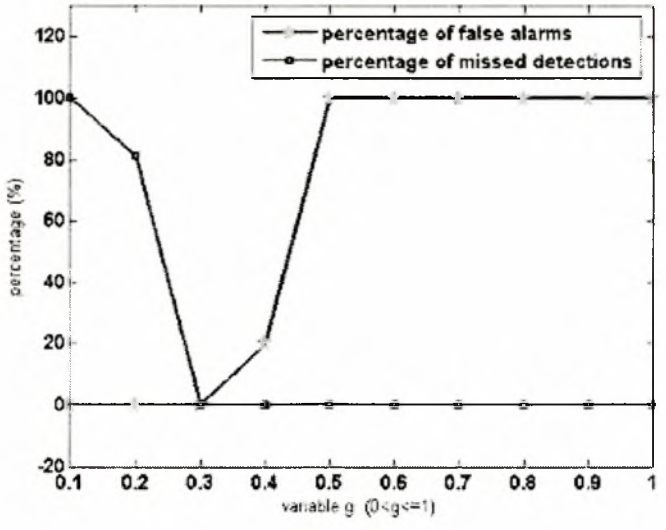

FIGURE 13. Επιλογή κατάλληλης τιμής για την παράμετρο g για τον αλγόριθμο 2.

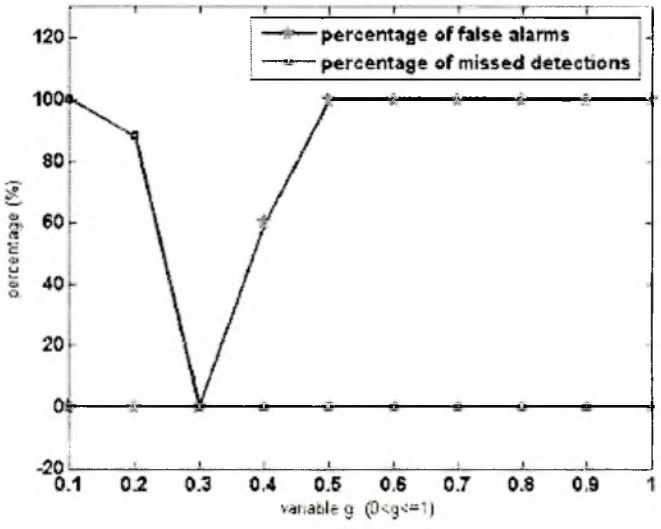

FIGURE 14. Επιλογή κατάλληλης τιμής για την παράμετρο g για τον αλγόριθμο 3.

ΚΕΦΑΛΑΙΟ 6

ΕΥΡΕΣΗ ΤΟΥ ΑΠΑΙΤΟΥΜΕΝΟΥ ΠΛΗΘΟΥΣ ΠΑΡΑΤΗΡΗΣΕΩΝ.

6.1 Πρόβλημα για την εύρεση του πλήθους των παρατηρήσεων των κόμβων ενός δικτύου.

Σε αυτό το κεφάλαιο θα αναλύσουμε ένα άλλο πρόβλημα γύρω από τη διαδικασία εντοπισμού κακόβουλων επιθέσεων. Αρχικά, υποθέτουμε ένα δίκτυο με δύο κόμβους-παρατηρητές και ένα fusion center (όπως φαίνεται στο σχήμα

15). Ο παρατηρητής 1 στέλνει στο fusion center τις μετρήσεις του (τις οποίες έχει κάνει με τον τρόπο που έχουμε εξηγήσει παραπάνω), που είναι K1 σε πλήθος και ο παρατηρητής 2 στέλνει κι αυτός τις μετρήσεις του που είναι K2 σε πλήθος. Για τις μετρήσεις(παρατηρήσεις) του κόμβου 1 ισχύουν τα εξής:

$H_0 : x1 = N1$

ή

$H_1 : x1 = \theta + N1$

και για τις μετρήσεις του κόμβου 2 ισχύουν τα εξής:

$H_0 : x2 = N2$

ή

$H_1 : x2 = \theta + N2,$

όπου H0 και H1 είναι οι υποθέσεις ότι δεν έχουμε επίθεση και ότι έχουμε

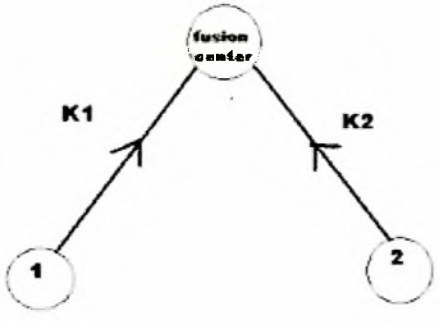

FIGURE 15

επίθεση αντίστοιχα. Οι N1 και N2 είναι Γκαουσιανές τυχαίες μεταβλητές, ανεξάρτητες μεταξύ τους, με $N1 \sim N(0, \sigma_1^2)$ και $N2 \sim N(0, \sigma_2^2)$, (με σ_1^2 και σ_2^2 διαφορετικά). Επίσης, η μεταβλητή θ είναι αυτή που προσδιορίζει την επίθεση.

Υποθέτουμε ότι οι κόμβοι 1 και 2 για να στείλουν μια μέτρησή τους απαιτείται να καταναλώσουν e1 και e2 joules αντίστοιχα. Επομένως, η συνολική ενέργεια που πρέπει να καταναλώσουν και οι δύο για να μεταδώσουν τις μετρήσεις τους είναι:

$$E_{o\lambda} = \sum_{i=1}^{2} K_i \cdot e_i. \tag{0.29}$$

Το fusion center με τη σειρά του, αφού λάβει τις μετρήσεις των παρατηρητών, υπολογίζει τον παρακάτω λόγο πιθανοφάνειας με στόχο να αποφασίσει για το αν υπάρχει υπάρχει ή όχι επίθεση στο δίκτυο:

$$L(\underline{x}) = \frac{P_1(\underline{x})}{P_0(\underline{x})} = \frac{P(\underline{x}|H_1)}{P(\underline{x}|H_0)}, \tag{0.30}$$

όπου $\underline{x} = (x_1^{(1)}, x_2^{(1)}, , x_{K_1}^{(1)}, x_1^{(2)}, x_2^{(2)}, , x_{K_2}^{(2)})$ είναι το διάνυσμα παρατηρήσεων των δύο παρατηρητών. Με τους δείκτες (1) και (2) προσδιορίζουμε τις μετρήσεις των κόμβων 1 και 2 αντίστοιχα.

Το fusion center αφού υπολογίσει τον λόγο της εξίσωσης (0.30), ανάλογα με το αποτέλεσμα παίρνει μία απόφαση:

- εάν $L(\underline{x}) > 1$ τότε αποφασίζει ότι ισχύει η υπόθεση H_1
- εάν $L(\underline{x}) < 1$ τότε αποφασίζει ότι ισχύει η υπόθεση H_0

Ισοδύναμα,

- εάν $\log L(\underline{x}) > 0$ τότε αποφασίζει ότι ισχύει η υπόθεση H_1
- εάν $\log L(\underline{x}) < 0$ τότε αποφασίζει ότι ισχύει η υπόθεση H_0.

Εάν τώρα ορίσουμε ως P_{FA} την πιθανότητα το fusion center να δώσει λάθος συναγερμό, δηλαδή να αποφασίσει "επίθεση" ενώ δεν υπάρχει επίθεση στο δίκτυο, αυτή είναι ίση με:

$$P_{FA} = P[H_1|H_0] = P[\log L(\underline{x}) > 0|H_0]. \tag{0.31}$$

Εφόσον οι παρατηρήσεις του κόμβου 1 ακολουθούν την Γκαουσιανή κατανομή, η συνάρτηση πυκνότητας πιθανότητάς (pdf) τους είναι η εξής:

- $f_1(x|H_0) = \frac{1}{\sigma_1\sqrt{2\pi}} \cdot e^{-x^2/2\sigma_1^2}$ εάν ισχύει η υπόθεση H_0

ή

- $f_1(x|H_1) = \frac{1}{\sigma_1\sqrt{2\pi}} \cdot e^{-(x-\theta)^2/2\sigma_1^2}$ εάν ισχύει η υπόθεση H_1.

Αντίστοιχα για την pdf των παρατηρήσεων του κόμβου 2 ισχύουν τα εξής:

- $f_2(x|H_0) = \frac{1}{\sigma_2\sqrt{2\pi}} \cdot e^{-x^2/2\sigma_2^2}$ εάν ισχύει η υπόθεση H_0

ή

- $f_2(x|H_1) = \frac{1}{\sigma_2\sqrt{2\pi}} \cdot e^{-(x-\theta)^2/2\sigma_2^2}$ εάν ισχύει η υπόθεση H_1.

Υποθέτουμε ότι όλες οι παραπάνω παράμετροι είναι γνώστες εκτός από τα K_1 και K_1. Για να γίνουν γνωστά θα προσπαθήσουμε να λύσουμε το παρακάτω πρόβλημα βελτιστοποίησης:

$\min P_{FA}(K_1, K_2)$

subject to: $e_1 \cdot K_1 + e_2 \cdot K_2 \leq E$

,όπου Ε είναι ένα κατώφλι-περιορισμός στην κατανάλωση ενέργειας.

Για να μπορέσουμε να λύσουμε το παραπάνω πρόβλημα θα πρέπει να εκφράσουμε την πιθανότητα P_{FA} ως προς K_1 και K_1 ως εξής:

$P_{FA}(K_1, K_2) = P[\ln L(\underline{x}) > 0 | H_0]$.

$L(\underline{x}) = \frac{P_1(\underline{x})}{P_0(\underline{x})} = \frac{P(\underline{x}|H_1)}{P(\underline{x}|H_0)} = \frac{\prod_{i=1}^{K_1} f_1(x_i^{(1)}|H_1) \cdot \prod_{i=1}^{K_2} f_2(x_i^{(2)}|H_1)}{\prod_{i=1}^{K_1} f_1(x_i^{(1)}|H_0) \cdot \prod_{i=1}^{K_2} f_2(x_i^{(2)}|H_0)}$

Επίσης,

$\ln L(\underline{x}) = -\sum_{i=1}^{K_1} \frac{(x_i^{(1)}-\theta)^2}{\sigma_1^2} - \sum_{i=1}^{K_2} \frac{(x_i^{(2)}-\theta)^2}{\sigma_2^2} + \sum_{i=1}^{K_1} \frac{(x_i^{(1)})^2}{\sigma_1^2} + \sum_{i=1}^{K_2} \frac{(x_i^{(2)})^2}{\sigma_2^2} =$
$\frac{2\theta}{\sigma_1^2} \sum_{i=1}^{K_1} x_i^{(1)} + \frac{2\theta}{\sigma_2^2} \sum_{i=1}^{K_2} x_i^{(2)} - \frac{K_1 \cdot \theta^2}{\sigma_1^2} - \frac{K_2 \cdot \theta^2}{\sigma_2^2}$

κι έτσι έχουμε:

$\ln L(\underline{x}) > 0 \Rightarrow \frac{2\theta}{\sigma_1^2} \sum_{i=1}^{K_1} x_i^{(1)} + \frac{2\theta}{\sigma_2^2} \sum_{i=1}^{K_2} x_i^{(2)} - \frac{K_1 \cdot \theta^2}{\sigma_1^2} - \frac{K_2 \cdot \theta^2}{\sigma_2^2} > 0$
$\Rightarrow \frac{2}{\sigma_1^2} \sum_{i=1}^{K_1} x_i^{(1)} - \frac{K_1 \cdot \theta}{\sigma_1^2} + \frac{2}{\sigma_2^2} \sum_{i=1}^{K_2} x_i^{(2)} - \frac{K_2 \cdot \theta}{\sigma_2^2} > 0$

Εφόσον ψάχνουμε την P_{FA}, όλα τα παραπάνω ισχύουν ύπο την υπόθεση H_0, κι έτσι η $\frac{2}{\sigma_1^2} \sum_{i=1}^{K_1} x_i^{(1)}$ αποτελεί μία Γκαουσιανή τυχαία μεταβλητή με μέση τιμή 0 και διασπορά $\frac{4K_1}{\sigma_1^2}$ ($\sim \mathrm{N}(0, \frac{4K_1}{\sigma_1^2})$) και η $\frac{2}{\sigma_2^2} \sum_{i=1}^{K_2} x_i^{(2)}$ αποτελεί μία Γκαουσιανή

τυχαία μεταβλητή με μέση τιμή 0 και διασπορά $\frac{4K_2}{\sigma_2^2}$ ($\sim$N$(0,\frac{4K_2}{\sigma_2^2})$). Επομένως, εάν θέσουμε ως Z=$\frac{2}{\sigma_1^2}\sum_{i=1}^{K_1} x_i^{(1)} + \frac{2}{\sigma_2^2}\sum_{i=1}^{K_2} x_i^{(2)}$, τότε η Z αποτελεί Γκαουσιανή τυχαία μεταβλητή με μέση τιμή m=0 και διασπορά $\sigma = \frac{4K_1}{\sigma_1^2} + \frac{4K_2}{\sigma_2^2}$ ($\sim$N$(0,\frac{4K_1}{\sigma_1^2} + \frac{4K_2}{\sigma_2^2})$).

Επομένως,

$$P_{FA}(K_1,K_2) = P[\ln L(\underline{x}) > 0|H_0] = P[\tfrac{2}{\sigma_1^2}\sum_{i=1}^{K_1} x_i^{(1)} + \tfrac{2}{\sigma_2^2}\sum_{i=1}^{K_2} x_i^{(2)} > \tfrac{K_1\cdot\theta}{\sigma_1^2} + \tfrac{K_2\cdot\theta}{\sigma_2^2}] = 1 - P[\tfrac{2}{\sigma_1^2}\sum_{i=1}^{K_1} x_i^{(1)} + \tfrac{2}{\sigma_2^2}\sum_{i=1}^{K_2} x_i^{(2)} < \tfrac{K_1\cdot\theta}{\sigma_1^2} + \tfrac{K_2\cdot\theta}{\sigma_2^2}]$$

Εάν θέσουμε $z_1 = \frac{K_1\cdot\theta}{\sigma_1^2} + \frac{K_2\cdot\theta}{\sigma_2^2}$ και ορίσουμε ως $F_Z(z)$ την cdf της τυχαίας μεταβλητής Z τότε έχουμε:

$$P_{FA}(K_1,K_2) = 1 - P[Z < z_1] = 1 - F_Z(z_1).$$

Επίσης, γνωρίζουμε ότι $F_X(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{(x-m)/\sigma} e^{-t^2/2}dt = \Phi(\frac{x-m}{\sigma})$ όπου $\Phi(x)$ είναι η cdf μιας Γκαουσιανής τυχαίας μεταβλητής με μέση τιμή m=0 και σ=1: $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt$, με παράγωγο $\varphi(x) = \frac{1}{\sqrt{2\pi}}e^{-x^2/2}$

Άρα: $P_{FA}(K_1,K_2) = 1 - \Phi(\frac{z_1}{\sigma})$

Για να λύσουμε το πρόβλημα βελτιστοποίησης ορίζουμε τη Lagrangian συνάρτηση $L(K_1,K_2) = P_{FA}(K_1,K_2) + \lambda(e_1\cdot K_1 + e_2\cdot K_2 - E) =$ $1 - \Phi(\frac{z_1}{\sigma}) + \lambda(e_1\cdot K_1 + e_2\cdot K_2 - E)$, όπου λ ο πολλαπλασιαστής Lagrange που αντιστοιχεί στον περιορισμό του προβλήματος.

Για να βρούμε τις τιμές των K_1, K_2 θέτουμε τις μερικές παραγώγους της Lagrangian συνάρτησης, ως προς K_1 και K_2, ίσες με το μηδέν:

$$\frac{\partial L}{\partial K_1} = \frac{\partial(1-\Phi(\frac{z_1}{\sigma})+\lambda(e_1\cdot K_1+e_2\cdot K_2-E))}{\partial K_1} = -\varphi(\frac{z_1}{\sigma})\cdot\frac{\partial(z_1/\sigma)}{\partial K_1}+\lambda\cdot e_1 =$$
$$= -\varphi(\frac{z_1}{\sigma})\cdot\frac{(\partial/\sigma_1^2)\cdot\sigma-4z_1/\sigma_1^2}{\sigma^2}+\lambda\cdot e_1 = 0$$

και

$$\frac{\partial L}{\partial K_2} = \frac{\partial(1-\Phi(\frac{z_1}{\sigma})+\lambda(e_1\cdot K_1+e_2\cdot K_2-E))}{\partial K_2} = -\varphi(\frac{z_1}{\sigma})\cdot\frac{\partial(z_1/\sigma)}{\partial K_2}+\lambda\cdot e_2 =$$
$$= -\varphi(\frac{z_1}{\sigma})\cdot\frac{(\partial/\sigma_2^2)\cdot\sigma-4z_1/\sigma_2^2}{\sigma^2}+\lambda\cdot e_2 = 0,$$

και λύνουμε το σύστημα των δύο εξισώσεων που προκύπτουν ως προς K_1 και K_2. Τέλος, αντικαθιστώντας τις εκφράσεις που βρίσκουμε για τις δύο μεταβλητές (οι οποίες περιέχουν το λ) στην εξίσωση του περιορισμού βρίσκουμε την τιμή του πολλαπλασιαστή Lagrange λ κι έτσι μπορούμε να βρούμε τις ακριβείς τιμές για τα K_1 και K_2.

ΣΥΝΟΨΗ

Σε αυτή την εργασία αναλύσαμε το πρόβλημα ανίχνευσης επιθέσεων σε ασύρματα δίκτυα. Προσπαθήσαμε να δώσουμε την δική μας εκδοχή στην επίλυση του προβλήματος με τη βοήθεια τριών νέων αλγορίθμων. Καθένας από αυτούς είχε ως στόχο να εκμεταλλευτεί με το δικό του τρόπο τη δυνατότητα χρήσης πολλών κόμβων-παρατηρητών έτσι ώστε να βελτιωθεί η απόδοση του συστήματος ανίχνευσης. Επίσης, μελετήσαμε διάφορα θέματα γύρω από αυτούς τους αλγορίθμους όπως π.χ. η επιλογή κατάλληλων παραμέτρων. Έπειτα, αναλύσαμε την απόδοση τους μέσω προσομοίωσης με τη βοήθεια του προγράμματος Matlab και τέλος, προσπαθήσαμε να επιλύσουμε ένα πρόβλημα γύρω από τον αριθμό των παρατηρήσεων που πρέπει να κάνει κάθε κόμβος έχοντας ως περιορισμό την ενέργεια που μπορεί να καταναλώσει κάθε κόμβος.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] M.Li, I. Koutsopoulos and R. Poovedran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks",IEEE INFOCOM, 2007.
http://www.ee.washington.edu/research/nsl/papers/infocom-2007.pdf

[2] S. Radosavac, J. S. Baras and I.Koutsopoulos, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks", 4th ACM Workshop on Wireless Security, Cologne, Germany, September 02, 2005.
http://www.isr.umd.edu/~baras/publications/papers/2005/RadosavacBK_2005.htm

[3] A.L. Toledo, Xiaodong Wang, "Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks", Telefonica Res., Barcelona, vol. 3, no. 3, pp. 347-358, Sept. 2008.
http://www.ieeexplore.ieee.org

[4]

[5] R. Viswanathan, P.K. Varshney, "Distributed detection with multiple sensors I. Fundamentals", Dept. of Electr. Eng., Southern Illinois Univ., Carbondale, IL, Proceedings of the IEEE, vol. 85, no. 1, pp. 54-63, Jan 1997.

[6] Anthony D. Wood and John A. Stankovic, "Denial of Service in Sensor Networks", Data Networks, Upper Saddle River, Prentice Hall, Inc, 1992.
http://www.cs.colorado.edu/ rhan/CSCI_7143_001_Fall_2002/Papers/Wood2002_DOS_SensorNets

[7] Pradeep Kyasanur and Nitin H. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks", dsn, pp.173, 2003 International Conference on Dependable Systems and Networks (DSN'03), 2003.
http://www2.computer.org/portal/web/csdl/doi/10.1109/DSN.2003.1209928

[8] Venugopal V. Veeravalli and Tamer Basar and H. Vincent Poor, " Minimax robust decentralized detection", IEEE Transactions on Information Theory, vol. 40, no. 1, pp. 35-40, 1994.
http://www.informatik.uni-trier.de/ ley/db/indices/a-tree/v/Veeravalli:Venugopal_V=.html

[9] S. Radosavac, J.S Baras, "Application of sequential detection schemes for obtaining performance bounds of greedy users in the IEEE 802.11 MAC", Univ. of Maryland, College

Park, Communications Magazine, IEEE, vol. 46, no. 2, pp. 148-154, February 2008.
http://www.ieeexplore.ieee.org

[10] Guofei Gu, Alvaro A. Cardenas, and Wenke Lee, "Principled Reasoning and Practical Applications of Alert Fusion in Intrusion Detection Systems.", In Proceedings of ACM Symposium on InformAction, Computer and Communications Security (ASIACCS'08), Tokyo, Japan, March 2008
http://faculty.cs.tamu.edu/guofei/pubs.htm

[11] G. Fellouris and G.V. Moustakides, "Asymptotically optimum tests for decentralized change detection", Proceedings 2008 International Workshop on Applied Probability, IWAP'2008, Compiegne, France, July 2008.
http://dsplab.ece.upatras.gr/moustaki/submitted.html

[12] G.V. Moustakides, "Decentralized CUSUM Change Detection", Dept. of Comput. and Commun. Eng., Univ. of Thessaly, Volos, Information Fusion, 2006 9th International Conference, pp. 1 – 6, July 2006.
http://portal.acm.org

[13] Bruno M. Jedynak, Sanjeev M. Khudanpur, "Maximum Likelihood Set for Estimating a Probability Mass Function", Neural Computation archive, MIT Press Cambridge, MA, USA, vol. 17 , no. 7 , pp. 1508 - 1530, (July 2005).
http://portal.acm.org

[14] A.L. Toledo and Xiaodong Wang, "A Robust Kolmogorov-Smirnov Detector for Misbehavior in IEEE 802.11 DCF", IEEE International Conference on Communications ICC 2007, Glasgow, UK.
http://www.ee.columbia.edu/~alberto/

[15] Alvaro A. Cardenas, Svetlana Radosavac and John S. Baras, "Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments".
http://ieeexplore.ieee.org