ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΕΞΕΛΙΞΕΙΣ ΣΤΑ ΔΙΚΤΥΑ PPDR

ΔΗΜΗΤΡΙΟΣ ΧΑΛΕΠΛΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
Επιβλέπων

ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

Λαμία, 2019

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

AMR (Adaptive Multi-Rate) Προσαρμοστικός πολλαπλός ρυθμός

FDMA (Frequency-division multiple access) Πολλαπλή Πρόσβαση Διαίρεσης Συχνότητας.

GSM (Global System for Mobile Communications) Παγκόσμιο σύστημα κινητών επικοινωνιών

GPRS (General Packet Radio Service) Γενική ραδιοφωνική υπηρεσία πακέτων

GPP (GeForce Partner Program) Σχέδιο σύμπραξης

GSMA (Global System for Mobile Communications) Ενεργοποιητές συστημάτων ομαδικής επικοινωνίας

IP (Internet Protocol address) Διεύθυνση πρωτοκόλλου ίντερνετ

ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) Διαλειτουργικότητα μεταξύ συστημάτων

LTE (Long Term Evolution) Δίκτυο μακροπρόθεσμης εξέλιξης

MELPe (Mixed-Excitation Linear Predictive enhanced) Προγνωστική μεικτή γραμμή διέγερσης

MIMO (multiple-input and multiple-output) Πολλαπλή είσοδος- πολλαπλή έξοδος

OFDM (orthogonal frequency-division multiplexing) ορθογώνια πολυπλεξία διαίρεση συχνότητας

OFDMA (Orthogonal frequency-division multiple access) Ορθογώνια πολλαπλή πρόσβαση με διαίρεση συχνότητας

PMR (Professional mobile radio) Επαγγελματική κινητή ραδιοφωνία

PPDR (Public Protection and Disaster Relief) δημόσιας προστασίας και ανακούφισης από καταστροφές

PTT (Push-to-talk) Μεταγωγέας ομιλίας

SACHH (Slow Associated Control Channel) βραδύ κανάλι επικοινωνίας

TDMA (Time-division multiple access) Χρονική κατανομή πολλαπλής πρόσβασης

TETRA (Terrestrial Trunked Radio) Πρότυπο Επίγειου ραδιοφωνικού σταθμού

TETRAPOL Πρότυπο Ψηφιακού επαγγελματικού ψηφιακού σταθμού

TMO (Trunked Mode Operation) Λειτουργία κατειλημμένης γραμμής

UMTS (Universal Mobile Telecommunications System) Παγκόσμιο σύστημα κινητών επικοινωνιών

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Σε γενικές γραμμές, οι χρήστες της δημόσιας προστασίας και ανακούφισης από καταστροφές PPDR (Public Protection and Disaster Relief) έχουν πρόσβαση σε φωνητικές υπηρεσίες στενής ζώνης, υψηλής ταχύτητας αποστολής καθώς και σε δίκτυα δεδομένων κινητής τηλεφωνίας. Πρόσφατα, οι χρήστες PPDR (Public Protection and Disaster Relief) εξέφρασαν κρίσιμες επιχειρησιακές απαιτήσεις για τις υπηρεσίες δεδομένων ευρείας ζώνης. Προκειμένου να αναπτυχθούν οι υφιστάμενες εθνικές υποδομές PPDR (Public Protection and Disaster Relief)για την υποστήριξη και των ευρυζωνικών δεδομένων, οι ρυθμιστικοί φορείς πρέπει να προσδιορίσουν το εναρμονισμένο φάσμα συχνοτήτων για επικοινωνίες ευρείας ζώνης PPDR (Public Protection and Disaster Relief).

Οι υπηρεσίες PPDR (Public Protection and Disaster Relief)παρέχονται από οργανισμούς προστασίας από φυσικές καταστροφές και κινδύνου καταστροφών, οι οποίοι είναι γνωστοί και ως «φορείς πρώτης αντίδρασης» και περιλαμβάνουν κυρίως τις αστυνομικές, πυροσβεστικές και ασθενοφόρες υπηρεσίες, την πολιτική άμυνα και τις βοηθητικές υπηρεσίες όπως τη στρατιωτική αναζήτηση και διάσωση. Οι εκδηλώσεις πολιτικής προστασίας είναι επεισόδια καθημερινής ζωής επιπέδου 1, όπως οδικά ατυχήματα, πυρκαγιές κατοικιών, επικίνδυνες καταστάσεις πλήθους, έγκλημα στο δρόμο κλπ., και εκδηλώσεις επιπέδου 2 όπως μεγάλες πυρκαγιές, απαγωγές κλπ. Συμβάντα επιπέδου 3 είναι φυσικές και ανθρωπογενείς καταστροφές ευρέως διαδεδομένου κοινωνικού κόστους που φτάνει σε μεγάλες καταστροφές.

Στη συγκεκριμένη εργασία πρόκειται να παρουσιαστούν τα δίκτυα PPDR (Public Protection and Disaster Relief)και οι εφαρμογές τους. Στο δεύτερο κεφάλαιο θα γίνει μια γενική παρουσίαση των δικτύων αυτών θα αναφερθεί σε ποιες περιπτώσεις μπορούν να χρησιμοποιηθούν και θα παρουσιαστούν οι τεχνολογίες τους.

Αναλυτική περιγραφή των τεχνολογιών που χρησιμοποιούνται στα δίκτυα PPDR (Public Protection and Disaster Relief)θα πραγματοποιηθεί στο κεφάλαιο 3 και συγκεκριμένα θα αναλυθούν οι τεχνολογίες TETRA (Terrestrial Trunked Radio), TETRAPOL ενώ η σύγχρονη τεχνολογία LTE (Long Term Evolution) θα παρουσιαστεί στο τέταρτο κεφάλαιο..

Στο πέμπτο κεφάλαιο θα αναφερθούν κάποια στοιχεία για την ασφάλεια των PPDR (Public Protection and Disaster Relief) δικτύων ενώ στο έκτο κεφάλαιο θα συνοψιστούν τα βασικά συμπεράσματα της εργασίας. Η συγκεκριμένη εργασία είναι βιβλιογραφική και αποσκοπεί στην δημιουργία ενός οδηγού για τα δίκτυα PPDR (Public Protection and Disaster Relief) και στην εξοικείωση με τη συγκεκριμένη τεχνολογία δικτύων.

ΚΕΦΑΛΑΙΟ 2

ΤΑ ΔΙΚΤΥΑ PPDR

Ο τομέας της δημόσιας προστασίας και ανακούφισης από τις καταστροφές (PPDR) φέρνει ουσιαστική αξία στην κοινωνία, δημιουργώντας ένα σταθερό και ασφαλές περιβάλλον για τη διατήρηση της δημόσιας τάξης και την προστασία της ζωής και των αξιών των πολιτών. Οι υπηρεσίες PPDR (Public Protection and Disaster Relief), όπως η επιβολή του νόμου, η πυρόσβεση, οι υπηρεσίες έκτακτης ανάγκης (EMS) και οι υπηρεσίες αποκατάστασης καταστροφών αποτελούν πυλώνες της κοινωνίας και η προστασία που διασφαλίζεται από τις υπηρεσίες PPDR (Public Protection and Disaster Relief) καλύπτει τους ανθρώπους, την ιδιοκτησία, το περιβάλλον και άλλες σχετικές αξίες για την κοινωνία. Αντιμετωπίζει ένα μεγάλο αριθμό απειλών τόσο φυσικών όσο και ανθρωπογενών. Ο τομέας PPDR (Public Protection and Disaster Relief) είναι για τα περισσότερα έθνη στενά συνδεδεμένος με τον δημόσιο τομέα της κοινωνίας, είτε άμεσα ως τμήμα της κυβερνητικής δομής είτε ως μια λειτουργία που ανατίθεται σε εξωτερικούς φορείς υπό αυστηρούς κανόνες και παρακολουθείται εντατικά από το συμβαλλόμενο υπουργείο ή τμήμα της κυβέρνησης. Τα ρυθμιστικά, οργανωτικά, επιχειρησιακά και τεχνικά στοιχεία που στηρίζουν την αποτελεσματική ετοιμότητα των PPDR (Public Protection and Disaster Relief)μπορούν να διαφέρουν σημαντικά από χώρα σε χώρα, ακόμη και μεταξύ περιφερειών ή δήμων σε χώρες όπου η τοπική ετοιμότητα μπορεί να είναι υπό την αιγίδα των περιφερειακών ή τοπικών δημόσιων αρχών (Report ITU M 2033).

Γενικά τα συστήματα PPDR (Public Protection and Disaster Relief)σχετίζονται με ειδικές υπηρεσίες ραδιοεπικοινωνίας που αποσκοπούν τόσο στην δημόσια προστασία όσο και στην αντιμετώπιση των καταστροφών. Οι ραδιοεπικοινωνίες που σχετίζονται με τη δημόσια προστασία χρησιμοποιούνται από τις δημόσιες υπηρεσίες και τους οργανισμούς που σχετίζονται με τη διατήρηση του νόμου και της τάξης την προστασία της ζωής και την ιδιοκτησία και τις καταστάσεις εκτάκτου ανάγκης. Από την άλλη μεριά οι ραδιοεπικοινωνίες για την αντιμετώπιση των καταστροφών χρησιμοποιούνται από τις αρχές και τους οργανισμούς που καλούνται να αντιμετωπίσουν σοβαρές καταστροφές που μπορεί να επηρεάσουν σημαντικά την κοινωνία απειλώντας την ανθρώπινη ζωή την υγεία και το περιβάλλον (Report ITU M 2033).

Μια συνηθισμένη ταξινόμηση των συστημάτων PPDR (Public Protection and Disaster Relief) γίνεται με βάση τα επιτυγχανόμενα bit σε συστήματα στενής ζώνης (narrowband), ευρείας ζώνης (wideband) και ευρυζωνικά (broadband). Στο κεφάλαιο αυτό παρουσιάζονται οι γενικές απαιτήσεις του δικτύου PPDR (Public Protection and Disaster Relief) καθώς και τα πρότυπα που χρησιμοποιούνται ευρέως σήμερα όπως τα TETRA (Terrestrial Trunked Radio), TETRAPOL.

2.1 Γενικές απαιτήσεις για τα συστήματα επικοινωνίας των PPDR (Public Protection and Disaster Relief)

Τα PPDR (Public Protection and Disaster Relief) είναι συστήματα που έχουν μοναδικές λειτουργικές παραμέτρους και για αυτό χρειάζονται πολλαπλές σύνθετες τεχνολογίες επικοινωνίας οι οποίες περιλαμβάνουν λύσεις επικοινωνίας που σε μερικές περιπτώσεις φαίνονται μόνο στα PPDR. Οι βασικές απαιτήσεις που πρέπει να καλύπτονται είναι (ETSI TR 102 181, 2008):

Δυνατότητες και απόδοση υπηρεσιών: Οι βασικές λειτουργίες των συστημάτων PPDR (Public Protection and Disaster Relief) είναι οι λειτουργίες PTT (Push-to-talk), οι εκπομπές και ομαδικές επικοινωνίες και η άμεση λειτουργία ομιλίας για τις φωνητικές υπηρεσίες. Είναι πιθανό σε ορισμένα συστήματα να απαιτούνται επιπρόσθετα δεδομένα υπηρεσιών όπως και συμπληρωματικές υπηρεσίες όπως απόκριση του περιβάλλοντος, εξουσιοδότηση κλίσης, καθυστερημένη είσοδο και πολλά άλλα. Οι συγκεκριμένες υπηρεσίες απαιτούν γρήγορη απόκριση και μικρό βαθμό καθυστέρησης ενώ ο χρησιμοποιούμενος εξοπλισμός υποστηρίζει τις περισσότερες λειτουργίες όταν ο χρήστης είναι σε κίνηση. Επιπλέον μπορεί να απαιτείται υψηλής ποιότητας ήχος και εξαρτήματα όπως μικρόφωνα και μπαταρίες μεγάλης διάρκειας ζωής.

Αυστηρός έλεγχος συστημάτων επικοινωνίας: Αυτό το κομμάτι περιλαμβάνει την κεντρική αποστολή για το συντονισμό και τον έλεγχο των διάυλων επικοινωνίας των συστημάτων PPDR (Public Protection and Disaster Relief) μαζί με τη διαχείριση των τερματικών των συνδρομητών και των ομαδικών κλήσεων. Σε περίπτωση της συμφόρησης του συστήματος ο έλεγχος διασφαλίζει ότι αντιμετωπίζονται πρώτα οι σημαντικές κλήσεις. Οι υποστηριζόμενες προτεραιότητες απαιτείται να αντανακλούν μια συγκεκριμένη ιεραρχία όπως επίσης και μια λειτουργική κατάσταση που απαιτεί ειδική επεξεργασία των κλήσεων ανεξάρτητα από την ιεραρχία. Η ιεράρχηση μπορεί

να περιλαμβάνει προληπτικές κλήσεις επείγουσας ανάγκης παρακάμπτοντας αν χρειαστεί τις συνεχείς κλήσεις χαμηλής προτεραιότητας.

Απαιτήσεις που σχετίζονται με την ασφάλεια. Αποτελεσματικές και αξιόπιστες επικοινωνίες μέσα σε ένα σύστημα PPDR (Public Protection and Disaster Relief) ανάμεσα σε σχετικούς οργανισμούς που θα καλύπτουν την ανάγκη για πιστοποίηση συνδρομητή / δικτύου και υποστήριξη μηχανισμών κρυπτογράφησης και ακεραιότητας μέσω της διασύνδεσης ραδιοσυχνοτήτων και, σε ορισμένες περιπτώσεις, απαιτούν ακόμη και χρήση κρυπτογράφησης από άκρο σε άκρο (E2EE) μεταξύ των τερματικών του τελικού σημείου. Παρόλα αυτά, ενδέχεται να υπάρξουν περιπτώσεις στις οποίες οι διοικήσεις ή οι οργανισμοί, οι οποίοι χρειάζονται ασφαλείς επικοινωνίες, φέρουν συγκεκριμένο εξοπλισμό για να ανταποκριθούν στις δικές τους απαιτήσεις ασφάλειας. Επιπλέον, πρέπει να σημειωθεί ότι πολλές διοικήσεις έχουν κανονισμούς που περιορίζουν τη χρήση ασφαλών επικοινωνιών για την επίσκεψη σε χρήστες PPDR (Public Protection and Disaster Relief).

Κάλυψη: Το σύστημα PPDR (Public Protection and Disaster Relief)συνήθως απαιτείται να παρέχει πλήρη κάλυψη για κανονική κυκλοφορία εντός της σχετικής δικαιοδοσίας ή/ και λειτουργίας. Η κάλυψη απαιτείται για 24 h/ημέρα 365 ημέρες το χρόνο. Συνήθως τα συστήματα που υποστηρίζουν τα συστήματα PPDR (Public Protection and Disaster Relief) σχεδιάζονται για μέγιστα φορτία και ευρείες διακυμάνσεις στη χρήση τους. Πρόσθετοι πόροι που ενισχύουν την ικανότητα του συστήματος μπορούν να προστεθούν κατά τη διάρκεια ενός περιστατικού με τεχνικές όπως η αναδιάταξη δικτύων με εντατική χρήση άμεσων τρόπων και επαναλήπτες οχημάτων. οι οποίες μπορεί να απαιτούνται για κάλυψη τοπικών περιοχών. Τα συστήματα που υποστηρίζουν τα PPDR (Public Protection and Disaster Relief) επίσης απαιτούν να παρέχουν αξιόπιστα δεδομένα εισόδου και εξωτερική κάλυψη, κάλυψη στις απομακρυσμένες περιοχές και κάλυψη σε υπόγειες ή μη προσβάσιμες περιοχές. Οι απαιτήσεις κάλυψης μπορούν να καθοριστούν για παράδειγμα στο 99.5% στην εξωτερική κάλυψη και στο 65% στην εσωτερική κάλυψη. Τα συστήματα PPDR (Public Protection and Disaster Relief) δεν εγκαθίστανται στο εσωτερικό των κτηρίων. Οι οντότητες PPDR (Public Protection and Disaster Relief) δεν έχουν ένα συνεχές ρεύμα στην εγκατάσταση υποστήριξης και διατηρούν μιας ισχυρής πυκνότητας υποδομή. Τα αστικά συστήματα PPDR (Public Protection and Disaster

Relief) σχεδιάζονται για μεγάλη και αξιόπιστη κάλυψη των εξωτερικών σταθμών με περιορισμένη πρόσβαση εσωτερικά μέσω των τοιχωμάτων. Τα υποσυστήματα μπορεί να εγκατασταθούν σε ειδικά κτήρια ή δομές αν η διείσδυση μέσω των τοίχων είναι ανεπαρκής. Τα συστήματα PPDR (Public Protection and Disaster Relief) τείνουν να χρησιμοποιούν μεγαλύτερες κυψέλες ακτίνας και κινητές και προσωπικές μονάδες υψηλότερης ισχύος από τους παρόχους εμπορικών υπηρεσιών.

Χωρητικότητα: Τα πολύ χαμηλά επίπεδα αποκλεισμού των κλήσεων είναι απαραίτητη προϋπόθεση στα δίκτυα PPDR (Public Protection and Disaster Relief). Η χωρητικότητα του συστήματος πρέπει να είναι τέτοια ώστε να ικανοποιεί τη διαχείριση της προβλεπόμενης κίνησης και παράλληλα να είναι ευέλικτη στο λειτουργικό της σχεδιασμό για να υποστηρίζει επίσης την επικοινωνία κατά τη διάρκεια των ιδιαίτερων συνθηκών που υπερβαίνουν την αναμενόμενη κυκλοφορία, χρησιμοποιώντας μια μεγάλη ποικιλία εφαρμογών δεδομένων.

Υψηλά επίπεδα διαθεσιμότητας υπηρεσιών. Η διαθεσιμότητα της υπηρεσίας σχετίζεται με το χρονικό διάστημα στο οποίο μια υπηρεσία είναι σε λειτουργία. Η επίτευξη υψηλών επιπέδων διαθεσιμότητας υπηρεσιών απαιτεί πολλά επίπεδα πλεονασμού καθώς και ανθεκτικό εξοπλισμό.

Αναδιαμόρφωση συστήματος: Συνήθως στα συστήματα PPDR (Public Protection and Disaster Relief) απαιτείται μια δυναμική αναδιαμόρφωση που περιλαμβάνει ισχυρή λειτουργία διαχείριση και συντήρηση των συστημάτων.

Διασύνδεση: Ενώ τα συστήματα PPDR (Public Protection and Disaster Relief) κυρίως αποσκοπούν να παρέχουν ιδιωτικές εντός συστήματος επικοινωνίες, απαιτούν τα κατάλληλα συστήματα διασύνδεσης στα δημόσια δίκτυα τηλεπικοινωνιών. Η απόφαση σχετικά με το επίπεδο διασύνδεσης πρέπει να βασίζεται στις ειδικές λειτουργικές παραμέτρους των PPDR (Public Protection and Disaster Relief)όπως επίσης σε αυτή βασίζεται και η πρόσβαση στα δίκτυα δημόσιων τηλεπικοινωνιών.

Χρήση και διαχείριση φάσματος: Ανάλογα με τις εθνικές συχνότητες οι χρήστες των PPDR (Public Protection and Disaster Relief) πρέπει να μοιράζονται μεταξύ τους κάποιες από τις εφαρμογές τους. Οι λεπτομέρειες της διευθέτησης των δικτύων εξαρτάται από το μερίδιο φάσματος και διαφέρει από χώρα σε χώρα σε χώρα. Στην ίδια γεωγραφική περιοχή μπορεί να υπάρχουν διαφορετικά συστήματα που

υποστηρίζουν PPDR (Public Protection and Disaster Relief) και η παρεμβολή ανάμεσα σε αυτά τα συστήματα και τα συστήματα που δεν υποστηρίζουν τα PPDR (Public Protection and Disaster Relief) ελαχιστοποιούνται όσο το δυνατόν περισσότερο. Ανάλογα με την νομοθεσία τα συστήματα που υποστηρίζουν τα PPDR (Public Protection and Disaster Relief) μπορεί να χρησιμοποιούν ειδικούς διαύλους ανάμεσα στις συχνότητες σταθερής και κινητής βάσης.

Απαιτήσεις σχετικές με το κόστος: Οι λύσεις αποτελεσματικού κόστους και οι εφαρμογές είναι εξαιρετικά σημαντικές στους χρήστες PPDR (Public Protection and Disaster Relief). Η δημιουργία δικτύων PPDR (Public Protection and Disaster Relief) απαιτεί συνήθως την επένδυση μεγάλου κεφαλαίου και για αυτό είναι μακροπρόθεσμη επένδυση που υποστηρίζεται από ανοικτά πρότυπα, ανταγωνιστική αγορά και οικονομίες κλίμακας. Επιπλέον οι αποτελεσματικές λύσεις που χρησιμοποιούνται συνήθως μπορούν να μειώσουν το κόστος ολοκλήρωσης σε σημαντικό βαθμό.

2.2 Τεχνολογίες που χρησιμοποιούνται στα δίκτυα επικοινωνίας PPDR

Τα συστήματα PPDR (Public Protection and Disaster Relief) ταξινομούνται κατά κύριο λόγο με βάση το μέσο ρυθμό δεδομένων που μεταφέρεται σε κάθε σύστημα (Report ITU-R M.2033, 2003): σε δίκτυα περιορισμένης και ευρείας ζώνης και ευρυζωνικά δίκτυα.

Τα δίκτυα περιορισμένης ζώνης αναφέρονται σε τεχνολογίες που αποσκοπούν στη μεταφορά κεντρικών υπηρεσιών φωνής και εφαρμογές δεδομένων χαμηλής ταχύτητας. Οι τυπικοί ρυθμοί δεδομένων φτάνουν τα μερικές δεκάδες kilobits ανά δευτερόλεπτο και λειτουργούν σε κανάλια ραδιοσυχνότητας που φτάνουν τα 25kHz. Σήμερα στα δίκτυα περιορισμένης ζώνης χρησιμοποιούνται ψηφιακές τεχνολογίες όπως η TETRA (Terrestrial Trunked Radio) και η TETRAPOL τα οποία χρησιμοποιούνται και για την ευρεία κάλυψη δικτύων.

Τα δίκτυα ευρείας ζώνης αναφέρονται σε τεχνολογίες που μπορεί να μεταφέρουν ρυθμούς δεδομένων μερικών εκατοντάδων kilobits ανά δευτερόλεπτο. Τα συστήματα για εφαρμογές ευρείας ζώνης που υποστηρίζουν PPDR (Public Protection and Disaster Relief)βρίσκονται υπό ανάπτυξη σε διάφορους πρότυπους οργανισμούς. Η

πιο συνηθισμένη τεχνολογία είναι το TETRA (Terrestrial Trunked Radio) που χρησιμοποιείται ευρέως στα PPDR (Public Protection and Disaster Relief). Παρόλα αυτά οι τεχνολογίες ευρείας ζώνης δεν θεωρούνται ικανοποιητικές για χρήση στα PPDR (Public Protection and Disaster Relief) και για αυτό προτιμούνται οι τεχνολογίες περιορισμένης ζώνης.

Η ευρυζωνικότητα αναφέρεται στις τεχνολογίες που ικανοποιούν το νέο επίπεδο λειτουργικότητας με επιπλέον χωρητικότητα για να υποστηρίξουν τις επικοινωνίες δεδομένων υψηλής ταχύτητας σε σχέση με τις τεχνολογίες ευρείας ζώνης και περιλαμβάνουν εφαρμογές όπως η μετάδοση βίντεο υψηλής ανάλυσης. Αρχικά το δίκτυο ευρυζωνικότητας αποσκοπούσε στη λειτουργία των συστημάτων PPDR (Public Protection and Disaster Relief) σε τοπικές περιοχές παρέχοντας ενδεικτικούς ρυθμούς δεδομένων της τάξης των διαφόρων megabits ανά δευτερόλεπτο. Τα διάφορα τοπικά σενάρια άνοιξαν διάφορες πιθανότητες εφαρμογών PPDR (Public Protection and Disaster Relief) όπως προσαρμοσμένα δίκτυα περιοχής, ανάπτυξη hot spot και δίκτυα ad hoc. Από την άποψη αυτή, είναι ήδη διαθέσιμα εξειδικευμένα μέσα επικοινωνίας, όπως εξοπλισμός τακτικής δικτύωσης που προορίζεται για την κάλυψη των αναγκών των ανταποκριτών του PPDR (Public Protection and Disaster Relief), αν και η υιοθέτησή τους από τους επαγγελματίες του PPDR (Public Protection and Disaster Relief) είναι πολύ περιορισμένη. Αυτά τα συστήματα επικοινωνίας βασίζονται κατά κύριο λόγο στα ασύρματα δίκτυα wi-fi και λειτουργούν σε ανοικτές ζώνες των 2.4-5.8Hz (Elmarsy, 2012). `

ΚΕΦΑΛΑΙΟ 3

ΒΑΣΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΣΥΣΤΗΜΑΤΩΝ PPDR

3.1 TETRA

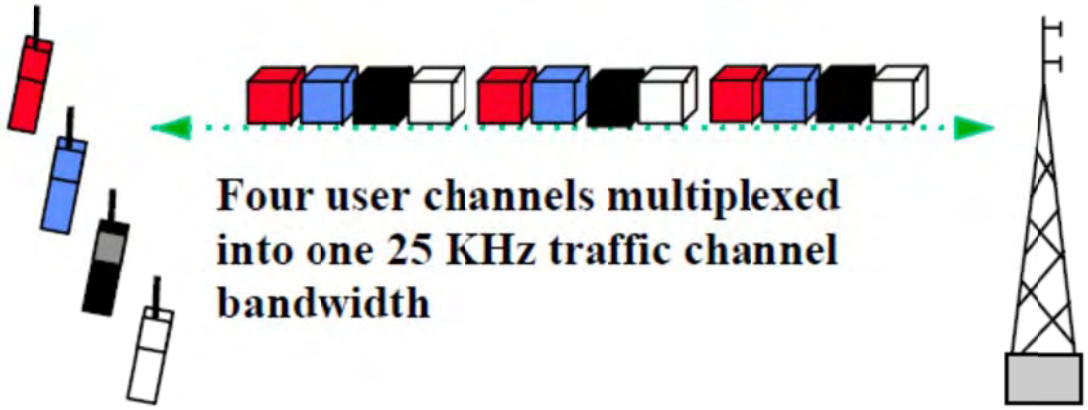
Η τεχνολογία TETRA (Terrestrial Trunked Radio) είναι μια υψηλής τεχνολογίας πλατφόρμα που παρέχει ολοκληρωμένες υπηρεσίες φωνής και δεδομένων. Η συγκεκριμένη τεχνολογία συνδυάζεται με εξωτερικές δυνατότητες σύνδεσης που συνθέτουν ένα υψηλό επίπεδο επαγγελματικής ραδιοτεχνολογίας (Et Industries 2017).

Το πρότυπο TETRA (Terrestrial Trunked Radio) αποτελεί ένα πρότυπο τηλεπικοινωνίας που χρησιμοποιείται για τα ιδιωτικά ραδιοδίκτυα PMR (Professional

mobile radio) που έχουν αναπτυχθεί και καλείται να καλύψει τις ανάγκες τις ανάγκες των χειριστών των ιδιωτικών ραδιοδικτύων που σχετίζονται με αυξημένη συσσώρευση δεδομένων και την αυξανόμενη ζήτηση δεδομένων και ομιλίας. Η ανάπτυξη της ψηφιακής τεχνολογίας έδειξε ένα τρόπο για την αντιμετώπιση των συγκεκριμένων ζητημάτων επιτρέποντας υψηλή απόδοση φάσματος και τη συνύπαρξη με τα αναλογικά συστήματα (Et Industries, 2017).

Τα ιδιωτικά ραδιοδίκτυα περιλαμβάνουν πολλές διαστάσεις όπως την συχνότητα το εύρος κάλυψης κλπ. Το Διευρωπαϊκό τηλεκατευθυνόμενο ραδιοφωνικό σύστημα (Trans-European Trunked Radio System, TETRA) αποτελεί το πρώτο ψηφιακό ιδιωτικό ραδιοπρώτυπο κινητής τεχνολογίας. Το TETRA (Terrestrial Trunked Radio) διεύρυνε περισσότερο τη διεθνή αγορά των ιδιωτικών ραδιοδικτύων με τις ευρέως αρμονισμένες συχνότητες. Το Ινστιτούτο Ευρωπαϊκών προτύπων τηλεπικοινωνιών (European Telecommunications Standards Institute ,ETSI) που συνδέει τις δυνάμεις των χειριστών του δικτύου, τους εθνικούς διαχειριστές τους κατασκευαστές του εξοπλισμού και τους χρήστες είναι αυτό που καθορίζει το πρότυπο. Τα κύρια σημεία του προτύπου TETRA (Terrestrial Trunked Radio) έγιναν αποδεκτά από είκοσι δύο χώρες στο τέλος του 1995. Το πρότυπο αυτό τέθηκε υπό διαβούλευση για την αποδοχή του έτσι ώστε να μπορεί να εξασφαλίσει υψηλή ποιότητα συγκριτικά με την ανάπτυξη των κατάλληλων λύσεων (Et Industries 2017).

Το TETRA (Terrestrial Trunked Radio) αποτελεί ένα πλήρες ψηφιακό σύστημα που παρέχει καλής ποιότητας φωνητικές υπηρεσίες και χαμηλό ρυθμό σφάλματος για τα δεδομένα. Το TETRA (Terrestrial Trunked Radio) υποστηρίζει φωνητικές υπηρεσίες δεδομένα μεταβλητού κυκλώματος και υπηρεσίες ομαδοποιημένων δεδομένων ενώ, παρέχει επίσης μια μεγάλη επιλογή ρυθμών μεταφοράς δεδομένων και επιπέδων προστασίας σφάλματος. Η συγκεκριμένη τεχνολογία χρησιμοποιεί χρονική διαίρεση πολλαπλής πρόσβασης (Time-division multiple access, TDMA) με τέσσερα κανάλια χρήστη τα οποία συνδέονται σε ένα φορέα με 25kHz με αποτέλεσμα να έχει εξαιρετική απόδοση στο φάσμα συχνότητας (Et Industries, 2017). Στους σταθμούς βάσης επιτυγχάνεται αποταμίευση κόστους αφού χρειάζεται μια ραδιομονάδα για κάθε τέσσερις χρήστες καναλιών.



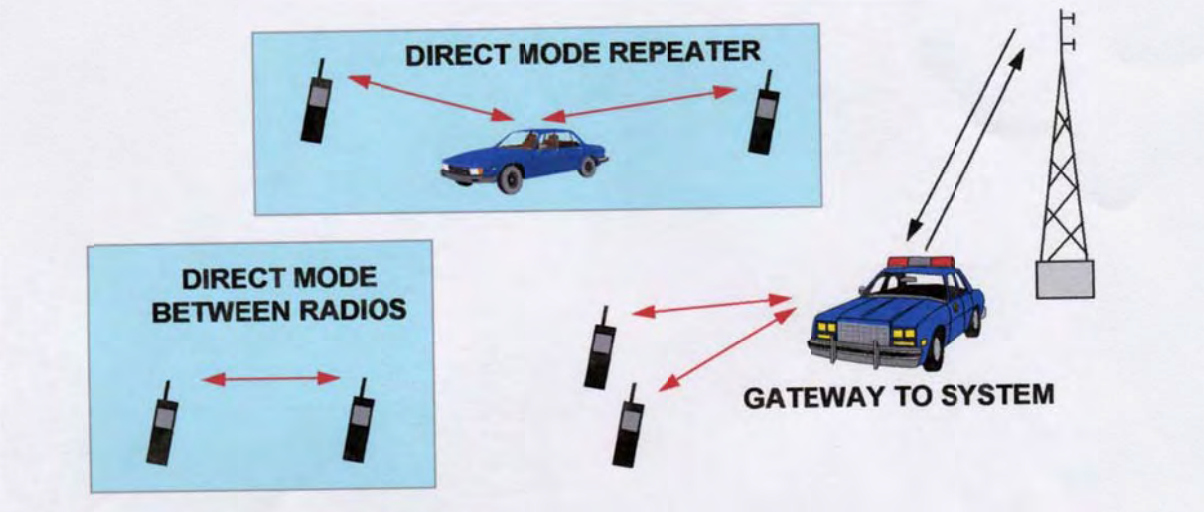
Σχήμα 3.1 Τεχνολογία TETRA (Et Industries, 2017).

Το TETRA (Terrestrial Trunked Radio) είναι σχεδιασμένο ως υπεραστικό σύστημα που υποστηρίζει λειτουργίες κοινής χρήσης του δικτύου αποτελεσματικά και οικονομικά διατηρώντας παράλληλα την ιδιωτικότητα και την κοινή ασφάλεια. Αποτελεί μια μεγάλης ασφάλειας τεχνολογία που περιλαμβάνει δυνατότητες κρυπτογράφησης φωνής δεδομένων και σήματος καθώς και της ταυτότητας των χρηστών. Η τεχνολογία TETRA (Terrestrial Trunked Radio) χρησιμοποιεί δύο μηχανισμούς κρυπτογράφησης την πεπλεγμένη και την από άκρη σε άκρη. Η πεπλεγμένη κωδικοποιεί τη ράδιο διαδρομή ανάμεσα στον τελικό σταθμό και στο σταθμό βάσης ενώ η από άκρη σε άκρη κρυπτογράφηση χρησιμοποιείται σε πιο κρίσιμες εφαρμογές όπου η κρυπτογράφηση απαιτείται για τη μετάδοση δεδομένων από το σύστημα σε έναν άλλο τερματικό σταθμό (Et Industries 2017). Η τεχνολογία TETRA (Terrestrial Trunked Radio) έχει πολύ γρήγορο χρόνο απόκρισης που είναι βασικό για τα συστήματα PPDR.

Το TETRA (Terrestrial Trunked Radio) έχει τέσσερις χρονικές θυρίδες ανά TDMA (Time-division multiple access) και διαμορφώνεται περαιτέρω σε 18 καρέ ανά πολυκάναλο. Κατά τη λειτουργία του κυκλώματος η κίνηση της φωνής και των δεδομένων από ένα χρονικό διάστημα 18 πλαισίων συμπιέζεται και μετατρέπεται σε 17 πλαισίων TDMA (Time-division multiple access) με αποτέλεσμα το 18^{o} πλαίσιο να χρησιμοποιείται για σηματοδότηση ελέγχου χωρίς να υπάρχει διακοπή των δεδομένων. Αυτό το 18^{o} πλαίσιο αποτελεί το πλαίσιο ελέγχου και παρέχει τη βάση για το βραδύ κανάλι ελέγχου SACHH (Slow Associated Control Channel) το οποίο παρέχει το υπόβαθρο για τον έλεγχο σηματοδότησης του καναλιού που υπάρχει

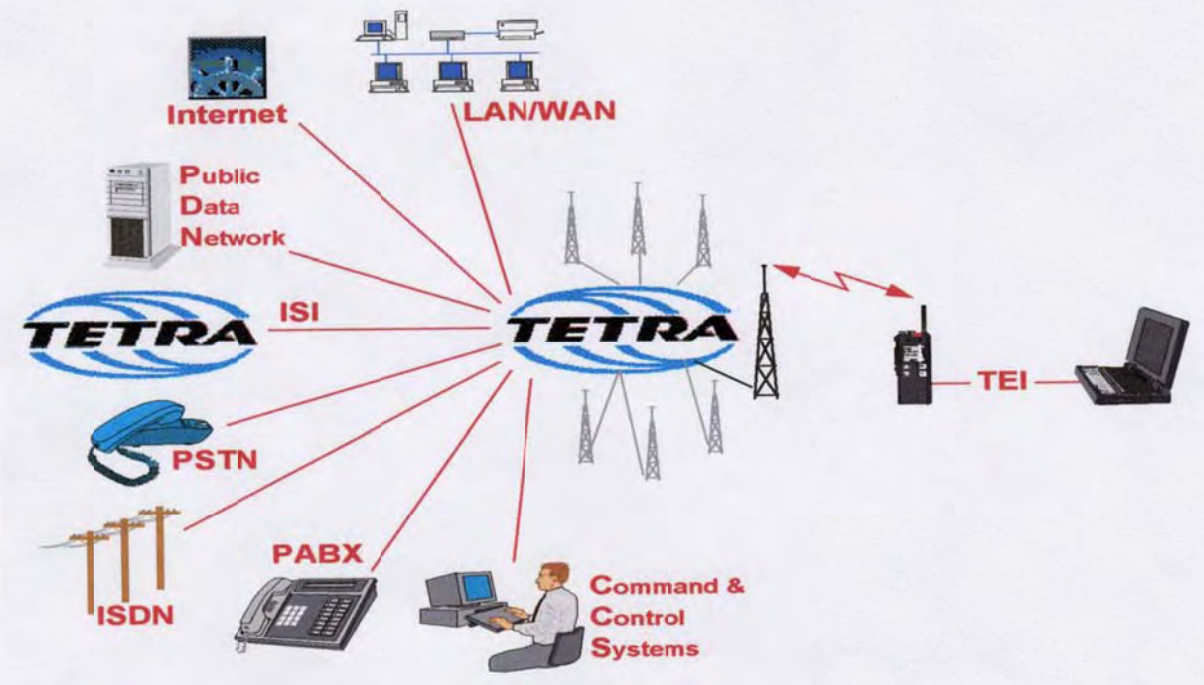
πάντα ακόμα και όταν όλα τα κανάλια λειτουργούν και αποτελεί το πιο ισχυρό χαρακτηριστικό του πρωτοκόλλου TETRA (Terrestrial Trunked Radio).

Το TETRA (Terrestrial Trunked Radio) χρησιμοποιεί την άμεση λειτουργία ανάμεσα στα ραδιοκινητά χωρίς να είναι απαραίτητη η ύπαρξη δικτύου ενώ οι λειτουργίες της πύλης και του επαναλήπτη επεκτείνουν την κάλυψη των χειροκίνητων ραδιοσυχνοτήτων τόσο στην άμεση λειτουργία όσο και στη λειτουργία δικτύου.



Σχήμα 3.2: Τρόποι λειτουργίας του TETRA

Τα δίκτυα TETRA (Terrestrial Trunked Radio) διευκολύνουν μια γκάμα συνδέσεων με εξωτερικά δίκτυα. Κατά συνέπεια μπορούν να συνδεθούν με δημόσια και ιδιωτικά τηλεφωνικά δίκτυα, με διαφορετικούς τύπους δικτύων δεδομένων καθώς και με μεγάλα συστήματα εντολών και ελέγχου. Όλα αυτά τα δίκτυα μπορούν να έχουν πρόσβαση από το κινητό τερματικό.



Σχήμα 3.3 Τρόποι σύνδεσης του TETRA (Terrestrial Trunked Radio) (Et Industries, 2017).

Το πρότυπο TETRA (Terrestrial Trunked Radio) ήταν το πρώτο σύστημα που έγινε γνωστό ως ανοικτό σύστημα για επαγγελματική ραδιοεπικοινωνία. Αναπτύχθηκε από το European Telecommunication Standard Institute (ETSI) σε συνεργασία με διάφορους οργανισμούς προκειμένου να εγκαθιδρύσει την καλή του λειτουργικότητα και γρήγορα υιοθετήθηκε σε όλον τον κόσμο. Οι προσπάθειες να προτυτοποιηθεί συνεχίζεται μέχρι σήμερα και έχουν προστεθεί καινούρια χαρακτηριστικά όπως είναι η πιθανότητα διασύνδεσης με πρότυπα κινητής τηλεπικοινωνίας όπως τα GSM (Global System for Mobile Communications), GPRS (General Packet Radio Service) και UMTS (Universal Mobile Telecommunications System).

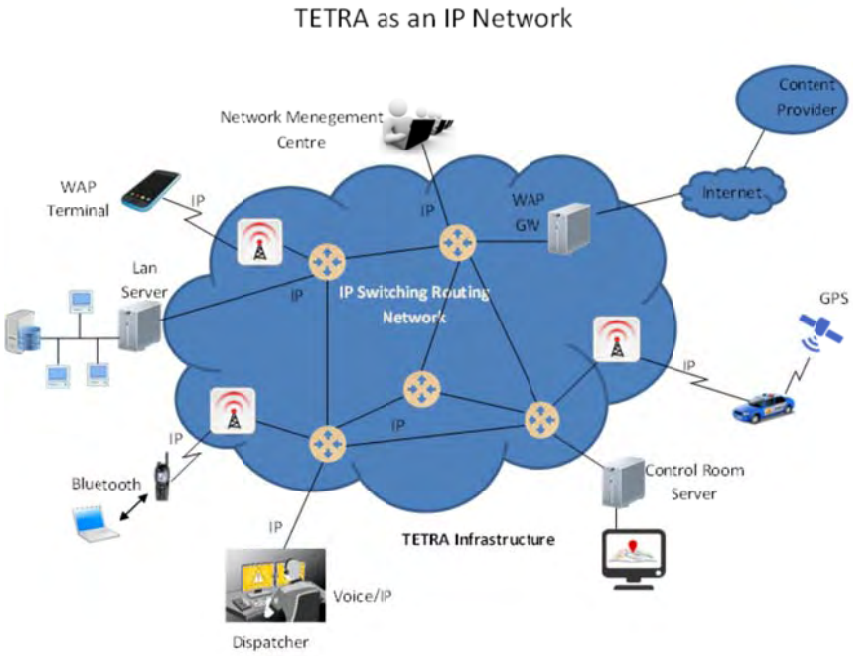
Η πρώτη έκδοση του συστήματος TETRA (Terrestrial Trunked Radio) παρείχε μια σειρά υπηρεσιών και δραστηριοτήτων αλλά οι αυξημένες απαιτήσεις των χρηστών οδήγησαν στην ανάπτυξη της τεχνολογίας. Οι αλλαγές στις ανάγκες της αγοράς οδήγησαν στην προτυτοποίηση της δεύτερης έκδοσης του προτύπου TETRA (Terrestrial Trunked Radio) στο οποίο περιλαμβάνονται (Bacra, 2017):

- Η επέκταση της κάλυψης TMO (Trunked Mode Operation) δηλαδή της λειτουργίας κατειλημμένης γραμμής

- Ο φωνητικός κωδικοποιητής AMR (Adaptive Multiple Rate)
- Ο προχωρημένος φωνητικός κωδικοποιητής (Predictive Mixed Excitation Liner) MELPe (Mixed-Excitation Linear Predictive enhanced) και
- Οι προηγμένες υπηρεσίες δεδομένων TEDS (Υπηρεσία εξυγίανσης δεδομένων TETRA).

Τα ραδιοφωνικά δίκτυα TETRA επιτρέπουν την επικάλυψη του TETRA (Terrestrial Trunked Radio) με IP (Internet Protocol) που πραγματοποιείται με την θύρα IP που είναι διαθέσιμη στα περισσότερα συστήματα TETRA. Αυτή η πύλη επιτρέπει στα δεδομένα και στα μυνήματα κατάστασης να ανταλλάσσονται μεταξύ του τερματικού σταθμού TETRA και μιας συσκευής που συνδέεται στην πύλη IP. Επιπλέον τα πακέτα δεδομένων που είναι διαθέσιμα σε ορισμένα από τα συστήματα TETRA επιτρέπουν μέσω του IP την ανταλλαγή δεδομένων ανάμεσα σε μια περιφερειακή συσκευή που είναι συνδεμένη στο TETRA και μια βασική εφαρμογή που περιέχει ο server μέσω Intranet (Pirnau and Botezatu 2016).

Μια εναλλακτική του TETRA με επικάλυψη IP είναι η χρήση ασύρματου πρωτοκόλλου εφαρμογής (WAP) στους τερματικούς σταθμούς. Η τοπολογία του δικτύου για το σύστημα TETRA με επικάλυψη IP είναι ιδιαίτερα ευέλικτη. Στην ουσία υποστηρίζεται οποιαδήποτε τοπολογία που περιλαμβάνει σύνδεση τύπου αστέρα, τοπολογία πλέγματος, τοπολογία δακτυλίου ή συνδυασμό τους. Η απαιτούμενη τοπολογία είναι απλά ζήτημα συνδέσμων και δρομολογητών (Bacra, 2017).



Σχήμα 3.4: Σύστημα TETRA (Terrestrial Trunked Radio) με επικάλυψη IP (Internet Protocol address) (Bacra, 2017).

Το TETRA (Terrestrial Trunked Radio) είναι ένα ανοικτό πρότυπο για την ψηφιακή PMR που δημιούργησε τα θεμέλια για αγορές με διάφορους παρόχους να εισάγουν προϊόντα TETRA (Terrestrial Trunked Radio) διαφόρων κατασκευαστών. Στόχος είναι να διασφαλιστεί ότι η διαλειτουργικότητα μπορεί να χρησιμοποιεί προϊόντα TETRA (Terrestrial Trunked Radio) - κυρίως τερματικά TETRA (Terrestrial Trunked Radio) - σε οποιοδήποτε δίκτυο από οποιονδήποτε πωλητή και να διευκολύνει τη ροή σημαντικών πληροφοριών. Αυτό θα βελτιώσει την επικαιρότητα και την ακρίβεια, μειώνοντας την απαραίτητη διάρκεια επικοινωνίας, περιορίζοντας τις πιθανές αιτίες διακοπής και μειώνοντας τον αριθμό των ατόμων που ενδέχεται να διαπράξουν σφάλματα.

Στην Ευρώπη η προτυποποίηση είναι η λέξη κλειδί για όλες σχεδόν τις διεθνείς δραστηριότητες που σχετίζονται με την ασφάλεια των δημόσιων επικοινωνιών. Σε διεθνές και τεχνικό επίπεδο υπάρχουν τα ακόλουθα τρία στοιχεία που λειτουργούν ως κίνητρο για την ανάπτυξη των τηλεπικοινωνιών (Bacra 2017):

- Η συνεργασία της αστυνομίας στα πλαίσια της συνθήκης της Σέγκεν
- Οι οργανισμοί προτυποποίησης και κυρίως το Ευρωπαϊκό Ινστιτούτο για τα πρότυπα τηλεπικοινωνιών (European Telecommunications Standards Institute ESTI) και
- Τα ινστιτούτα που υποστηρίζουν τα ευρωπαϊκά πρότυπα όπως το TETRA (Terrestrial Trunked Radio) MoY

Η διαλειτουργικότητα μεταξύ των εμπόρων των δικτύων και των τερματικών σταθμών είναι σημαντική στο πλαίσιο της δημιουργίας ενός μεγάλου κοινόχρηστου δικτύου και παράλληλα επιτρέπει την ευελιξία και τις τιμές των χρηστών των προϊόντων. Η διασφάλιση της διαλειτουργικότητας γίνεται μέσω δοκιμών που πραγματοποιούνται από ανεξάρτητο φορέα ο οποίος αποδίδει και τα σχετικά πιστοποιητικά σύμφωνα με όσα ορίζει το TETRA (Terrestrial Trunked Radio) MoU.

Οι πρώτοι χρήστες που εφάρμοσαν το TETRA (Terrestrial Trunked Radio) ήταν οι ευρωπαϊκές υπηρεσίες δημόσιας ασφάλειας και έκτακτης ανάγκης, δηλαδή η αστυνομία. & ο στρατός, οι αξιωματούχοι συνοριακών ελέγχων κλπ. Υπήρχαν

τεχνικοί και πολιτικοί λόγοι που ευνόησαν τη χρήση των συστημάτων. Τα υφιστάμενα δίκτυα δημόσιας ασφάλειας βρίσκονταν στο τέλος της οικονομικής ζωής τους και η TETRA παρέχοντας τα βασικά χαρακτηριστικά όπως η κρυπτογράφηση, ο άμεσος τρόπος λειτουργίας και ο χρόνος ρύθμισης της τελευταίας κλήσης για αυτές τις υπηρεσίες ήταν μια ελκυστική επιλογή για αυτές τις υπηρεσίες (Et Industries 2017).

Το συσσωρευτικό μέγεθος των υπηρεσιών εκτάκτου ανάγκης έχει περισσότερο από ένα εκατομμύριο χρήστες στην Ευρώπη. Οι περισσότερες δυτικοευρωπαϊκές χώρες έχουν λάβει την πολιτική απόφαση για την κοινή χρήση των TETRA (Terrestrial Trunked Radio) συστημάτων στις υπηρεσίες εκτάκτου ανάγκης. Τα σχέδια ολοκλήρωσης των συγκεκριμένων συστημάτων περιλαμβάνουν (Et Industries, 2017): 100.000 χρήστες της αστυνομίας και των ομάδων διάσωσης στο Ηνωμένο Βασίλειο, 400.000 χρήστες της αστυνομίας και των ομάδων διάσωσης στη Γερμανία, στη Φιλανδία 50.000 χρήστες από την αστυνομία την πυροσβεστική και άλλες υπηρεσίες καθώς και σε άλλες χώρες όπως η Αυστρία η Ελλάδα, η Ουγγαρία και η Πορτογαλία.

3.3 TETRAPOL

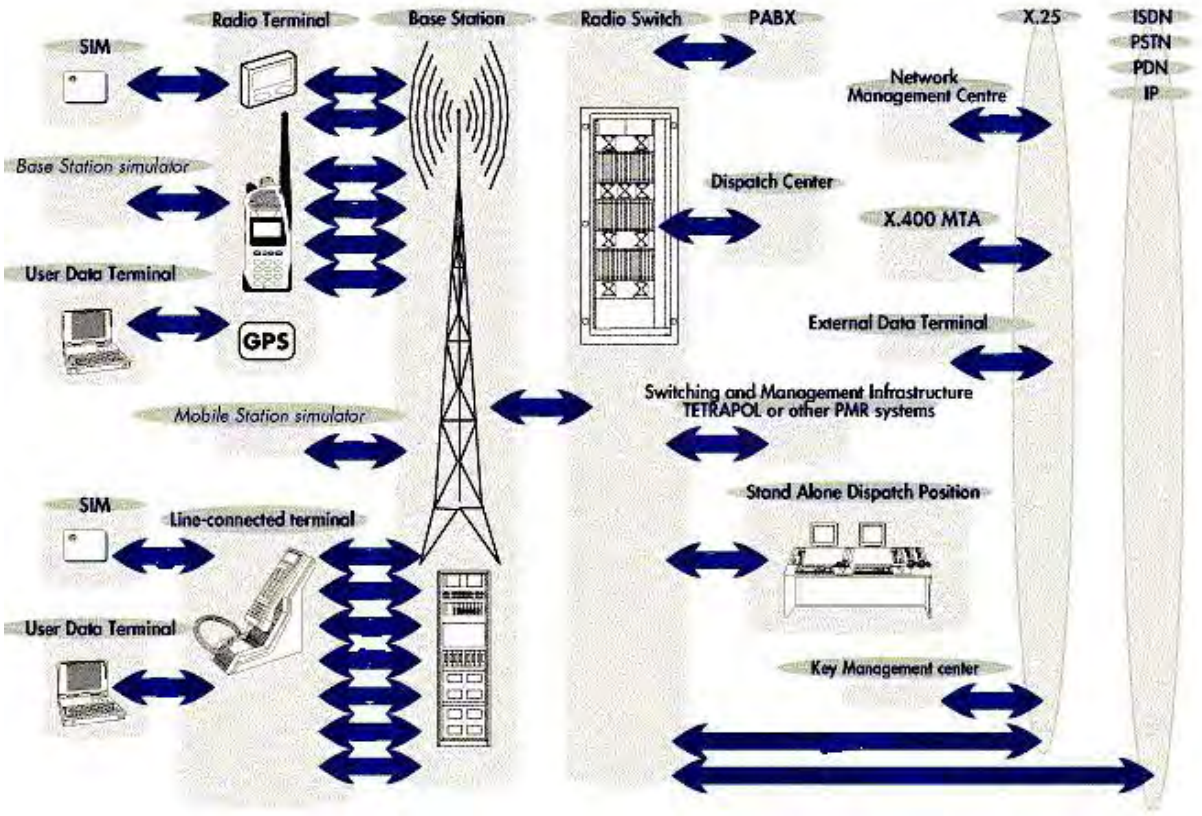
Το TETRAPOL είναι ένα ψηφιακό κυψελοειδές ραδιοφωνικό σύστημα για επικοινωνίες φωνής και δεδομένων. Αρχικά πρωτοεμφανίστηκε στην Γαλλία όπου χρησιμοποιήθηκε από την αστυνομία και τη χωροφυλακή και δημιουργήθηκε από τη Matra Communication ενώ σήμερα υποστηρίζεται από δύο ακόμα οργανισμούς το Tetrapol Forum που υποστηρίζεται κυρίως από κατασκευαστές και το Tetrapol´s user club (χρήστες οργανισμού) (OFCOM, 2015).

Τα ψηφιακά ραδιοσυστήματα είναι σύγχρονα ραδιοσυστήματα που χρησιμοποιούνται για ιδιωτικές και δημόσιες επαγγελματικές ραδιοεπικοινωνίες και για εφαρμογές ραδιοεπικοινωνιών έκτακτης ανάγκης PPDR (Public Protection and Disaster Relief). Σε αντίθεση με τα παλαιότερα συμβατικά αναλογικά συστήματα σταθερών καναλιών, στην περίπτωση ραδιοσυχνοτήτων, οι συχνότητες κατανέμονται δυναμικά σε μεμονωμένους χρήστες και υπηρεσίες. Είναι επομένως δυνατή η πλήρης αξιοποίηση του λεγόμενου κέρδους καναλιών και η αύξηση της απόδοσης του ραδιοφάσματος. Επιπλέον, η ποιότητα και η ασφάλεια των ραδιοσυστημάτων θα μπορούσε να βελτιωθεί σημαντικά χρησιμοποιώντας την ψηφιακή τεχνολογία. Τα ασύρματα ραδιοσυστήματα διαφέρουν από τα δημόσια

ραδιοσυστήματα όπως το GSM (Global System for Mobile Communications) ή το UTMS κυρίως όσον αφορά στην ταχύτερη ρύθμιση κλήσεων τις ομαδικές κλήσεις, τις κλήσεις προτεραιότητας την κρυπτογράφηση από άκρο σε άκρο και τη δυνατότητα απευθείας κλήσεων από κινητό σε κινητό σταθμό χωρίς καμία σύνδεση μέσω σταθμού βάσης.

Το Tetrapol αναπτύχθηκε κυρίως για το σημαντικό και προκλητικό τμήμα της αγοράς "έκτακτης ανάγκης ραδιοεπικοινωνιών". Η ανάπτυξη του Tetrapol ξεκίνησε το 1987 με βάση μια πρόσκληση υποβολής προσφορών από τη γαλλική χωροφυλακή για ένα εθνικό ψηφιακό ραδιοφωνικό σύστημα. Η επιλεγμένη μέθοδος πρόσβασης καναλιού ήταν FDMA (Frequency-division multiple access) (Πολλαπλή Πρόσβαση Διαίρεσης Συχνότητας). Το FDMA (Frequency-division multiple access) είναι η κλασική μέθοδος πρόσβασης καναλιού στην οποία κάθε χρήστης διαθέτει μια συγκεκριμένη συχνότητα για μια σύνδεση. Σε κάθε κύτταρο ένα κανάλι ελέγχου εκπέμπεται συνεχώς σε έναν συγκεκριμένο φορέα. Αυτό το κανάλι ελέγχου χρησιμοποιείται για τη μεταφορά των δεδομένων του δικτύου στον κινητό εξοπλισμό (OFCOM, 2015).

Το TETRAPOL μπορεί να χρησιμοποιηθεί σε συχνότητες μεταξύ 70 και 520 MHz αλλά στην πράξη χρησιμοποιούνται μόνο οι τυπικές συχνότητες στη ζώνη των 80, 160 και 400 MHz.



Σχήμα 3.4 Το δίκτυο TETRAPOL (www.tetrapol.org)

Το σύστημα Tetrapol συμμορφώνεται με τις απαιτήσεις PMR (Professional Mobile Radio) και εξασφαλίζει μια αποδοτική ραδιοφωνική κάλυψη και μείωση των δαπανών για τα μεγάλα δίκτυα, που εκτείνονται σε πυκνοκατοικημένες ή απρόσιτες περιοχές.

ΚΕΦΑΛΑΙΟ 4

ΕΞΕΛΙΞΕΙΣ ΣΤΑ ΔΙΚΤΥΑ PPDR

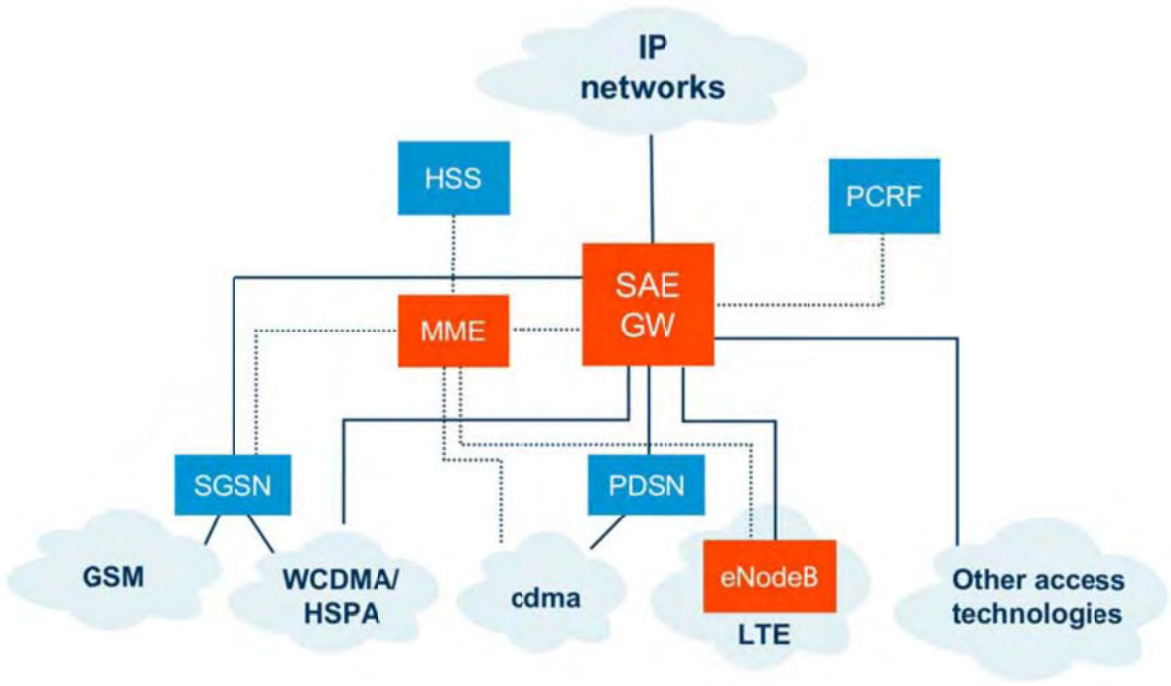
4.1 Το δίκτυο LTE (Long Term Evolution)

Το LTE (Long Term Evolution) είναι το επόμενης γενιάς βήμα στις ραδιοεπικοινωνίες και θα εισαχθεί στο πρόγραμμα συνεργασίας τρίτης γενιάς (3GPP). Το LTE (Long Term Evolution) χρησιμοποιεί την ορθογώνια πολυπλεξία διαίρεση συχνότητας (Orthogonal Frequency Division Multiplexing OFDM) ως τεχνολογία πρόσβασης μαζί με προηγμένες τεχνολογίες κεραίας. Το 3GPP είναι μια διεθνής συμφωνία συνεργασίας που υπογράφηκε το 1998 και φέρνει μαζί ως οργανωτικούς εταίρους ένα πλήθος διαφορετικών τεχνολογιών ραδιοεπικοινωνιών (Erricson 2007).

Τα βασικά χαρακτηριστικά της τεχνολογίας LTE (Long Term Evolution) είναι η επίπεδη αρχιτεκτονική (λίγα στοιχεία δικτύου), η βασισμένη σε IP (Internet Protocol address) βάση (επικοινωνίες που βασίζονται στο IP από άκρο σε άκρο) και η πολύ ευέλικτη προς τη χρήση του φάσματος (όσον αφορά το μέγεθος του καναλιού φάσματος και τη ζώνη φάσματος συχνοτήτων). Διαθέτει ανώτερη απόδοση ραδιοσυχνοτήτων και ευρυζωνικές δυνατότητες σε σύγκριση με τα προηγούμενα πρότυπα ραδιοεπικοινωνιών λόγω της χρήσης προηγμένων χαρακτηριστικών όπως OFDMA (Orthogonal frequency-division multiple access), MIMO (multiple-input and multiple-output), κωδικοποίηση turbo, 64QAM και 256QAM, συσσωμάτωση φορέα. Οι κορυφαίοι ρυθμοί θεωρητικών δεδομένων που μπορούν να επιτευχθούν με κοινά διαθέσιμες συσκευές σε φάσμα 20MHz FDD είναι 150Mbps (κατεύθυνση κατερχόμενης ζεύξης) και 50Mbps (κατεύθυνση ανερχόμενη ζεύξη). Οι προηγμένες συσκευές που χρησιμοποιούν περισσότερο φάσμα και περισσότερες δυνατότητες μπορούν να επιτύχουν πέρα από την προς τα κάτω σύνδεση (downlink) των 400Mbps και την ανερχόμενη ζεύξη 100 Mbps (Detecon).

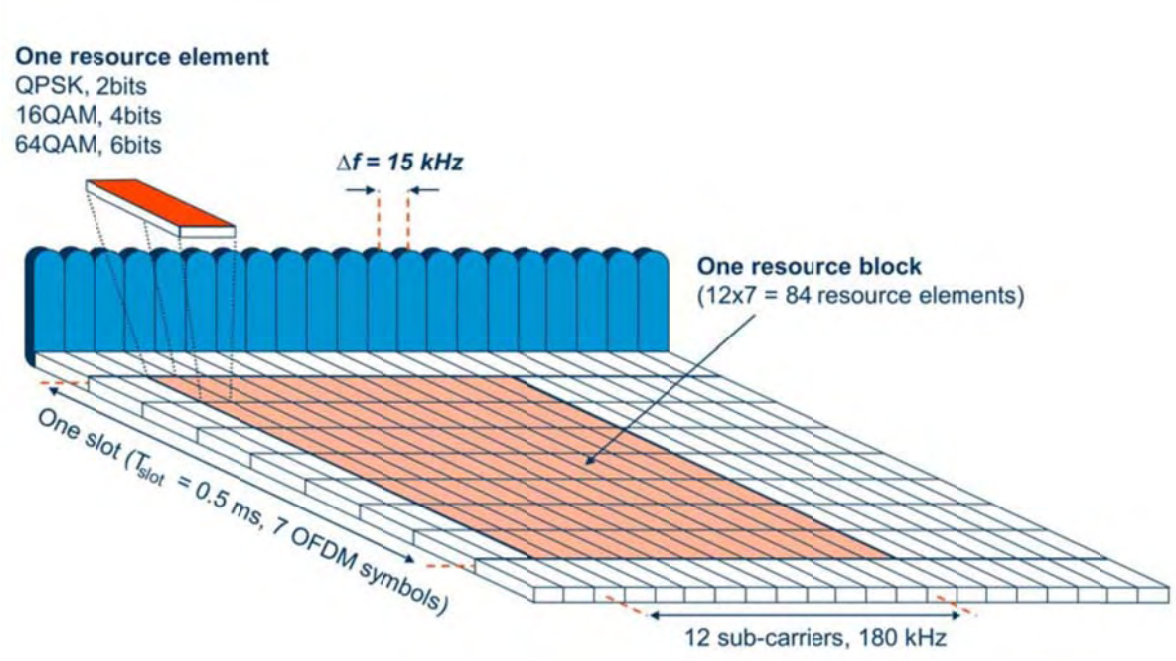
Παράλληλα με την ραδιοπρόσβαση LTE (Long Term Evolution) εξελίσσονται ταυτόχρονα τα δίκτυα των πυρηνικών πακέτων στην αρχιτεκτονική SAE η οποία είναι μια νέα αρχιτεκτονική που έχει σχεδιαστεί για τη βελτιστοποίηση της απόδοσης του δικτύου, τη βελτίωση της οικονομικής απόδοσης και τη διευκόλυνση της αγοράς των υπηρεσιών με βάση τη διεύθυνση IP (Erricson, 2007).

Στην αρχιτεκτονικής SAE υπάρχουν μόνο δύο κόμβοι, ο σταθμός βάσης LTE (Long Term Evolution) και η πύλη SAE. Οι σταθμοί βάσης LTE (Long Term Evolution) συνδέονται στο κεντρικό δίκτυο χρησιμοποιώντας τη διεπιφάνεια RAN S1- κεντρικού δικτύου. Η επίπεδη αρχιτεκτονική μειώνει τον αριθμό των κόμβων που περιλαμβάνονται στη σύνδεση.



Σχήμα 4.1 Αρχιτεκτονική του δικτύου LTE (Long Term Evolution) (Erricson 2007).

Το δίκτυο LTE (Long Term Evolution) χρησιμοποιεί για το downlink την OFDM (orthogonal frequency-division multiplexing) τεχνολογία και συνδέει το σταθμό βάσης με το τερματικό. Η OFDM (orthogonal frequency-division multiplexing) ραδιοτεχνολογία καλύπτει τις απαιτήσεις του LTE για ευελιξία φάσματος και προσδίδει οικονομικές λύσεις για ευρύ φάσμα φορέων με υψηλούς ρυθμούς. Η OFDM (orthogonal frequency-division multiplexing) χρησιμοποιεί μεγάλο αριθμό υποφορέων προκειμένου να μεταδίδονται δεδομένα μεταξύ πολλαπλών φορέων. Η βασική κατερχόμενη ζεύξη του LTE μπορεί να θεωρηθεί ως ένα πλέγμα χρονικής συχνότητας με το Δf στο εύρος συχνότητας να είναι 15kHz (Erricson, 2007).



Σχήμα 4.2 Η κατερχόμενη ζεύξη φυσικών πόρων του LTE (Long Term Evolution) με βάση την OFDM (orthogonal frequency-division multiplexing) (Erricson, 2007)

Τα OFDM (orthogonal frequency-division multiplexing) σύμβολα ομαδοποιούνται σε ομάδες πηγών με μέγεθος 180kHz στο εύρος συχνότητας και ανά 0.5ms στο χρονικό εύρος. Κάθε χρονικό διάστημα μετάδοσης 1ms αποτελείται από δύο υποδοχείς. Κάθε χρήστης διαθέτει μια ομάδα πόρων στο πλέγμα χρόνου- συχνότητας. Όσο περισσότερες ομάδες πόρων λαμβάνει ένας χρήστης και όσο μεγαλύτερη διαμόρφωση χρησιμοποιείται τόσο μεγαλύτερος είναι ο ρυθμός των bit.

Στην ανερχόμενη ζεύξη το LTE (Long Term Evolution) χρησιμοποιεί μια προ-κωδικοποιημένη έκδοση της OFDM (orthogonal frequency-division multiplexing) που ονομάζεται Πολλαπλή πρόσβαση διαιρεμένης συχνότητας απλού φορέα (SC-FDMA). Αυτό αντισταθμίζει το βασικό μειονέκτημα της κανονικής OFDM (orthogonal frequency-division multiplexing) που παρουσιάζει μεγάλο λόγο κορυφής προς μέση ισχύ (PARP) ο οποίος απαιτεί μεγάλο κόστος και είναι αναποτελεσματικός ενισχυτής ισχύος ενώ επιπλέον παρουσιάζει μεγάλες απαιτήσεις ευθυγράμμισης.

Ο αρχικός στόχος των εμπορικών φορέων ήταν να χρησιμοποιήσουν το LTE (Long Term Evolution) ως συμπληρωματικό δίκτυο δεδομένων υψηλής ταχύτητας δίπλα στα δίκτυα GSM (Global System for Mobile Communications) (2η γενιά) και UMTS (Universal Mobile Telecommunications System) (3ης γενιάς). Με στόχο την

αποτελεσματικότερη χρήση των δικτύων και την ελευθέρωση των πηγών ραδιοφάσματος, οι φορείς εκμετάλλευσης άρχισαν να εισάγουν ολόκληρη σειρά κινητών υπηρεσιών (φωνητικές και βιντεοκλήσεις, σύντομα μηνύματα, δεδομένα διαδικτύου) μέσω LTE (Long Term Evolution). Αυτό διευκολύνθηκε από την ανάπτυξη της πλατφόρμας IMS που χειριζόταν το στρώμα υπηρεσιών μέσω του επιπέδου συνδεσιμότητας IP (Internet Protocol address) που παρέχονταν από την ασύρματη πρόσβαση LTE (Long Term Evolution).

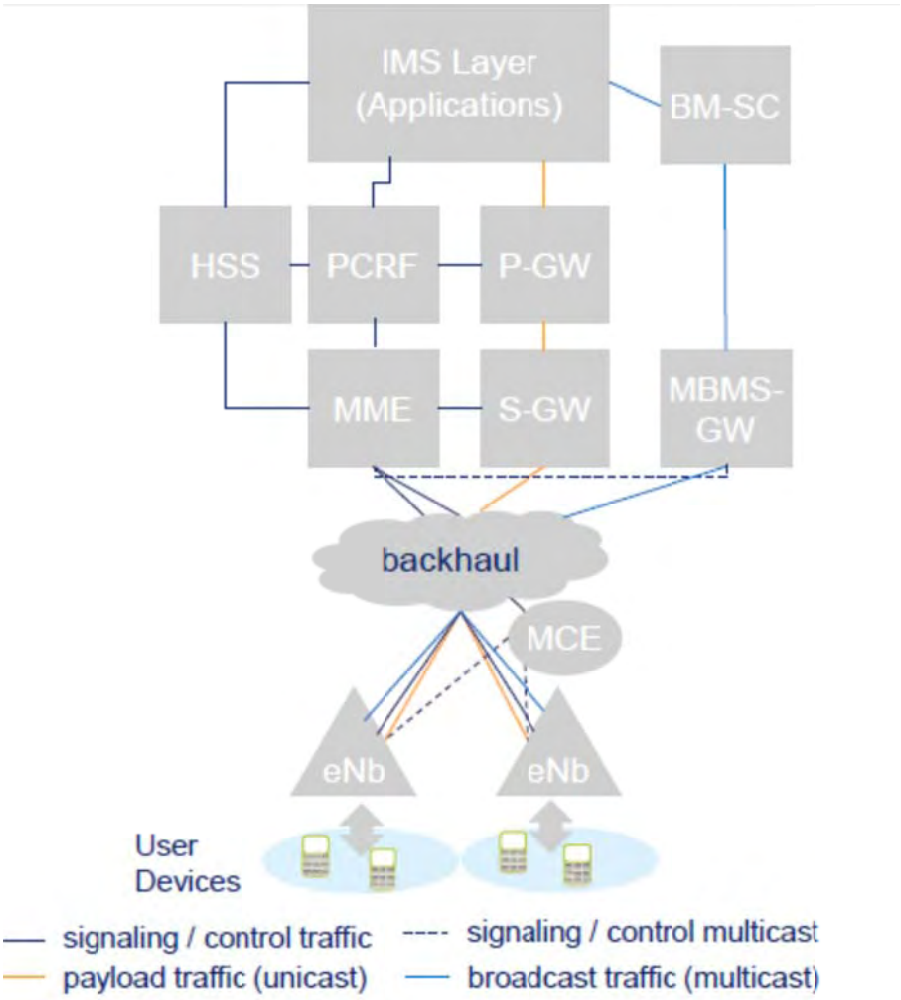
Όσον αφορά τα συστήματα PPDR το LTE (Long Term Evolution) δεν παρέχει το φάσμα υπηρεσιών του TETRA (Terrestrial Trunked Radio) αλλά το κενό αυτό γίνεται προσπάθεια να καλυφθεί. Συγκεκριμένα στο δίκτυο LTE (Long Term Evolution) βρίσκονται υπό ανάπτυξη οι ακόλουθες υπηρεσίες:

- Ομαδικές κλήσεις έκτακτης ανάγκης σε 300ms και μέγιστη καθυστέρηση λήξης έως 150ms (ETSI 122468)
- Ενεργοποιητές συστημάτων ομαδικής επικοινωνίας (Global System for Mobile Communications GSMA)
- Υπηρεσίες προσέγγισης
- Μεμονωμένη λειτουργία για τη δημόσια ασφάλεια (λειτουργία σε συγκεκριμένη περιοχή που είναι αποσυνδεμένη από το κεντρικό δίκτυο).
- Αποστολή κρίσιμων βίντεο και δεδομένων.

Το δίκτυο LTE (Long Term Evolution) μπορεί να λειτουργεί παράλληλα με τα υπάρχοντα δίκτυα (TETRA, TETRAPOL). Η διαλειτουργικότητα γίνεται σε δύο επίπεδα. Από τη μια στη στρώση εξυπηρέτησης μεταξύ των εφαρμογών της δημόσιας ασφαλείας LTE (Long Term Evolution) και από την άλλη στα δίκτυα PPDR (Public Protection and Disaster Relief) στενής ζώνης. Όσον αφορά στις συσκευές αυτές έχουν τη δυνατότητα να συνδεθούν και στα δύο δίκτυα. Σύμφωνα με τις προβλέψεις τα δίκτυα PPDR θα συνεχίσουν να υπάρχουν με την τωρινή τους μορφή μέχρι το 2025 (P3 TCCA , 2015).

Σε όρους συχνότητας φάσματος αναμένεται στην Ευρώπη να χρησιμοποιούνται ζώνες της τάξης του 1GHz. Προτείνεται πως θα υπάρχει μια ευέλικτη αρμονική συχνότητα που εστιάζει σε ζώνες των 400-700MHz. Η ζώνη των 400MHz χρησιμοποιείται ήδη για πλήθος υπηρεσιών επικοινωνίας και ιδιωτικών δικτύων. Η

διαθεσιμότητα των 10MHz είναι περιορισμένη. Τα 700MHz μέχρι τα 30MHz του φάσματος FDD αναμένεται να είναι διαθέσιμα στην Ευρώπη για εμπορική χρήση.



Σχήμα 4.3: Η αρχιτεκτονική δομή δικτύου LTE με PPDR (Public Protection and Disaster Relief) (DETECON)

ΚΕΦΑΛΑΙΟ 5

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ PPDR

Όπως ήδη έχει αναφερθεί οι περισσότερες ευρωπαϊκές χώρες χρησιμοποιούν τα δίκτυα PPDR (Public Protection and Disaster Relief) που βασίζονται κατά κύριο λόγο στις τεχνολογίες TETRA και TERTRAPOL για να καλύψουν τις ανάγκες των PPDR (Public Protection and Disaster Relief) συστημάτων σε εθνικό επίπεδο (Becchetti et al. 2013). Η χρήση ενός ενιαίου δικτύου PPDR σε εθνικό επίπεδο διευκολύνει τη συνεργασία μεταξύ των διαφόρων εθνικών φορέων PPDR (Public Protection and Disaster Relief) που μπορούν να διατεθούν με τις κατάλληλες ομάδες ομιλίας συντονισμού. Ωστόσο η διακρατική συνεργασία ανάμεσα στα συστήματα PPDR (Public Protection and Disaster Relief) των διαφόρων κρατών μελών της Ευρωπαϊκής Ένωσης δεν έχει ακόμα επιτευχθεί και αποτελεί έναν από τους βασικούς λόγους έλλειψης διασύνδεσης ανάμεσα στα εθνικά δίκτυα PPDR (Public Protection and Disaster Relief) στις διάφορες χώρες. Αυτή η έλλειψη διασύνδεσης αποτρέπει την υποστήριξη των υπηρεσιών περιαγωγής με αποτέλεσμα οι ομάδες PPDR (Public Protection and Disaster Relief) να μην μπορούν να διατηρήσουν την επικοινωνία τους όταν βρίσκονται σε ξένο έδαφος. Η ανάπτυξη του εγκλήματος σε διεθνές επίπεδο απαιτεί τη συνεργασία των δυνάμεων της αστυνομίας στις διάφορες περιοχές σε διασυνοριακό επίπεδο. Η ανάγκη για συνεργασία αυξάνεται με δεδομένες τις φυσικές καταστροφές που καταγράφονται την τελευταία δεκαετία και γενικά είναι επιτακτική ανάγκη η ανάπτυξη των συστημάτων πολιτικής προστασίας. Με δεδομένο ότι οι φυσικοί πόροι είναι περιορισμένοι και ο χρόνος πολύτιμος στην εκδήλωση φυσικών καταστροφών η διεθνής συνεργασία μεταξύ των μηχανισμών PPDR (Public Protection and Disaster Relief) μπορεί να είναι ιδιαίτερα αποτελεσματική.

Για την αποτελεσματική διασύνδεση των συστημάτων PPDR (Public Protection and Disaster Relief) σε διακρατικό επίπεδο απαιτούνται οικονομικοί πόροι και η αναγκαιότητα της είναι ήδη αναγνωρισμένη μέσα από τις διάφορες διεθνείς συνθήκες. Στη συνθήκη της Λισαβόνας αναγνωρίζεται πως η Ευρωπαϊκή Ένωση πρέπει να μετακινεί πόρους ανάμεσα στα κράτη μέλη της για την παροχή βοήθειας σε περίπτωση τρομοκρατικών επιθέσεων και φυσικών καταστροφών (Becheti, 2013).

Η απαίτηση για αξιόπιστες και αποτελεσματικές επικοινωνίες ανάμεσα στα συστήματα PPDR (Public Protection and Disaster Relief) είναι κοινή για τους οργανισμούς που οργανώνουν την αποτελεσματικότερη λειτουργία τους. Παρόλα αυτά ενδέχεται να υπάρξουν περιπτώσεις στις οποίες οι διοικήσεις ή οι οργανισμοί που χρειάζονται ασφαλείς επικοινωνίες φέρνουν εξοπλισμό για να ικανοποιήσουν τις δικές τους απαιτήσεις ασφαλείας. Επιπλέον πολλές διοικήσεις έχουν κανονισμούς που περιορίζουν τη χρήση ασφαλών επικοινωνιών στους περιστασιακούς χρήστες των PPDR (Public Protection and Disaster Relief) (ITU-R, 2015).

Τα ευρυζωνικά δίκτυα PPDR (Public Protection and Disaster Relief) μπορούν να δημιουργήσουν ένα ασφαλές περιβάλλον στο οποίο οι απαιτήσεις ασφαλείας συνοψίζονται στις ακόλουθες (ITU-R, 2015):

- Στην τεχνολογία κωδικοποίησης
- Την υποστήριξη των αλγορίθμων κωδικοποίησης
- Τον καθορισμό και την τοποθέτηση του χρήστη, την κωδικοποίηση της διεπιφάνειας του αέρα και την ολοκληρωμένη προστασία
- Την κωδικοποίηση από άκρο σε άκρο
- Την υποστήριξη για τη διαχείριση των τρίτων μερών
- Την πιστοποίηση του συστήματος διαχείρισης και
- Την ενημέρωση των βασικών στοιχείων (OTAR)

Επιπρόσθετα σε αυτές τις απαιτήσεις ασφαλείας του συστήματος υπάρχουν και προσιτές λειτουργίες που χρειάζεται να αναπτυχθούν για να ολοκληρωθούν τα απαιτούμενα επίπεδα ασφάλειας των πληροφοριών που διαπερνούν το δίκτυο.

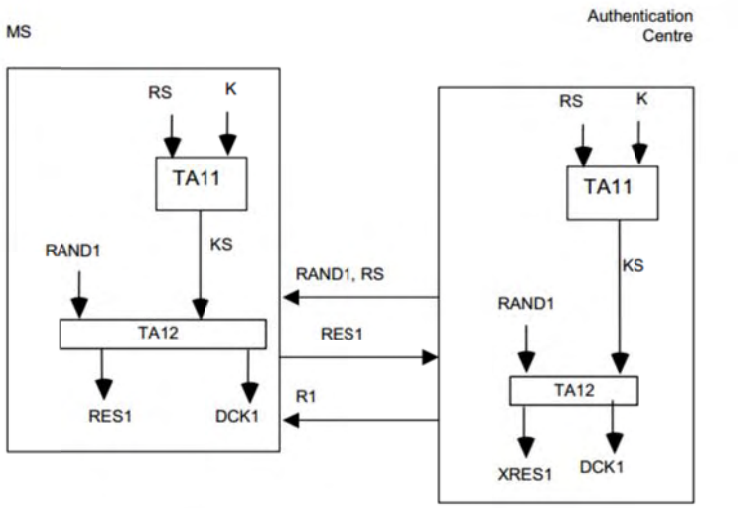
5.2 Ζητήματα ασφαλείας στα TETRA (Terrestrial Trunked Radio)

Η κύρια υπηρεσία ασφάλειας στο TETRA (Terrestrial Trunked Radio) είναι η βάση για κάθε μηχανισμό ασφάλειας έχει πολλές ομοιότητες με τον μηχανισμό ασφάλειας στα GSM (Global System for Mobile Communications) και βασίζεται στη γνώση ότι ένα μυστικό μοιράζεται μεταξύ του τερματικού σταθμού και του πιστοποιημένου κέντρου. Μετά από μια ρητή ανταλλαγή ελέγχου ταυτότητας, υπάρχει μια συνεχής σιωπηρή εξακρίβωση ταυτότητας ενός τερματικού, καθώς τα κλειδιά κρυπτογράφησης που στη συνέχεια χρησιμοποιούνται για την κρυπτογράφηση διεπαφής αέρα στην προς τα άνω ζεύξη συνδέονται με αυτή την αρχική ανταλλαγή ελέγχου ταυτότητας (Patkisson 2001). Στα συγκεκριμένα συστήματα ασφαλείας δεν

υπάρχει χρήση ούτε ασύμμετρης κρυπτογραφίας (δημόσιο κλειδί) ούτε ψηφιακών πιστοποιητικών.

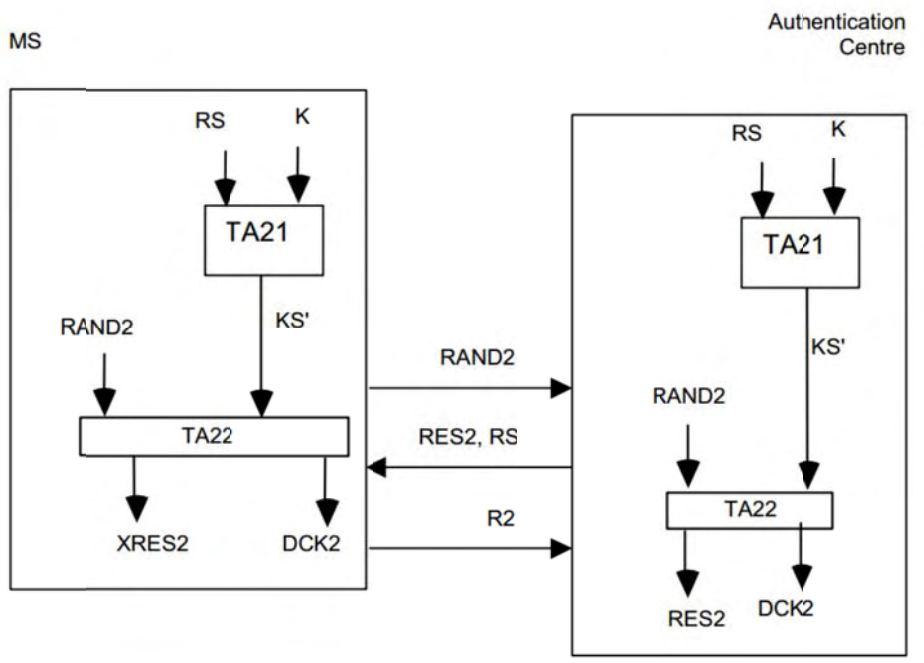
Ο έλεγχος ταυτότητας στα συστήματα TETRA (Terrestrial Trunked Radio) μπορεί να πραγματοποιηθεί σε τρία επίπεδα: στον έλεγχο ταυτότητας της υποδομής ενός κινητού σταθμού, στον έλεγχο ταυτότητας ενός κινητού σταθμού από την υποδομή και στον αμοιβαίο έλεγχο ταυτότητας. Σε κάθε περίπτωση πραγματοποιείται έλεγχος ταυτότητας από τους συμμετέχοντες που δείχνουν ο ένας στον άλλο πως γνωρίζουν το κοινό κλειδί που ήδη τους έχει μοιραστεί. Στη διαδικασία αναγνώρισης ταυτότητας συμμετέχουν οι κινητοί σταθμοί και οι υποδομές. Ο κινητός σταθμός αντιπροσωπεύει το χρήστη όπως αυτός ορίζεται στη μοναδική ταυτότητα του TETRA (Terrestrial Trunked Radio) ενώ οι υποδομές είναι πιο ευέλικτες στη διαδικασία με έναν αξιόπιστο σταθμό βάσης να αναπαριστά ένα κέντρο ταυτοποίησης. Οι γνώσεις που παρέχονται από το AuC κατά τη διάρκεια της ανταλλαγής ταυτότητας χρησιμεύουν επίσης ως κλειδί ελέγχου ταυτότητας τμήματος (KS). Το κλειδί ταυτότητας του κινητού σταθμού είναι ορατό μόνο στα όρια του κέντρου ταυτοποίησης. Τα κοινά κλειδιά παράγονται με αλγόριθμους πάνω στην διεπιφάνεια του αέρα και οι υποδομές είναι υπεύθυνες για την ολοκλήρωση της διαδικασίας. Η διαδικασία αναγνώρισης ταυτότητας είναι ένα πρωτόκολλο πρόκλησης- απόκρισης και η επιτυχής ολοκλήρωση της επιτρέπει την περαιτέρω ασφάλεια των λειτουργιών (ETSI EN 300 392-7).

Στην περίπτωση που η αναγνώριση ταυτότητας γίνεται από τις υποδομές το κέντρο ταυτοποίησης παράγει το κλειδί ταυτοποίησης το οποίο υπολογίζεται και από αλγόριθμο στον κινητό σταθμό. Από την υποδομή υπάρχει άλλος αλγόριθμος που υπολογίζει την απόκριση και επίσης παράγει ένα κλειδί κοινό. Μια τιμή στόχος παράγεται από την υποδομή στην οποία δίνει απόκριση ο σταθμός βάσης. Η διαδικασία αυτή ευθύνεται για την παραγωγή ενός τμήματος του μεταφερόμενου κοινού κλειδιού.



Σχήμα 5.1: Αναγνώριση ταυτότητας κινητού σταθμού στο TETRA (Terrestrial Trunked Radio) (ETSI EN 300 392-7)

Στην αναγνώριση της ταυτότητας από την υποδομή πραγματοποιείται η αντίστροφη διαδικασία. Η αρχική πρόκληση παράγεται από το κινητό σταθμό και η ισοδύναμη απόκριση υπολογίζεται από την πλευρά της υποδομής. Η όλη διαδικασία έχει ως αποτέλεσμα την παραγωγή του κοινού κλειδιού. Στη συνέχεια συγκρίνονται οι παραγόμενες τιμές με αυτές που υπολογίστηκαν στην αναγνώριση ταυτότητας στο σταθμό βάσης και αν συμφωνούν η αναγνώριση ταυτότητας είναι επιτυχής ενώ αν όχι η αναγνώριση ταυτότητας αποτυγχάνει. Το κλειδί αναγνώρισης ταυτότητας είναι το ίδιο όπως και στην προηγούμενη περίπτωση όμως διαφέρουν οι αλγόριθμοι που χρησιμοποιούνται.



Σχήμα 5.2 Αναγνώριση ταυτότητας από την υποδομή (ETSI EN 300 392-7)

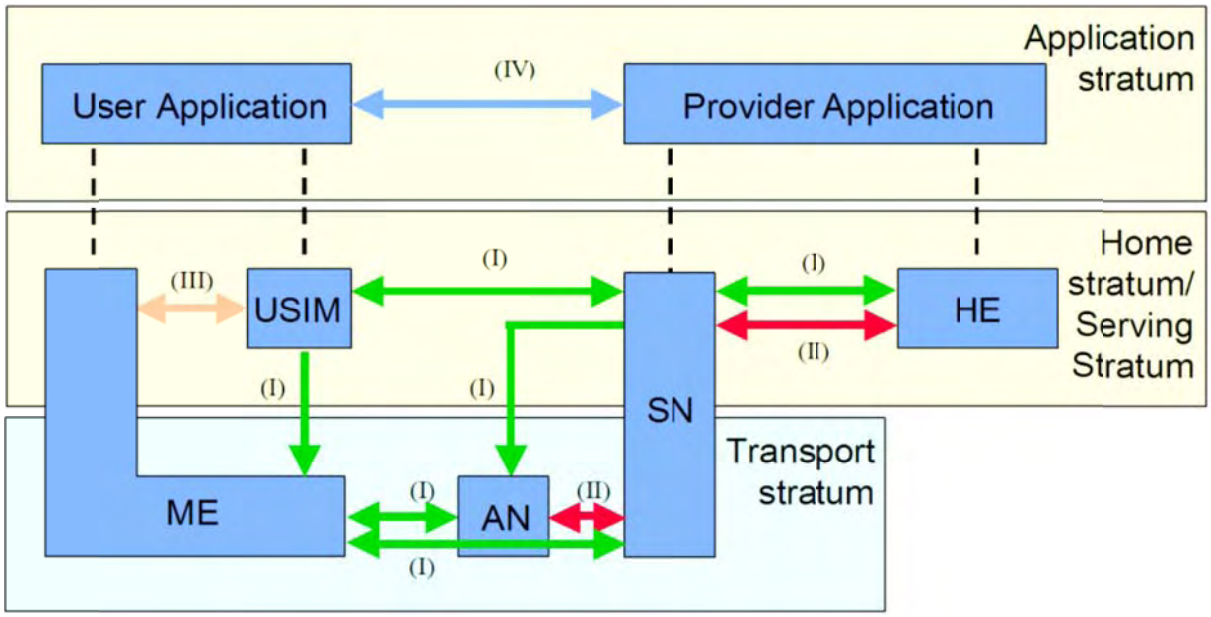
Αντίθετα με τις δύο προηγούμενες περιπτώσεις η κοινή αναγνώριση ταυτότητας πραγματοποιείται με μια διαδικασία τριων σταδίων με τους ίδιους αλγόριθμους και τα διαθέσιμα κλειδιά που ήδη αναφέρθηκαν

5.2 Ζητήματα ασφαλείας στα LTE

Τα δίκτυα LTE (Long Term Evolution), ευρέως γνωστά ως 4G, αποτελούν πρότυπο για τις ασύρματες επικοινωνίες υψηλής ταχύτητας, το οποίο αναπτύχθηκε από το 3GPP. Το LTE (Long Term Evolution) βασίζεται στις τεχνολογίες δικτύων GSM / EDGE και UMTS / HSPA προς ένα σύστημα από άκρη σε άκρη επιτυγχάνοντας αυξημένη χωρητικότητα και ταχύτητα χρησιμοποιώντας διαφορετική ραδιοφωνική διασύνδεση μαζί με τις βελτιώσεις του κεντρικού δικτύου.

Η πρώτη έκδοση του LTE (Long Term Evolution) αναπτύχθηκε υπό την προϋπόθεση ότι οι τελικοί συντελεστές κατερχόμενης ζεύξης των 150Mbit / s, οι ρυθμοί αιχμής ανερχόμενης ζεύξης 50Mbit / s και QoS προβλέπουν καθυστέρηση μεταφοράς μικρότερη από 10ms στο δίκτυο LTE (Long Term Evolution). Επί του παρόντος, το 3GPP λειτουργεί στις εκδόσεις 12 και 13 του προτύπου. Με αυξημένους ρυθμούς δεδομένων, βελτιωμένη αποδοτικότητα φάσματος και σύστημα βελτιστοποιημένο για πακέτα, η τεχνολογία LTE (Long Term Evolution) έχει ρυθμιστεί ώστε να λειτουργεί σε διαφορετικές τεχνολογίες συσκευών και σε εφαρμογές έντασης δεδομένων. Το

LTE (Long Term Evolution) τα τελευταία χρόνια έχει εισαχθεί στα συστήματα PPDR (Public Protection and Disaster Relief) και έχει συγκεκριμένες απαιτήσεις σχετικά με την ασφάλεια και την αξιοπιστία λόγω των ευαίσθητων πληροφοριών που μεταδίδονται σε αυτά τα δίκτυα.



Σχήμα 5.1: Αρχιτεκτονική ασφαλείας του LTE (3GPP TS 33.401 v12.10.0)

Η αρχιτεκτονική ασφαλείας του LTE (Long Term Evolution) διαιρείται σε πέντε διαφορετικές ομάδες ή τομείς η οποία διαίρεση διευκολύνει την περιγραφή των διαφόρων χαρακτηριστικών των πακέτων δεδομένων (EPS) δεδομένου ότι κάθε τομέας έχει τις δικές του απειλές ασφάλειας και κατά συνέπεια εφαρμόζονται μεμονωμένες λύσεις για κάθε τομέα. Οι βασικοί τομείς ασφαλείας είναι (Olsson et al 2012):

Ασφάλεια πρόσβασης στο δίκτυο (I): χαρακτηριστικά ασφαλείας που παρέχουν σε έναν χρήστη ασφαλή πρόσβαση στο EPS.

Ασφάλεια τομέα δικτύου (II): χαρακτηριστικά που επιτρέπουν σε διαφορετικούς κόμβους δικτύου να ανταλλάσσουν δεδομένα με ασφάλεια και να προστατεύονται από επιθέσεις στο δίκτυο μεταξύ των κόμβων

Ασφάλεια τομέα χρήστη (III): χαρακτηριστικά ασφαλείας που εξασφαλίζουν την πρόσβαση σε τερματικά, δηλ. Τη χρήση του Προσωπικού Αριθμού Αναγνώρισης (PIN).

Ασφάλεια τομέα εφαρμογών (IV): χαρακτηριστικά ασφάλειας που χρησιμοποιούνται από εφαρμογές όπως HTTP (για πρόσβαση στο διαδίκτυο) ή υποσυστήματα πολυμέσων IP (Internet Protocol address) (IMS).

Ορατότητα και δυνατότητα ρύθμισης της ασφάλειας: αυτό είναι το σύνολο χαρακτηριστικών που επιτρέπει στο χρήστη να μάθει εάν λειτουργεί ή όχι ένα χαρακτηριστικό ασφάλειας και αν η χρήση και η παροχή υπηρεσιών θα πρέπει να εξαρτάται από τη λειτουργία ασφαλείας.

Ο τομέας ασφάλειας πρόσβασης δικτύου εστιάζει στις λειτουργίες ασφαλείας που παρέχουν σε έναν χρήστη ασφαλή πρόσβαση στα EPS. Αυτές περιλαμβάνουν την αμοιβαία αναγνώριση της ταυτότητας καθώς και τα χαρακτηριστικά προστασίας των προσωπικών δεδομένων την προστασία κυκλοφορίας και την κυκλοφορία σε επίπεδα του χρήστη. Κατά συνέπεια στον τομέα πρόσβασης στο δίκτυο τα κύρια χαρακτηριστικά ασφάλειας είναι: η ανωνυμία του χρήστη, η ταυτοποίηση του χρήστη, η εμπιστευτικότητα των δεδομένων και η ολοκλήρωση των δεδομένων.

Το LTE (Long Term Evolution) περιέχει πολλές οντότητες δικτύου και σημεία αναφοράς μεταξύ αυτών των οντοτήτων. Η ασφάλεια στον τομέα δικτύου αναφέρεται στις δυνατότητες που επιτρέπουν στους κόμβους δικτύου να ανταλλάσσουν δεδομένα με ασφάλεια και να προστατεύονται από επιθέσεις στο δίκτυο μεταξύ των κόμβων. Η προστασία μεταξύ κόμβων δικτύου μπορεί να παρέχεται από το Network Domain Security για δίκτυα ελέγχου που βασίζονται στην IP (NDS / IP) (Olsson et al. 2012).

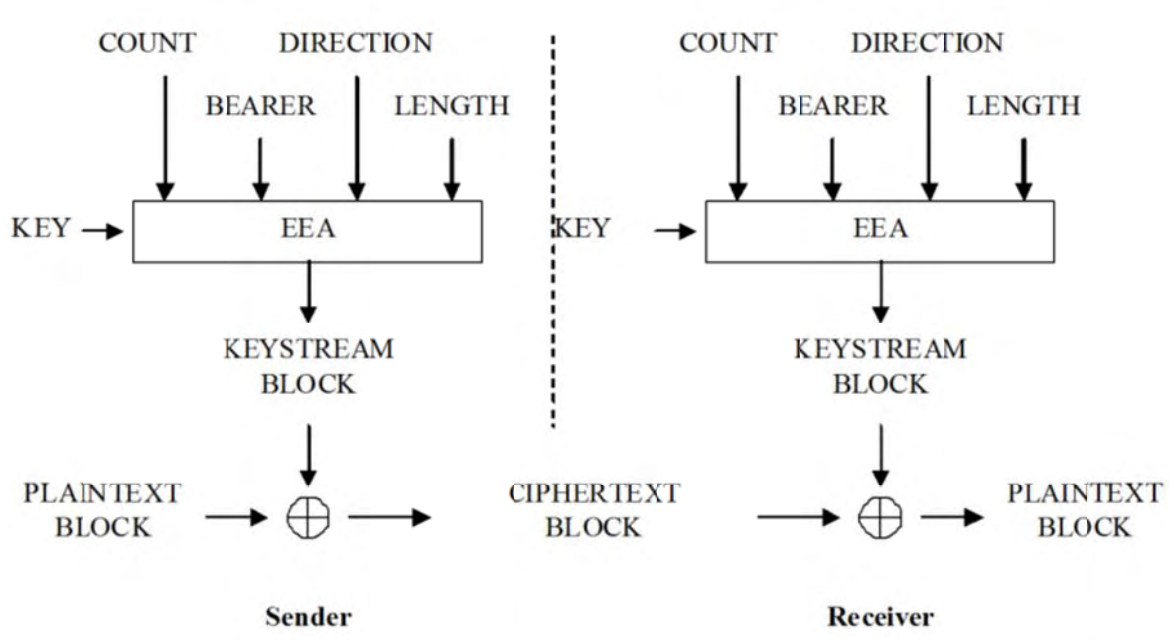
Στην ισχύουσα έκδοση του LTE (Long Term Evolution) ο τομέας ασφάλειας του χρήστη αναφέρεται στην ομάδα των ρυθμίσεων ασφαλείας που διασφαλίζουν ασφαλή πρόσβαση στους τερματικούς σταθμούς. Μέχρι τώρα το μόνο χαρακτηριστικό ασφαλείας του χρήστη είναι η χρήση προσωπικού κωδικού πρόσβασης (PIN) (Olsson et al. 2012).

Ο τομέας ασφάλειας εφαρμογών αποτελείται από τα χαρακτηριστικά ασφαλείας που χρησιμοποιούνται από τις εφαρμογές των συστημάτων. Ο συγκεκριμένος τομέας ασφάλειας εφαρμόζεται από άκρο σε άκρο στο δίκτυο και σχετίζεται με τον κωδικό ασφαλείας και έρχεται σε αντίθεση με τους προηγούμενους τομείς που η ασφάλεια εφαρμόζεται αποκλειστικά στο δίκτυο. Αν κάθε κρίκος της αλυσίδας του δικτύου είναι

ασφαλής τότε και η συνολική σύνδεση του συστήματος είναι ασφαλής (Olsson et al. 2012).

Η ορατότητα και η διαμορφωσιμότητα του δικτύου περιγράφεται ως μια ομάδα χαρακτηριστικών που επιτρέπει στο χρήστη να γνωρίζει αν ένα χαρακτηριστικό ασφαλείας είναι σε λειτουργία ή όχι και αν η χρήση και η παροχή υπηρεσιών υπόκειται σε χαρακτηριστικά ασφαλείας. Στις περισσότερες περιπτώσεις τα χαρακτηριστικά ασφαλείας είναι διαφανή ως προς το χρήστη και ο χρήστης αμφιβάλλει ότι η ασφάλεια είναι ενεργή. Ο χρήστης μπορεί να είναι ενήμερος για κάποια χαρακτηριστικά ασφαλείας που είναι ενεργοποιημένα (Olsson et al. 2012).

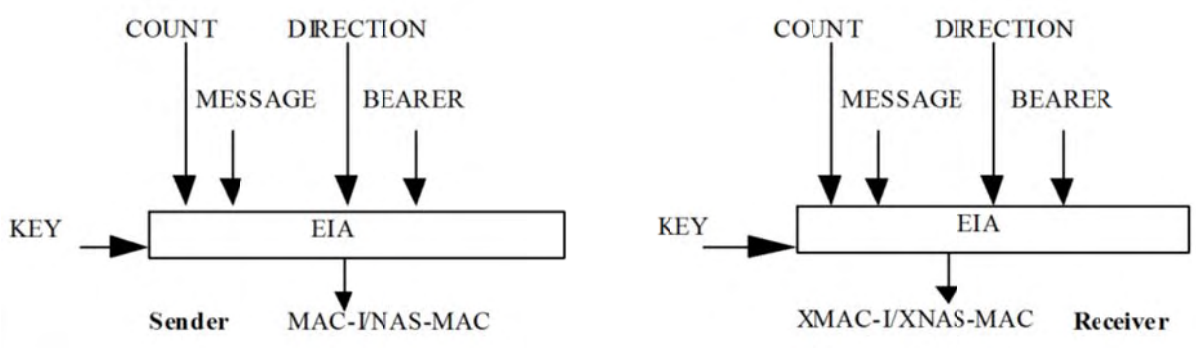
Η εμπιστευτικότητα ως χαρακτηριστικό του δικτύου αποτρέπει τις ευαίσθητες πληροφορίες να μεταφερθούν σε λάθος αποδέκτες ενώ διασφαλίζει ότι αυτές λαμβάνονται από τους σωστούς αποδέκτες. Στα δίκτυα LTE (Long Term Evolution) τα περισσότερα δεδομένα είναι προστατευμένα μέσω τεσσάρων αλγορίθμων EPS. Ο κάθε ένας από αυτούς τους αλγόριθμους σχετίζεται με έναν καθορισμό 4bit που αφήνει χώρο για 12 επιπλέον αλγορίθμους κωδικοποίησης (Olsson et al 2012).



Σχήμα 5.2: Διαδικασίες και δημιουργία ομάδων για την κρυπτογράφηση των δεδομένων στο LTE (3GPP TS 33.401 v12.10.0).

Η πληρότητα περιλαμβάνει τη διατήρηση της συμβατότητας της ακρίβειας και της αξιοπιστίας των δεδομένων στον εσωτερικό κύκλο ζωής τους. Τα δεδομένα δεν πρέπει να αλλοιώνονται στην μεταφορά τους και πρέπει να διασφαλίζεται πως δεν

τα χειρίζονται αναρμόδιοι χρήστες (Techtarget). Στα συστήματα LTE (Long Term Evolution) σχεδόν όλα τα δεδομένα είναι προστατευμένα για την πληρότητα τους μέσω τεσσάρων αλγορίθμων πληρότητας (EIA) που χρησιμοποιούνται για την πλήρη προστασία των δεδομένων.



Σχήμα 5.3: Λειτουργίες ολοκλήρωσης δεδομένων στο LTE (Long Term Evolution) (3GPP TS 33.401 v12.10.0).

5.3 Εξελίξεις στα Συστήματα ασφαλείας στα PPDR

Στο πλαίσιο της ανάπτυξης της διακρατικής συνεργασίας σε Ευρωπαϊκό επίπεδο βρίσκεται σε εξέλιξη το πρόγραμμα ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) το οποίο αποσκοπεί στην ανάπτυξη πρότυπων διαδικασιών τεχνολογιών και νομικών συμφωνιών προκειμένου να επιτευχθεί μια αποτελεσματική λύση για την ασφαλή διακρατική σύνδεση ανάμεσα στις χώρες της Ευρώπης (http://isitep.eu/). Οι τελικοί χρήστες που συμμετέχουν στο ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) υποκινούνται από την απαίτηση της διασφάλισης νόμιμης, λειτουργικής και τεχνικής συνοχής. Το ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) θα δημιουργήσει πλήρη αντανάκλαση της διεπιφάνειας για τις πηγές PPDR (Public Protection and Disaster Relief) στα διάφορα σενάρια που μπορεί να προκύψουν. Το αναμενόμενο αποτέλεσμα του συγκεκριμένου προγράμματος είναι η δημιουργία μιας νέας διεπιφάνειας εσωτερικού συστήματος που θα δημιουργεί τη διασύνδεση των δικτύων TETRA (Terrestrial Trunked Radio) τα οποία θα ολοκληρώνονται μέσω μιας σύνδεσης IP(Internet Protocol address) (ETSI EN 300 392-3-1, 2010).

Η νέα αυτή διεπιφάνεια πρόκειται να συνδέει τα δίκτυα TETRA (Terrestrial Trunked Radio) και TETRAPOL καθώς επίσης να συνδέει και τα όμοια δίκτυα μεταξύ τους.

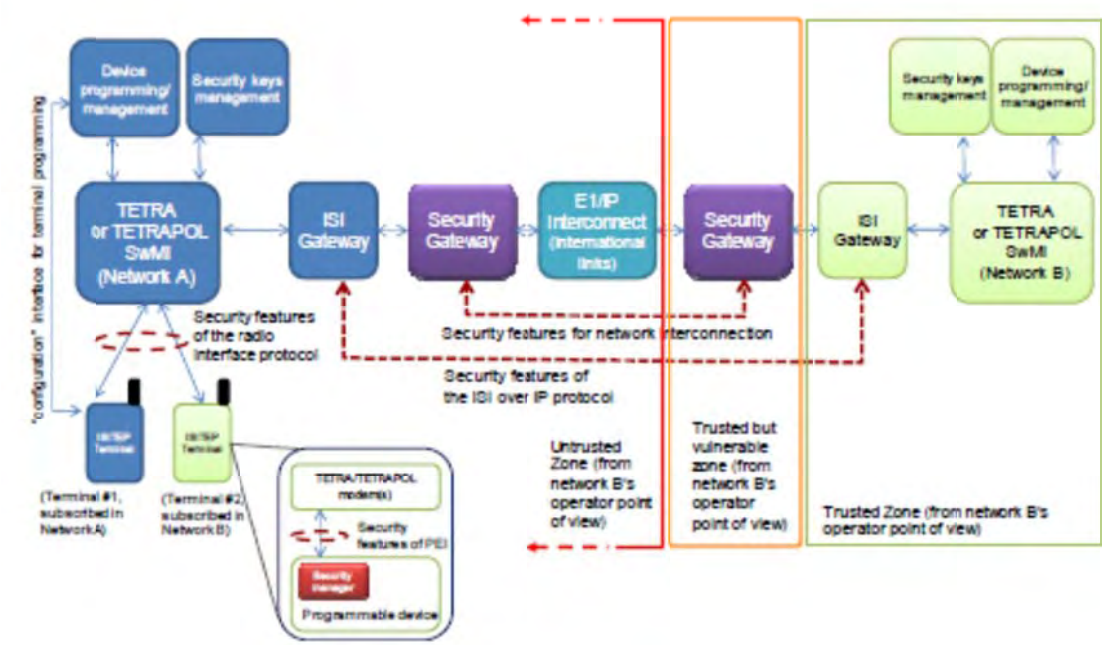
Ενώ ο κοινός στόχος του ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) είναι η ανάπτυξη ενός δικτύου IP έτσι ώστε να διασυνδέονται τα διάφορα δίκτυα TETRAPOL και TETRA (Terrestrial Trunked Radio) μεταξύ των διαφόρων χωρών το συγκεκριμένο δίκτυο αναμένεται να ολοκληρώσει τα δίκτυα στενής ζώνης των δικτύων PPDR (Public Protection and Disaster Relief) δημιουργώντας διάφορες πλατφόρμες. Το βασικό ζήτημα που προκύπτει στα δίκτυα αυτά είναι το ζήτημα της ασφάλειας των επικοινωνιών. Οι απειλές στα διασυνδεμένα συστήματα επικοινωνιών και στους τερματικούς σταθμούς μπορούν να μειωθούν σημαντικά με τη βοήθεια τεχνικών διαδικαστικών και περιβαλλοντικών μετρήσεων. Αυτό καθιστά απαραίτητη την κατανόηση των ασφαλών και έμπιστων συστημάτων επικοινωνίας που χρειάζονται στα PPDR (Public Protection and Disaster Relief) συστήματα.

Στο σύστημα ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) γίνεται η παραδοχή πως τα διασυνδεμένα τελικά σημεία είναι έμπιστα αλλά η σύνδεση του δικτύου δεν είναι αξιόπιστη. Κατά συνέπεια σε ένα σύστημα PPDR μπορεί να αναγνωριστούν τρεις περιοχές ασφαλείας για ένα δεδομένο χειριστή δικτύου PPDR και ανάλογα με τον λειτουργικό έλεγχο του χειριστή δικτύου, την τοποθεσία των ειδικών στοιχείων του δικτύου και τη συνδεσιμότητα τους με άλλα στοιχεία του δικτύου. Οι τρεις αυτές ζώνες είναι (i3 forum, 2011):

-Αξιόπιστη ζώνη στην οποία διαμένουν τα στοιχεία του χειριστή ή του παροχού του δικτύου

- αξιόπιστη αλλά ευάλωτη ζώνη στην οποία τα στοιχεία του δικτύου λειτουργούν από τον χρήστη του δικτύου ή τον παροχό των υπηρεσιών αλλά δεν ελέγχονται απαραίτητα από τον χειριστή ή τον παροχό των υπηρεσιών.

- μη αξιόπιστη ζώνη στην οποία περιλαμβάνονται τα στοιχεία που ανήκουν στους υπόλοιπους χειριστές του δικτύου τους παροχούς των υπηρεσιών ή τους τελικούς πελάτες.



Σχήμα 5.1. Ανάπτυξη συστήματος ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) για την ανάπτυξη των απαιτήσεων ασφαλείας των συστημάτων PPDR.

Αξίζει να σημειωθεί ότι όταν ένα στοιχείο βρίσκεται στην ζώνη αξιοπιστίας είναι και ασφαλές. Τα στοιχεία της αξιόπιστης ζώνης μπορούν επίσης να προστατευτούν από ένα συνδυασμό διαφόρων μεθόδων.

Στο ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) προτείνεται η ανάπτυξη μιας θύρας ασφαλείας που θα παρέχει ενισχυμένη ασφάλεια στην κυκλοφορία και την σήμανση των πληροφοριών που κινούνται στα όρια των συστημάτων PPDR (Public Protection and Disaster Relief). Η θύρα ασφαλείας σύμφωνα με το σχεδιασμό αυτό τοποθετείται στην αξιόπιστη αλλά ευπαθή ζώνη και βασικός της ρόλος είναι η προστασία των στοιχείων που βρίσκονται στη ζώνη αξιοπιστίας από επιθέσεις ασφαλείας που μπορεί να προκαλούνται από την μη αξιόπιστη ζώνη. Ειδικότερα το πλαίσιο ασφαλείας ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) βασίζεται στις θύρες ασφαλείας και καλείται να αντιμετωπίσει δύο βασικά στοιχεία. Από τη μια παρέχει εμπιστευτικότητα και ολοκλήρωση της μεταφοράς δεδομένων ανάμεσα στα δίκτυα και από την άλλη να αποτρέπει τις παρεμβολές στα εθνικά δίκτυα (i3 forum, 2011).

Οι αλγόριθμοι κωδικοποίησης TETRA (Terrestrial Trunked Radio) μπορεί να χρησιμοποιηθούν για την προστασία των πληροφοριών βάση της αέριας

διεπιφάνειας που αποτελεί πρότυπο για την δημόσια ασφάλεια στην Ευρώπη. Στα συστήματα TETRA (Terrestrial Trunked Radio) η ασφάλεια παρέχεται στη βάση της κωδικοποίησης της Αέριας διεπιφάνειας (AIE) και βάσει της κωδικοποίησης από άκρο σε άκρο (E2EE).

ΚΕΦΑΛΑΙΟ 6

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στη συγκεκριμένη εργασία παρουσιάστηκαν οι βασικές τεχνολογίες για τα συστήματα PPDR (Public Protection and Disaster Relief) που χρησιμοποιούνται σήμερα και που αναπτύσσονται. Τα συνηθέστερα συστήματα που χρησιμοποιούνται σήμερα βασίζονται στις τεχνολογίες TETRA (Terrestrial Trunked Radio) και TETRAPOL και βρίσκουν εφαρμογή στα περισσότερα συστήματα. Τα συστήματα αυτά είναι ιδιαίτερα ασφαλή και στηρίζουν την ασφάλεια τους σε αλγόριθμους ασφαλείας και στην αναγνώριση ταυτότητας.

Τις τελευταίες δεκαετίες που μεγαλώνουν οι ανάγκες επικοινωνίας και στα συστήματα φυσικών καταστροφών επιβάλλεται η συνεργασία σε επίπεδο κρατών έγινε αναγκαία η ανάπτυξη ψηφιακών συστημάτων LTE (Long Term Evolution) που έχει πολλά πλεονεκτήματα έναντι της τεχνολογίας TETRA (Terrestrial Trunked Radio) και τα οποία όμως έχουν ιδιαίτερα ζητήματα ασφάλειας που πρέπει να επιλυθούν.

Το TETRA (Terrestrial Trunked Radio) είναι το μόνο σύστημα ραδιοεπικοινωνιών που υπάρχει ανεπτυγμένο στην Ευρώπη και με το οποίο οι δημόσιες υπηρεσίες ασφαλείας έχουν ένα ευρύ δίκτυο κάλυψης και νέες λειτουργικές δυνατότητες. Το πλεονέκτημα του TETRA (Terrestrial Trunked Radio) όπως ήδη αναφέρθηκε είναι πως παρέχει σε μεγάλο εύρος την ασφάλεια φωνής και τη μετάδοση δεδομένων και επίσης μπορεί εκτός από δεδομένα να μεταφέρει και φωτογραφίες μέσω κινητών τερματικών σταθμών. Ανάμεσα στις ευρωπαϊκές χώρες που έχουν υιοθετήσει τα συστήματα TETRA (Terrestrial Trunked Radio) είναι και η Ελλάδα στην οποία όμως το σύστημα δεν βρίσκεται σε ευρεία εξάπλωση.

Στην προσπάθεια αύξησης της ασφάλειας των ήδη υπάρχοντων τεχνολογιών στα συστήματα PPDR (Public Protection and Disaster Relief) δημιουργήθηκε τα

τελευταία χρόνια ένα σύστημα ασφαλείας το ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) το οποίο εξασφαλίζει την διαλειτουργικότητα των δικτύων TETRA (Terrestrial Trunked Radio) και TETRAPOL. Αποδεικνύεται ότι η ασφάλεια των συγκεκριμένων συστημάτων είναι μια διαδικασία που απαιτεί την κατανόηση της λειτουργίας του δικτύου και σχετίζεται άμεσα τόσο με το σχεδιασμό του όσο και με την απόδοση της λειτουργίας του.

Βιβλιογραφία

Barca, C., 2017. Tetra system-open platform- intercoperability and applications Journal of Information Systems and operations management, ftp://ftp.repec.org/opt/ReDIF/RePEc/rau/jisomg/SU17/JISOM-SU17-A15.pdf.

Becchetti, C.; Frosali, F.; Lezaack, E., 2013. "Transnational Interoperability: A System Framework for Public Protection and Disaster Relief," Vehicular Technology Magazine, IEEE , vol.8, no.2, pp.46,54

Detecon LTE for Public Safety Cost efficient upgrade from narrowband to broadband – is it possible? Opinion Paper V.1.1

Report ITU-R M.2033, 'Radiocommunication objectives and requirements for public protection and disaster relief', 2003.

Elmasry G. F., 2012 'Tactical Wireless Communications and Networks: Design Concepts and Challenges', Hoboken, NJ: John Wiley & Sons, Inc.,

Erricson, 2007. Long Term Evolution (LTE): an introduction, White paper

ETSI TR 102 181, 'Emergency Communications (EMTEL); Requirements for communication between authorities/ organisations during emergencies', February 2008.

ETSI 122468 - Group Communication System Enablers for LTE (GCSE_LTE) (3GPP TS 22.468 version 12.1.0 Release 12)

ETSI EN 300 392-3-1,2010 "TETRA V+D ISI General Design", V1.3.1,

ETSI EN 300 392-7, "Voice plus Data (V+D); Part 7: Security".

Et Industries 2017. Introducttion to Tetra Technology, http://www.tetramou.com

EU Research Project on "Inter-system interoperablity for TETRATETRAPOL networks (ISITEP)". http://isitep.eu/

GSMA - https://www.gsmaintelligence.com/research/2015/02/the-global-mvnofootprint-a-changing-environment/490/

3GPP TS 33.401 v12.10.0, "3GPP System Architecture Evolution (SAE); Security architecture

i3 Forum, 2011. "Security for IP Interconnections (Release 1.0)",

ITU-R 2015. Radiocommunication objectives and requirements for Public Protection and Disaster Relief (PPDR), M Series Mobile, radiodetermination, amateur and related satellite services

OFCOM, 2015. Tetrapol Factsheet Trunked radio system for emergency services, Federal Department of the Environment, Transport, Energy and Communications

DETEC

ttps://www.bakom.admin.ch/dam/bakom/en/dokumente/faktenblatt_tetrapol.pdf.download.pdf/factsheet.pdf.

Olsson, M. Sultana, S. Rommer, S. Frid L. Mulligan, C. 2009. SAE and the Evolved Packet Core, Linacre House, Jordan Hill, Oxford OX2 8DP, UK: Elsevier Ltd.

Parkinson, D. W. **2001**, "TETRA Security". BT Technology Journal, 19, pp. 81-88

P3 TCCA – **2015**. Study on the relative merits of TETRA, LTE and other broadband technologies for critical communications markets. Version 1.1

Pirnau,C., Botezatu, M.A., 2016 Service-Oriented Architecture (SOA) and Web Services -Database Systems Journal VII

Techtarget, "What is confidentiality, integrity, and availability (CIA)?," http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Developments in PPDR networks

DIMITRIOS CHALEPLIS

Master thesis

STAMOULIS GEORGIOS

Lamia

18/03/2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

ΕΞΕΛΙΞΕΙΣ ΣΤΑ ΔΙΚΤΥΑ PPDR

ΔΗΜΗΤΡΙΟΣ ΧΑΛΕΠΛΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η ΔΗΛΩΝ/-ΟΥΣΑ

Ημερομηνία

Υπογραφή

ΕΞΕΛΙΞΕΙΣ ΣΤΑ ΔΙΚΤΥΑ PPDR

ΔΗΜΗΤΡΙΟΣ ΧΑΛΕΠΛΗΣ

Τριμελής Επιτροπή:

Ονοματεπώνυμο, ΓΕΩΡΓΙΟΣ ΣΤΑΜΟΥΛΗΣ

Ονοματεπώνυμο, ΓΕΩΡΓΙΟΣ ΔΗΜΗΤΙΟΥ

Ονοματεπώνυμο, ΜΑΡΙΑ ΚΟΖΥΡΗ

Επιστημονικός Σύμβουλος:

Ονοματεπώνυμο ΙΩΑΝΝΗΣ ΚΟΡΙΝΘΙΟΣ