ΑΝΩΤΑΤΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ
ΤΕΧΝΟΛΟΓΙΚΟΥ ΤΟΜΕΑ

ΑΕΙ Πειραιά Τεχνολογικού Τομέα: Τμήμα Μηχανικών Η/Υ Συστημάτων

Θέμα πτυχιακής εργασίας:

Ασύρματα Δίκτυα Αισθητήρων

Επιβλέπουσα καθηγήτρια:

Αναστασία Βελώνη

Συγγραφέας:

Ειρήνη Μπούντου

Ιούνιος 2018

Το παρόν περιέχει 135 σελίδες

Περιεχόμενα

1 Περίληψη

Η παρούσα πτυχιακή εργασία έχει ως στόχο της να δημιουργήσει ένα γενικότερο πλαίσιο κατανόησης και γνώσης σε σχέση με το θέμα των ασύρματων δικτύων αισθητήρων, γνωστά και ως wireless network sensors (WSN), καθώς και να παρουσιάσει τις εφαρμογές τους μέσα από ένα πρίσμα αλληλεπίδρασης και θεματολογίας ασφάλειας που ανακύπτει από τη χρήση τους.

Πιο συγκεκριμένα, στο πρώτο κεφάλαιο γίνεται μια ιστορική αναδρομή των ασυρμάτων δικτύων αισθητήρων, μια γενικότερη παρουσίαση τους που σκοπό έχει να εξοικειώσει τον αναγνώστη με το θέμα καθώς και μια ανάλυση δυνατών και αδύνατων σημείων, ευκαιριών και απειλών (SWOT) που δημιουργεί η χρήση τους μεταξύ άλλων.

Στα μετέπειτα δύο κεφάλαια παρουσιάζονται με λεπτομέρειες τα τεχνικά στοιχεία που διέπουν τα δίκτυα των ασύρματων δικτύων αισθητήρων, τα επίπεδα λειτουργίας τους καθώς και τα διάφορα πρότυπα και πρωτόκολλα επικοινωνίας και οι τοπολογίες που εφαρμόζονται.

Στο έκτο κεφάλαιο γίνεται μια εκτενής αναφορά και ανάλυση σε σχέση με τις εφαρμογές που βρίσκουν τα ασύρματα δίκτυα αισθητήρων σε διάφορα πεδία με βάση τα πρωτοκόλλα επικοινωνίας τους και τα γενικότερα υφιστάμενα χαρακτηριστικά τους με βάση την εφαρμοσιμότητα ανά τον τομέα ενδιαφέροντος (λόγου χάριν ιατρικό, επιχειρηματικό, επιστημονικό κ.α.).

Στο έβδομο και όγδοο κεφάλαιο αναφερόμαστε σε κενά ασφαλείας που δημιουργεί η χρήση της τεχνολογίας των ασύρματων δικτύων αισθητήρων καθώς και στις σημαντικότερες τεχνικές που χρησιμοποιούνται για την θωράκισή τους ώστε να ελαχιστοποιείται η δυνατότητα παραβίασής τους. Κατόπιν γίνεται μια ανάλυση των νομικών και οικονομικών ζητημάτων που ανακύπτουν από περιστατικά παραβίασης της ασφάλειας των ασύρματων δικτύων αισθητήρων με ιδιαίτερη έμφαση στον κανονισμό Προστασίας

Προσωπικών Δεδομένων γνωστό και ως General Data Protection regulation (GDPR).

Τέλος στο ένατο κεφάλαιο υπάρχει μια επισκόπηση των τεχνολογιών ασύρματων δικτύων αισθητήρων με βάση την εφαρμοσιμότητά τους υπό το πρίσμα ενός ασφαλούς περιβάλλοντος επικοινωνίας.

2 Abstract

The purpose of this paper in to build a framework of better understanding and knowledge related to wireless sensor networks (WSN). Also its intention is to better present actual real life examples of WSNs whilst taking into account possible security threats that may arise.

In detail, in the first chapter a brief introduction to WSN will take place in order to help the reader gain a better understanding of the subject. Furthermore we will present a SWOT analysis (strengths, weaknesses, opportunities threats) of WSN in order to enhance the relevant business acumen of our readers.

In the next two chapters technical specifications of WSNs will be further presented. Topologies, protocols and communication layers will be elaborated on.

In the sixth chapter elaborate presentation of real life examples of WSNs takes place based on communication protocols and other characteristics as well as implementation by sector.

Both the seventh and eighth chapters refer to WSN technology security matters as well as cyber-attacks. A special reference is done with regards to the General Data Protection Regulation (GDPR).

Finally, in the last chapter, we lay out conclusions and opinion with regards to the WSN technology, how it is implemented, it’s viability under the prism of emerging threats.

3 Εισαγωγή στα Ασύρματα Δίκτυα Αισθητήρων

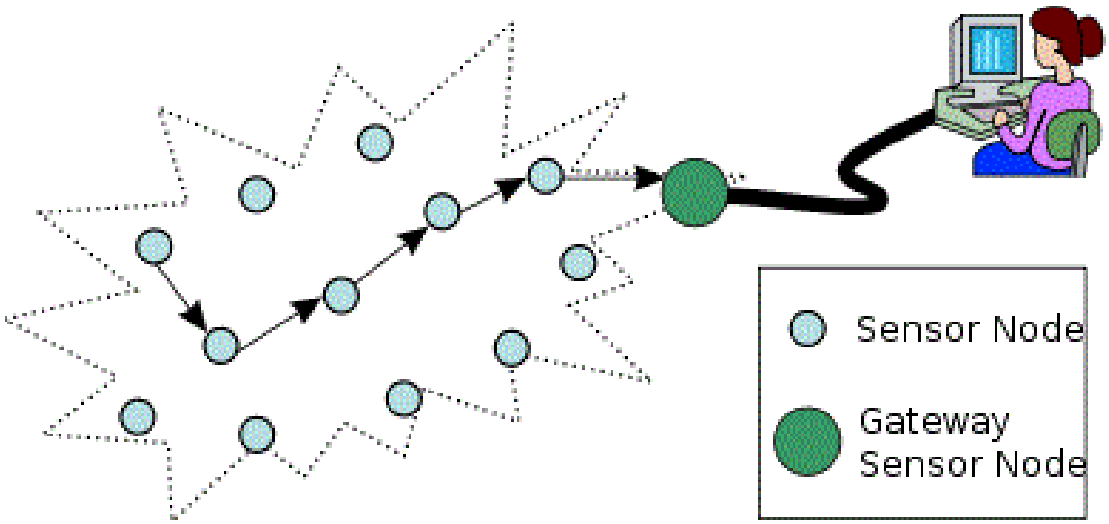
3.1 Ασύρματα Δίκτυα Αισθητήρων με μια ματιά

Τα ασύρματα δίκτυα αισθητήρων ή Wireless Sensor Networks (εφεξής “ΑΔΑ”) αποτελούν μια τεχνολογική καινοτομία η οποία έχει ολοένα και μεγαλύτερη εφαρμογή τα τελευταία χρόνια, σε διάφορα πεδία της επιστήμης των υπολογιστών και με διάφορες μορφές. Πρόκειται για την από κοινού χρήση ενός πλήθους υπολογιστικών συστημάτων για την επίτευξη ενός συγκεκριμένου στόχου. Σε συνδυασμό με τις εξελίξεις στον τομέα του υλικού (hardware) και των ασύρματων τηλεπικοινωνιών, τα παραπάνω ορίζουν το μέγεθος, την υπολογιστική ισχύ καθώς και τον τρόπο της μεταξύ τους επικοινωνίας δημιουργώντας ένα ορίζοντα δυνατοτήτων και εφαρμογών.

Ένα ΑΔΑ αποτελείται από διασκορπισμένους αυτόνομους υπολογιστές-αισθητήρες οι οποίοι μεταξύ άλλων έχουν ως σκοπό τους την παρακολούθηση φυσικών ή περιβαλλοντολογικών συνθηκών (π.χ. θερμοκρασία, ήχο, ατμοσφαιρική πίεση κ.α.) και μέσω συνεργασίας να μεταφέρει τα δεδομένα μέσω του δικτύου σε μια συγκεκριμένη τοποθεσία. Τα πιο μοντέρνα δίκτυα είναι ικανά και να δίνουν αλλά και να δέχονται πληροφορίες πράγμα που τους επιτρέπει να ελέγχουν την δραστηριότητα των αισθητήρων. Αρχικά, το κίνητρο για την ανάπτυξη των ασύρματων δικτύων με αισθητήρες αποτέλεσαν οι στρατιωτικές εφαρμογές όπως η παρακολούθηση των πεδίων μάχης ενώ σήμερα τέτοια δίκτυα χρησιμοποιούνται σε πολλές καταναλωτικές και βιομηχανικές εφαρμογές όπως η παρακολούθηση και ο έλεγχος της βιομηχανικής παραγωγής, η παρακολούθηση των μηχανημάτων υγείας και πολλά άλλα.

Πιο συγκεκριμένα, ένα τυπικό ασύρματο δίκτυο αισθητήρων (βλέπε Σχήμα 1) αποτελείται από κόμβους - από μερικές σε αρκετές εκατοντάδες η ακόμα και χιλιάδες, όπου κάθε κόμβος συνδέεται σε έναν (η κάποιες φορές σε αρκετούς)

αισθητήρες. Κάθε τέτοιος κόμβος του δικτύου αισθητήρων έχει χαρακτηριστικά μερικά κομμάτια: ένα ράδιο-πομποδέκτη με μια εσωτερική κεραία ή μια σύνδεση με μια εξωτερική κεραία, ένα μικρό-ελεγκτή, ένα ηλεκτρονικό κύκλωμα για τη διασύνδεση με τους αισθητήρες και μια πηγή ενέργειας, συνήθως μια μπαταρία ή μια ενσωματωμένη μορφή συγκομιδής ενέργειας. Ένας αισθητήριος κόμβος μπορεί να ποικίλει σε μέγεθος από εκείνο ενός κουτιού παπουτσιών μέχρι το μέγεθος ενός κόκκου σκόνης.



Σχήμα 1 - Τυπικό Ασύρματο Δίκτυο Αισθητήρων

Το κόστος των αισθητήριων κόμβων ποικίλει, ξεκινώντας από μερικά και φτάνοντας σε εκατοντάδες ευρώ, αναλόγως την πολυπλοκότητα των μεμονωμένων αισθητήριων κόμβων. Οι περιορισμοί σε μέγεθος και κόστος έχουν ως αποτέλεσμα αντίστοιχους περιορισμούς σε πόρους όπως ενέργεια,μνήμη, υπολογιστική ταχύτητα καθώς και το εύρος ζώνης των επικοινωνιών. Η τοπολογία των αισθητήρων μπορεί να διαφέρει από ένα δίκτυο τοπολογίας αστέρος σε ένα αναπτυγμένο ασύρματο δίκτυο πλέγματος multi-hop.

Τα ασύρματα δίκτυα αισθητήρων έχουν ένα αρκετά ευρύ πεδίο εφαρμογών, το οποίο είναι ακόμα ανοιχτό, δηλαδή συνεχώς γίνονται νέες προτάσεις για

εφαρμογές στις οποίες τα ΑΔΑ αντικαθιστούν τις υπάρχουσες μεθόδους ενώ παράλληλα μας δίνουν τη δυνατότητα υλοποίησης εφαρμογών που προγενέστερα αποτελούσαν απλώς φαντασία. Φυσικά η υλοποίηση των ΑΔΑ για εφαρμογές όπως αυτές που αναφέρθηκαν προγενέστερα, βασίζεται σε ένα κοινό πρότυπο, δηλαδή έχουμε ένα μεγάλο πλήθος από κόμβους ασύρματων δικτύων αισθητήρων τοποθετημένους σε συγκεκριμένη θέση, οι οποίοι με βάση της δυνατότητες τους και το εγκατεστημένο λογισμικό αντλούν πληροφορίες από το περιβάλλον τους τις οποίες προωθούν με το κατάλληλο δικτυακό πρωτόκολλο επικοινωνίας σε ένα κέντρο ελέγχου.

Σε αντίθεση με την απλότητα της αρχικής ιδέας, η υλοποίηση των ΑΔΑ δεν αποτελεί καθόλου εύκολη υπόθεση. Μάλιστα οι προκλήσεις που παρουσιάζονται σε ερευνητικό επίπεδο εφαρμογής έχουν να κάνουν με την συνεχή επιδίωξη κατασκευής μικρών σε μέγεθος κόμβων δικτύων σε ολοένα και μεγαλύτερες αποστάσεις που να λειτουργούν σε αντίξοες συνθήκες ενώ παράλληλα να καταναλώνουν ελάχιστη ενέργεια. Μόλις τα τελευταία χρόνια κατέστη δυνατή η κατασκευή ολοκληρωμένων ΑΔΑ που να είναι παραγωγικά και να μην εξυπηρετούν μόνο ερευνητικούς και στρατιωτικούς σκοπούς.

3.2 Ανάλυση SWOT

Η ανάλυση SWOT που αποτελεί ακρώνυμο των Strengths, Weaknesses, Opportunities, Threats, αποτελεί ένα εργαλείο στρατηγικού σχεδιασμού το οποίο χρησιμοποιείται για την ανάλυση του εσωτερικού και εξωτερικού περιβάλλοντος μίας επιχείρησης, όταν η επιχείρηση πρέπει να λάβει μία απόφαση σε σχέση με τους στόχους που έχει θέσει ή με σκοπό την επίτευξή τους. Κατά την ανάλυση SWOT μελετώνται τα δυνατά (Strengths) και αδύνατα (Weaknesses) σημεία μίας επιχείρησης, οργανισμού ή και περιοχής, καθώς και οι ευκαιρίες (Opportunities) και οι απειλές (Threats) που υπάρχουν.

Πιο συγκεκριμένα, τα δυνατά και αδύνατα σημεία αφορούν το εσωτερικό περιβάλλον της επιχείρησης καθώς προκύπτουν από τους εσωτερικούς πόρους που αυτή κατέχει (π.χ. ικανότητες προσωπικού και στελεχών, ιδιότητες και χαρακτηριστικά της επιχείρησης, τεχνογνωσία, χρηματοοικονομική υγεία και ικανότητα να ανταποκριθεί σε νέες επενδύσεις, κλπ.). Ενώ στον αντίποδα οι ευκαιρίες και οι απειλές αντανακλούν μεταβλητές του εξωτερικού περιβάλλοντος της επιχείρησης τις οποίες η επιχείρηση θα πρέπει να εντοπίσει, να προσαρμοστεί σε αυτές ή ακόμα και να τις προσαρμόσει όπου κάτι τέτοιο είναι εφικτό (π.χ. είσοδος νέων ανταγωνιστών, ρυθμίσεις στο νομικό περιβάλλον, δημιουργία ή/και εμφάνιση νέων αγορών, κλπ.).

Στην περίπτωση των ΑΔΑ επιχειρούμε να εμφανίσουμε κάποιους παράγοντες που αποτελούν δυνατά σημεία, αδυναμίες καθώς και ευκαιρίες ή απειλές στο πλαίσιο μιας γενικότερης προεργασίας που καλλιεργεί στον αναγνώστη ένα τρόπος σκέψης που προσομοιάζει υπό το πρίσμα της βιωσιμότητας και της συνεχούς ροής πληροφοριών σε σχέση με τα ΑΔΑ στην εργασία αυτή την διαδικασία λήψης αποφάσεων. Ουσιαστικά κατά τη διάρκεια της ανάγνωσης των παρακάτω κεφαλαίων ο αναγνώστης καλείται να κατατάσσει συνεχώς τις προσλαμβάνουσες πληροφορίες και να μπορέσει να οδηγηθεί σε αποφάσεις ως προς τη βιωσιμότητα και την εφαρμογή των ΑΔΑ στην εποχή μας.

Στον παρακάτω πίνακα, παραθέτουμε μια ανάλυση SWOT σε σχέση με τα ΑΔΑ με σκοπό τη δημιουργία του κατάλληλου γνωστικού υπόβαθρου αλλά και τρόπου σκέψης που έχει σαν σκοπό τη λήψη επιχειρηματικών αποφάσεων.

ΠΙΝΑΚΑΣ 1 – SWOT Ανάλυση στα ΑΔΑ

Δυνάμεις	**Αδυναμιες**
Τοποθεσία - Τα ΑΔΑ μπορούν να χρησιμοποιηθούν και να παράξουν αποτέλεσμα σε τοποθεσίες όπου η συλλογή και επεξεργασία δεδομένων είναι απαγορευτική με άλλες μεθόδους. Π.χ. σε ένα δύσβατο δάσος ή σε υπόγεια περιοχή	Τοποθεσία - Τα ΑΔΑ μπορούν να χρησιμοποιηθούν μόνο εφόσον δεν υπάρχει κώλυμα συνυφασμένο με την τοποθεσία. Π.χ ιδιοκτησία, νομική απαγόρευση

Μικρό κόστος υλοποίησης σε σχέση με άλλες μεθόδους συλλογής και επεξεργασίας δεδομένων. Π.χ. εύκολη και οικονομική παρακολούθηση παραμέτρων αγροτικής παραγωγής	Εξυπηρέτηση πελατών και διαχείριση περιστατικών. Συχνά τα ΑΔΑ λόγω της φύση τους ως προς το μέγεθος και την τοποθεσία τους, είναι εξαιρετικά κοστοβόρα για να επισκευασθούν. Π.χ. 10 εξαιρετικά σημαντικοί πομποί σε ένα πολύ δύσβατο σημείο έχουν υποστεί βλάβη. Η επισκευή τους κρίνεται ασύμφορη και νέοι πομποδέκτες τοποθετούνται στο δίκτυο.
Ιδιαιτερότητα προϊόντος. Λόγω της ιδιαιτερότητας του προϊόντος, συχνά οι λύσεις ΑΔΑ μπορούν να δημιουργήσουν μεγάλο περιθώριο κέρδους. Π.χ. ΑΔΑ με μετρήσεις βασισμένες σε δείκτες υγείας του ανθρώπινου σώματος	
Δυνατότητα προσωποποιημένων λύσεων. Λόγω της υψηλής δυνατότητας παραμετροποίησης τα ΑΔΑ μπορούν να χρησιμοποιηθούν για να καλύψουν ιδιαίτερα πολύπλοκες απαιτήσεις. Π.χ. ΑΔΑ για την αναγνώριση φίλιων πυρών στο πεδίο της μάχης	
Τεχνολογικά προηγμένα. Τα ΑΔΑ αποτελούν ένα τομέα που χαίρει ιδιαίτερης ανάπτυξης λόγω της συνεχούς τεχνολογικής δυναμικής. Π.χ. Τα ΑΔΑ με βάση την δυνατότητα επεξεργασίας δεδομένων των υλικών που χρησιμοποιούν δίνουν λύσεις σε προβλήματα ήταν οικονομικά ασύμφορο. Π.χ. λόγω της μικρής πιθανότητας καταστροφής από πυρκαγιά αλλά και της μεγάλης ανάγκης σε ισχύς για τη συνεχή παρακολούθηση παραμέτρων που συνιστούν μια πιθανή πυρκαγιά, τα αυτόνομα ΑΔΑ με χρήση ηλιακής ενέργειας αποτελούν λύση.	
Οικονομία κλίμακας. Τα ΑΔΑ με κάθε επιπλέον πομπό διευρύνουν την ποιότητα των δεδομένων που συλλέγουν και επεξεργάζονται, αποδίδοντας ένα καλύτερο προϊόν πληροφορίας. Π.χ. Ένα ολοένα αυξανόμενο ΑΔΑ μπορεί να δώσει πιο λεπτομερή και ορθά στοιχεία με κάθε επιπλέον πομπό που προστίθεται στο δίκτυό του.	
Ευκαιρίες	**Απειλές**

Τεχνολογική Εξέλιξη. Τα ΑΔΑ με την εξέλιξη της τεχνολογίας μπορούν να δώσουν καλύτερες ή νέες υπηρεσίες σε μικρότερο κόστος ή να δημιουργήσουν νέες αγορές. Π.χ. Ένα ΑΔΑ σε μια δύσβατη περιοχή χρειάζεται 25 πομπούς για να παράξει πληροφορία. Η επεξεργασία και πώληση της πληροφορίας ίσα που καλύπτει τα κόστη λειτουργίας της εταιρίας. Με τη χρήση νέων τεχνολογιών προστίθενται άλλοι 10 πομποδέκτες εξοπλισμένοι με καλύτερους αισθητήρες ικανοί να παράγουν πληροφορία μεγαλύτερης αξίας της οποίας η πώληση δίνει τη δυνατότητα στην εταιρία να επενδύσει στην αναπτυξιακή της πολιτική. Π.χ. Πομποδέκτες ικανοί να ανιχνεύσουν στοιχεία που σχετίζονται με δείκτες υγείας στον άνθρωπο δημιουργούν μια νέα αγορά καθώς και ένα νέο προϊόν.	Αλλαγές στη νομοθεσία. Συχνά αλλαγές στη νομοθεσία διέπουν τα τεχνολογικά προϊόντα. Αυτό ανεβάζει το ρυθμιστικό και το κόστος συμμόρφωσης. Π.χ. Με το GDPR πολλά ΑΔΑ χρειάζεται να επανασχεδιαστούν με σκοπό την προστασία των προσωπικών δεδομένων που συλλέγουν.
	Αλλαγές στο πολιτικό πλαίσιο. Συχνά βλέπουμε αλλαγές στο πολιτικό πλαίσιο μιας χώρας δημιουργώντας ένα περιβάλλον ρίσκου για επιχειρήσεις που στηρίζουν το κύκλο εργασιών τους σε τεχνολογίες ευάλωτες στις αποφάσεις κυβερνήσεων. Π.χ. Η Κυβέρνηση εισάγει ένα νέο φορολογικό σύστημα σε ότι έχει να κάνει με εισαγωγές τεχνολογίας αιχμής εκτός Ε.Ε.
	Κυβερνό-επιθέσεις. Λόγω του ότι τα ΑΔΑ χρησιμοποιούν τα ίδια η παρόμοια πρωτόκολλα επικοινωνίας με τα ήδη υπάρχοντα στα οποία στηρίζονται δίκτυα επικοινωνίας υπολογιστών αποτελούν στόχο κυβερνοεπιθέσεων. Π.χ. Ένα ΑΔΑ που συλλέγει ευαίσθητα ιατρικά προσωπικά δεδομένα μπορεί να πέσει θύμα hacker.

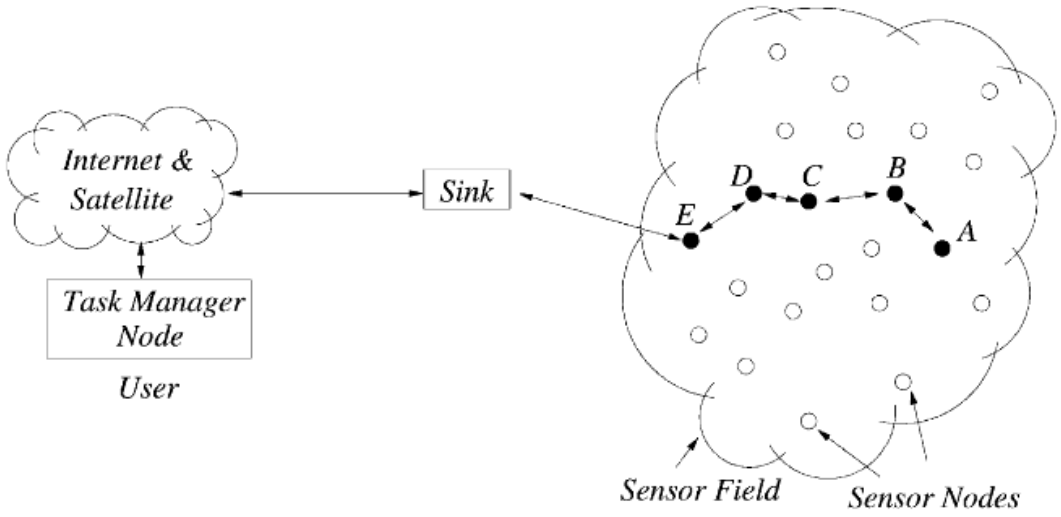
4 Αρχιτεκτονική Ασύρματων Δικτύων Αισθητήρων

4.1 Βασικά χαρακτηριστικά των Ασύρματων Δικτύων Αισθητήρων

Η πρόοδος της τεχνολογίας στις ασύρματες επικοινωνίες και στην ηλεκτρονική έχουν καταστήσει εφικτή την ανάπτυξη αισθητήρων:

1. Χαμηλού κόστους,
2. χαμηλής ισχύος,
3. μικρού μεγέθους που τους χαρακτηρίζει η ενεργειακή αυτονομία και είναι ικανοί να επικοινωνήσουν σε μικρές σχετικά αποστάσεις μεταξύ τους.

Ένα ασύρματο δίκτυο αισθητήρων, όπως έχει ήδη αναφερθεί, αποτελείται από ένα μεγάλο αριθμό κόμβων αισθητήρων κατάλληλα τοποθετημένων κοντά στο φαινόμενο παρατήρησης ή μέσα σε αυτό. Η θέση των αισθητήρων μπορεί να είναι ή να μην είναι σχεδιασμένη. Η τελευταία υπόθεση επιτρέπει την τυχαία ανάπτυξη τους σε περιβάλλοντα μη προσπελάσιμα από τον άνθρωπο ή σε επιχειρήσεις αντιμετώπισης καταστροφών. Από την άλλη πλευρά, η ίδια υπόθεση προϋποθέτει ότι τα πρωτόκολλα των δικτύων αυτών (καθώς τα πρωτόκολλα θα αναφερθούν αναλυτικά σε επόμενο κεφάλαιο - ο αναγνώστης μπορεί να θεωρεί τα πρωτόκολλα ως τους αλγόριθμος που χαρακτηρίζουν και περιγράφουν τα χαρακτηριστικά των ΑΔΑ) έχουν την ικανότητα να οργανώνονται από μόνα τους. Στο Σχήμα 2 φαίνεται ένα τέτοιο δίκτυο από διάσπαρτους αισθητήρες.



Σχήμα 2 - Δίκτυο διάσπαρτων ασύρματων αισθητήρων σε περιοχή παρακολούθησης

Όσον αφορά στον τρόπο επικοινωνίας μεταξύ των κόμβων αισθητήρων, έχει επίσης αναφερθεί πως ο κάθε κόμβος ενσωματώνει ηλεκτρονικά και ηλεκτρικά στοιχεία για το σκοπό αυτό. Μεταξύ άλλων, ο επεξεργαστής δίνει στον κάθε κόμβο τη δυνατότητα, αντί να στείλει κατευθείαν τα δεδομένα που έχει συλλέξει ο ίδιος σε έναν άλλον κόμβο που έχει καθοριστεί στο να αναλάβει τη μίξη δεδομένων των υπόλοιπων κόμβων (σταθμός βάσης), να χρησιμοποιεί ο ίδιος πρώτα τον επεξεργαστή του για την εκτέλεση καθορισμένων απλών υπολογισμών και στη συνέχεια να αποστέλλει μόνο τα απαραίτητα και μερικώς επεξεργασμένα δεδομένα. Η ενσωμάτωση αυτής δυνατότητας για τοπική επεξεργασία και αποθήκευση δεδομένων επιτρέπει στις μονάδες να εκτελέσουν πολύπλοκες λειτουργίες σύμφωνα με την εκάστοτε εφαρμογή που υλοποιούν. Επίσης, η δυνατότητα επικοινωνίας μεταξύ τους επιτρέπει όχι μόνο τη μεταφορά και τον έλεγχο των δεδομένων κατά μήκος του δικτύου, αλλά και τη συνεργασία μεταξύ των μονάδων κόμβων προς επίτευξη πολύπλοκων αλγορίθμων και εργασιών, όπως είναι η συνάθροιση δεδομένων (data aggregation), η στατιστική δειγματοληψία και η παρακολούθηση της κατάστασης και της υγείας ενός συστήματος [1-5].

Τα ΑΔΑ μπορούν να θεωρηθούν δίκτυα υπολογιστικών συσκευών τα οποία χαρακτηρίζονται από βασικές ιδιότητες και ταυτόχρονα έχουν βασικές διαφορές από τα παραδοσιακά δίκτυα δεδομένων.

Οι βασικές ιδιότητες των ασύρματων δικτύων αισθητήρων συνοψίζονται στα παρακάτω σημεία [3].

1. Δυνατότητα αυτό-οργάνωσης,
2. επικοινωνία περιορισμένου βεληνεκούς και δρομολόγηση πολλαπλών αλμάτων (multi-hop),
3. πυκνή τοποθέτηση των κόμβων και συνεργατική προσπάθεια
4. συχνά μεταβαλλόμενη τοπολογία λόγω εξασθένησης του σήματος και αποτυχίας των κόμβων,
5. περιορισμοί στην ενέργεια, την ισχύ εκπομπής, την μνήμη και την υπολογιστική δυνατότητα και
6. πιθανότατα έλλειψη γενικής αναγνώρισης (identification) των κόμβων λόγω υψηλού overhead και μεγάλου αριθμού κόμβων.

Κάποιες από τις βασικές διαφορές των ΑΔΑ από τα παραδοσιακά δίκτυα δεδομένων [6] συγκεντρώνονται παρακάτω, ενώ δίνονται περιληπτικά κάποιες επιπρόσθετες διαφορές στον Πίνακα 1:

1. Σε σχέση με τα κλασικά δίκτυα υπολογιστών έχουν χαμηλότερη υπολογιστική ισχύ και περιορισμούς στην ενέργεια, την αποθήκευση και το εύρος ζώνης. Η δρομολόγηση και η διαχείριση κινητικότητας, στα παραδοσιακά ασύρματα δίκτυα, εκτελούνται με σκοπό τη βελτιστοποίηση του QoS (Quality of service: είναι το μέτρο της καθολικής απόδοσης μίας υπηρεσίας). Η κατανάλωση ενέργειας συνιστά δευτερεύουσα απαίτηση, καθώς η πηγή ενέργειας μπορεί να αντικατασταθεί ή να επαναφορτιστεί οποιαδήποτε στιγμή. Τα ασύρματα δίκτυα αισθητήρων έχουν σχεδιαστεί για εφαρμογές σε περιβάλλον λειτουργίας χωρίς την ανάγκη ανθρώπινης

παρέμβασης. Συνεπώς, η υπηρεσίατης δρομολόγησης πρέπει να αποσκοπεί στη βελτιστοποίηση της χρήσης της ενέργειας, με σκοπό τη μεγιστοποίηση της διάρκειας ζωής του δικτύου.

2. Η συνήθης κίνηση δεδομένων στα παραδοσιακά δίκτυα υπολογιστών προκύπτει από χρήστες που συνδέονται με ένα κόμβο και απαιτούν κάποια υπηρεσία. Η σύνδεση μεταξύ των δυο αυτών κόμβων πιθανότατα θα πραγματοποιείται με τη βοήθεια και άλλων ενδιάμεσων κόμβων, όμως το μοντέλο αλληλεπίδρασης είναι ευθύ, από την άποψη πως ο χρήστης αλληλεπιδρά άμεσα με το χρήστη ή την υπηρεσία στο άλλο άκρο επικοινωνίας. Από την άλλη, τα ασύρματα δίκτυα αισθητήρων μοιάζουν περισσότερο σε κατανεμημένα συστήματα και όχι σε τυπικά δίκτυα. Οι κόμβοι συνεργάζονται για την παραγωγή των αποτελεσμάτων, ενώ ο χρήστης συνήθως δεν ενδιαφέρεται για τα αποτελέσματα μεμονωμένων κόμβων. Τα ασύρματα δίκτυα αισθητήρων λοιπόν, δεν παρέχουν υπηρεσίες διασύνδεσης απομακρυσμένων κόμβων, αλλά πληροφορίες μεταβολών καταστάσεων από περιοχές του δικτύου, στους χρήστες.
3. Οι κόμβοι ενός ασύρματου δικτύου αισθητήρων στις περισσότερες εφαρμογές είναι στατικοί αφού τοποθετηθούν, με λίγες εξαιρέσεις σε εφαρμογές όπου η κινητικότητα των κόμβων αποτελεί απαίτηση.
4. Στους κόμβος των ασύρματων δικτύων αισθητήρων διακινούνται δεδομένα με χαμηλό ρυθμό μετάδοσης, με εμφανές το φαινόμενο του πλεονασμού (Επεξήγηση του φαινομένου του πλεονασμού γίνεται παρακάτω, στο ίδιο κεφάλαιο).

ΠΙΝΑΚΑΣ 2 – [6]

	ΑΔΑ	**Παραδοσιακά δίκτυα δεδομένων**
Αριθμός κόμβων	Μεγάλος, εκατοντάδες έως χιλιάδες κόμβοι ή και περισσότεροι	Μικρός μέχρι μέσος
Πυκνότητα κόμβων	Υψηλή	Σχετικά χαμηλή
Πλεονασμός Δεδομένων	Υψηλός	Περιορισμένος
Τροφοδότηση Ισχύος	Μη επαναφορτιζόμενη λειτουργία - Αναντικατάστατες Μπαταρίες	Επαναφορτιζόμενη λειτουργία και/ή αντικατάσταη μπαταριών
Ρυθμός δεδομένων	Χαμηλός 1-100kbps	Υψηλός
Κινητικότητα των κόμβων	Χαμηλή	Πιθανότατα υψηλή Κινητικότητα
Κατεύθυνση της ροής δεδομένων	Κυρίως μονοκατευθυντήρια ροή ασύρματοι κόμβοι/ sink	Δικατευθυντήρια από άκρο σε άκρο
Προώθηση πακέτων	Πολλοί κόμβοι σε έναν. Κατεύθυνση προσανατολισμένη στα δεδομένα (data centric)	Από άκρο σε άκρο. Κατεύθυνση προσανατολισμένη στη διεύθυνση (address centric)
Φύση αίτησης	Βασισμένη στην κατάσταση (attribute based)	Βασισμένη στον κόμβο
Μετάδοση αιτήσεων	Πολύ-εκπομπή (broadcast)	Πολύ-εκπομπήή hop by hop
Διευθυνσιοδότηση	Έλλειψη γενικού identification	Χρήσηγενικού identification (global id)
Ενεργό Duty cycle	Χαμηλό, έως και 1%	Υψηλό

Σε αυτό το σημείο έχει σημασία να αναφερθεί πως τα ασύρματα δίκτυα αισθητήρων μπορούν να ταξινομηθούν βάση διαφόρων κριτηρίων. Κάποια από

τα κριτήρια αναφέρονται αναλυτικά παρακάτω και παρουσιάζονται συνοπτικά στον Πίνακα 4 [6]. Τα ΑΔΑ μπορούν να ταξινομηθούν:

1. Σύμφωνα με τις απαιτήσεις του χώρου της εφαρμογής σε υπέργεια, υπόγεια, υποθαλάσσια, πολυμεσικά (multimedia) και κινούμενα, τα χαρακτηριστικά των οποίων συνοψίζονται στον Πίνακα 3 [3].

ΠΙΝΑΚΑΣ 3 – {3]

	Ορισμός	**Προκλήσεις**	**Εφαρμογές**
Υπέργεια ΑΔΑ	Το δίκτυο αποτελείται από εκατοντάδες ή χιλιάδες ασύρματους κόμβους τοποθετημένους στο έδαφός	In network συγκέντρωση δεδομένων για βελτίωση της απόδοσης στην επικοινωνία, στο ενεργειακό κόστος και την καθυστέρηση. Ελαχιστοποίηση ενεργειακού κόστους. Μείωση της ποσότητας των δεδομένων επικοινωνίας. Εύρεση βέλτιστης διαδρομής. Κατανομή ενεργειακής κατανάλωσης. Περιορισμός πλεονασμού.	Αίσθηση και επίβλεψη περιβάλλοντος. Βιομηχανική επίβλεψη. Εξερευνήσεις επιφάνειας.
Υπόγεια ΑΔΑ	Το δίκτυο από ασύρματους κόμβους τοποθετημένους υπόγεια, ή σε σπηλιές, ορυχεία.	Ακριβή εφαρμογή, συντήρηση υψηλό κόστος εξοπλισμού. Απειλές για τις συσκευές (περιβάλλον ζώα). Οι μπαταρίες δεν μπορούν εύκολα να αντικατασταθούν. Προκλήσεις τοπολογίας σε	Επίβλεψη στη γεωργία. Υπόγεια δομική επίβλεψη. Υπόγεια επίβλεψη εδάφους, ορυκτών ή υδάτων. Επίβλεψη στρατιωτικών

		περίπτωση προσχεδιασμένης εφαρμογής. Υψηλά επίπεδα εξασθένησης και απώλειας σήματος.	συνόρων.
Υποθαλάσσια ΑΔΑ	Το δίκτυο από ασύρματους κόμβους τοποθετημένους στο περιβάλλον του ωκεανού	Ακριβοί υποθαλάσσιοι αισθητήρες. Αστοχία του υλικού λόγω περιβαλλοντικών παραγόντων (π.χ. διάβρωση). Οι μπαταρίες δεν μπορούν εύκολα να αντικατασταθούν. Αραιή κατανομή κόμβων. Περιορισμένο εύρος ζώνης. Μεγάλη καθυστέρηση διάδοσης, φαινόμενα εξασθένησης του σήματος.	Παρατήρηση περιβαλλοντικής μόλυνσης. Υποθαλάσσια εξερεύνηση και επιτήρηση. Παρατήρηση σεισμικής δραστηριότητας. Επιτήρηση εξοπλισμού. Υποθαλάσσια ρομποτική.
Multimedia ΑΔΑ	Το δίκτυο από ασύρματους κόμβους, ικανούς να επεξεργάζονται, να αποθηκεύουν και να εξάγουν δεδομένα (βίντεο, εικόνα, ήχο)	In network επεξεργασία φιλτράρισμα και συμπίεση multi-media περιεχομένου. Υψηλή κατανάλωση ενέργειας και υψηλές απαιτήσεις εύρους ζώνης. Ευέλικτη αρχιτεκτονική για την υποστήριξη ποικίλων εφαρμογών. Απαιτείται ενσωμάτωση ποικίλων ασύρματων	Ενίσχυση στις υπάρχουσες εφαρμογές όπως επίβλεψη και εντοπισμός.

		τεχνολογιών. Δύσκολη διασφάλιση QoS λόγω της χωρητικότητας της ζεύξης και των καθυστερήσεων. Αποτελεσματικός crosslayer σχεδιασμός.	
Κινούμενα ΑΔΑ	Το δίκτυο από κινούμενους ασύρματους κόμβους	Καθοδήγηση και έλεγχος κινούμενων κόμβων. Απαίτηση αυτό-οργάνωσης. Συνδυασμός localization και κινητικότητας. Ελαχιστοποίηση ενεργειακής κατανάλωσης. Διατήρηση συνδεσιμότητας δικτύου. In network επεξεργασία δεδομένων. Κατανομή δεδομένων. Διαχείριση κινητικότητας. Διατήρηση επαρκούς sensing κάλυψης.	Επίβλεψη περιβαλλοντικών συνθηκών. Παρακολούθηση σε Στρατιωτικές εφαρμογές. Ανίχνευση στόχων. Αναζήτηση και διάσωση.

2. Σε σχέση με την απόσταση των κόμβων από το σταθμό βάσης, τα ασύρματα δίκτυα αισθητήρων διακρίνονται σε συστήματα επικοινωνίας μονού άλματος (single-hop) ή πολλαπλών αλμάτων (multi-hop). Η πρώτη περίπτωση είναι κατάλληλη για μικρές περιοχές και όλοι οι κόμβοι αποστέλλουν τα δεδομένα απευθείας στο σταθμό βάσης. Το δίκτυο έχει απλούστερη δομή ενώ μπορούν να επιτευχθούν μεγαλύτερα επίπεδα

ασφάλειας. Σε εφαρμογές όπου η περιοχή κάλυψης είναι μεγάλη η επικοινωνία πολλαπλών αλμάτων είναι μονόδρομος. Οι κόμβοι μεταδίδουν τα δεδομένα τους στο σταθμό βάσης μέσω ενδιάμεσων κόμβων οι οποίοι εκτελούν τη λειτουργία της δρομολόγησης αλλά και της συγκέντρωσης δεδομένων.

3. Σε σχέση με το πόσο πυκνά τοποθετημένοι είναι οι κόμβοι και την επεξεργασία που υπόκεινται τα δεδομένα στους κόμβους, μπορούμε να κατηγοριοποιήσουμε τα ασύρματα δίκτυα αισθητήρων σε aggregating και non-aggregating. Στα δίκτυα της δεύτερης κατηγορία οι κόμβοι αποστέλλουν τα δεδομένα τους στον προορισμό χωρίς να τα επεξεργαστούν. Η τακτική αυτή οδηγεί σε χαμηλό υπολογιστικό φόρτο στους ενδιάμεσους κόμβους και υψηλή ακρίβεια στο δίκτυο. Ωστόσο, σε μεγαλύτερα δίκτυα η αυξημένη κίνηση ενδέχεται να επιφέρει συγκρούσεις δεδομένων και καθυστέρηση στο δίκτυο. Τα συγκεκριμένα συστήματα είναι κατάλληλα για δίκτυα με χαμηλή πυκνότητα κόμβων στα οποία απαιτείται υψηλή ακρίβεια από τους χρήστες. Από την άλλη πλευρά, σε δίκτυα με πυκνή κατανομή, κάθε κόμβος βρίσκεται συνήθως πλησιέστερα στους γειτονικούς του, με αποτέλεσμα τη δημιουργία πλεονασμού δεδομένων. Έτσι, απαιτείται υλοποίηση συνεργατικών λειτουργιών συγκέντρωσης και αποστολής δεδομένων για τον περιορισμό του φαινομένου αυτού. Με τον τρόπο αυτό μειώνεται η συμφόρηση του δικτύου και εξοικονομείται ενέργεια, ενώ παράλληλα αυξάνονται οι εκτελούμενοι υπολογισμοί, αυξάνοντας τις απαιτήσεις μνήμης. Ενδείκνυται κατά συνέπεια αυτή η κατηγορία για ασύρματα δίκτυα αισθητήρων μεγάλης κλίμακας, με πυκνή τοποθέτηση κόμβων.
4. Σε σχέση με τον σχεδιασμό του δικτύου μπορούν να διακριθούν σε ντετερμινιστικά ή δυναμικά. Στα ντετερμινιστικά συστήματα η θέση των κόμβων είναι σταθερή ή προσχεδιασμένη, με αποτέλεσμα απλούστερο έλεγχο και εφαρμογή του συστήματος. Ωστόσο, σε πολλές περιπτώσεις η

θέση των κόμβων είναι άγνωστη. Συνεπώς, οι κόμβοι οφείλουν να λειτουργούν με δυναμικό και κατανεμημένο τρόπο, που παρέχει μεγαλύτερη ευελιξία και επεκτασιμότητα, αλλά απαιτεί πολυπλοκότερους αλγορίθμους ελέγχου.

5. Σε σχέση με την προσέγγιση του ελέγχου, τα ασύρματα δίκτυα αισθητήρων ταξινομούνται σε αυτοπροσδιορίσιμα και μη.

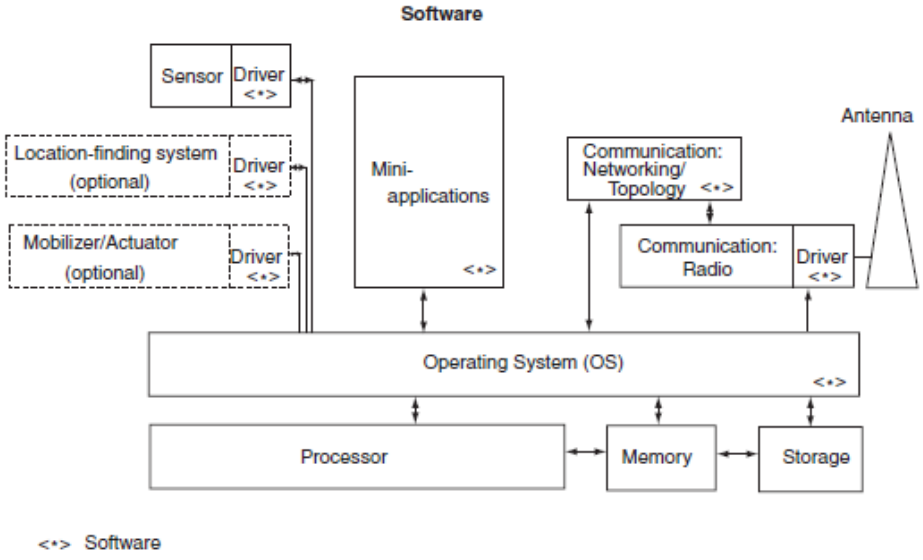
ΠΙΝΑΚΑΣ 4 – [6]

Παράγοντες ταξινόμησης	**Κατηγορίες ΑΔΑ**
Απόσταση από το σταθμό βάσης/κέντρο επεξεργασίας	Single hop ή Multi hop
Εξάρτηση δεδομένων	Aggregating ή non aggregating
Κατανομή κόμβων	Ντετερμινιστικά η δυναμικά
Προσέγγιση ελέγχου	Non self-configurable ή self-configurable
Εφαρμογή	Πολυάριθμες κατηγορίες (Υπέργεια, Υπόγεια κτλ)

4.2 Υποσυστήματα της αρχιτεκτονικής των Ασύρματων Δικτύων Αισθητήρων

Η συνήθης αρχιτεκτονική λογισμικού ενός κόμβου ασύρματου δικτύου αισθητήρων περιλαμβάνει υποσυστήματα όπως καταγράφονται παρακάτω και παρουσιάζονται στην Εικόνα 2 [7]:

1. Κώδικας λειτουργικού συστήματος (middleware): Το λειτουργικό σύστημα αποτελεί ένα περιβάλλον επικοινωνίας λογισμικού και επιπέδου μηχανής του μικροεπεξεργαστή σχεδιασμένο με προτεραιότητα την εξοικονόμηση πόρων. Η χρήση ανοιχτού κώδικα λογισμικών, σχεδιασμένων για ασύρματα δίκτυα αισθητήρων, τα οποία συνήθως χρησιμοποιούν αρχιτεκτονική που επιτρέπει ταχεία εφαρμογή και ελαχιστοποίηση του μεγέθους του κώδικα είναι μια προτεινόμενη λύση.
2. Οδηγοί (drivers) αισθητήρων: είναι τμήματα λογισμικού τα οποία διαχειρίζονται τις βασικές λειτουργίες των πομποδεκτών των κόμβων.
3. Επεξεργαστές επικοινωνίας: είναι υπεύθυνοι για τις λειτουργίες επικοινωνίας, όπως δρομολόγηση, ενταμίευση και προώθηση πακέτων, διατήρηση της τοπολογίας και έλεγχος πρόσβασης στο μέσο, κρυπτογράφηση (encryption)και Forward Error Correction (FEC).
4. Οδηγοί (drivers) επικοινωνίας: είναι τμήματα λογισμικού τα οποία βοηθούν στην κωδικοποίηση στο φυσικό επίπεδο, διαχειρίζονται τις οδηγίες που αφορούν το μέσο μετάδοσης, συμπεριλαμβανομένου του χρονισμού και συγχρονισμού, την κωδικοποίηση σήματος και τη διαμόρφωση.
5. Εφαρμογές επεξεργασίας δεδομένων: είναι βασικές εφαρμογές, συνήθως μικρού μεγέθους, για την επεξεργασία δεδομένων εντός δικτύου (in-network) στον κόμβο.

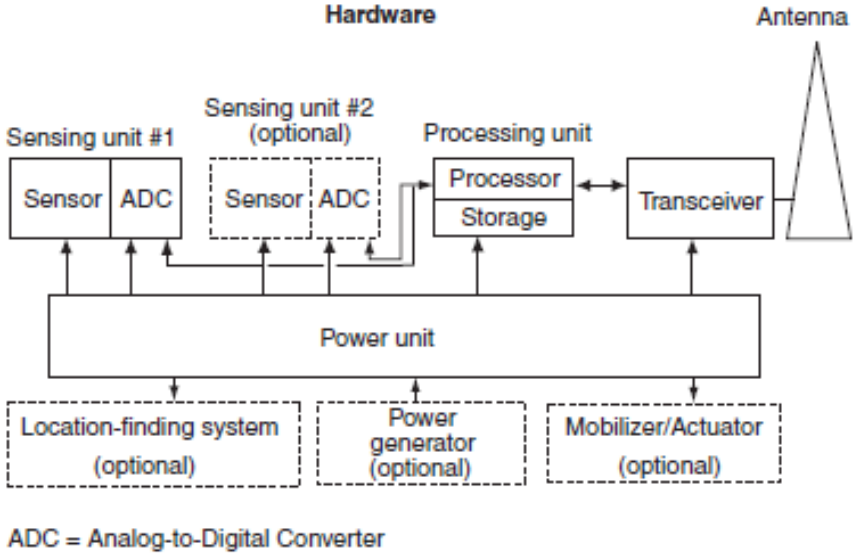


Σχήμα 3 - Βασική αρχιτεκτονική λογισμικού ασύρματου κόμβου

Η βασική αρχιτεκτονική υλικού ενός κόμβου ασύρματου δικτύου αισθητήρων περιλαμβάνει τα παρακάτω υποσυστήματα και παρουσιάζεται αντίστοιχα στην Εικόνα 3 [1],[7]:

1. Υποσύστημα αισθητήρων: παρέχει τη διεπαφή (interface) για τη μετατροπή των σημάτων από το φυσικό περιβάλλον σε ηλεκτρικά σήματα κατάλληλα για επεξεργασία από ηλεκτρονικές συσκευές. Έτσι οι αισθητήρες μετατρέπουν φυσικά μεγέθη σε ηλεκτρικά σήματα.
2. Υποσύστημα επεξεργασίας: είναι η μονάδα επεξεργασίας των δεδομένων. Οι σύγχρονοι μικροελεγκτές που απαρτίζουν τη μονάδα αυτή αποτελούνται από μνήμες τύπου flash και RAM, μετατροπείς αναλογικού σήματος σε ψηφιακό (A/D converters) και ψηφιακά I/O σε ένα ολοκληρωμένο κύκλωμα χαμηλού κόστους. Η επιλογή του ελεγκτή βασίζεται σε παράγοντες όπως η κατανάλωση ενέργειας, οι απαιτήσεις σε τάση λειτουργίας, το κόστος, η υποστήριξη περιφερειακών, ο χρόνος αφύπνισης και η ταχύτητα του.

3. Υποσύστημα επικοινωνιών: αποτελείται από τον πομπό και τον δεκτή. Στη μονάδα αυτή γίνεται η μεγαλύτερη κατανάλωση ενέργειας του συστήματος, επηρεάζοντας την απόδοση του κόμβου αλλά και τη συνολική απόδοση του δικτύου.
4. Υποσύστημα τροφοδοσίας: αποτελείται συνήθως από κάποια μπαταρία ή από κάποια μονάδα μετατροπής ηλιακής, αιολικής ενέργειας. Παρέχει την απαιτούμενη ενέργεια στον κόμβο ενώ η αντικατάσταση ή η φόρτιση της μονάδας αυτής συνήθως δεν είναι εύκολη. Για τον λόγο αυτό η φιλοσοφία των ασύρματων δικτύων αισθητήρων στρέφεται στην μέγιστη εξοικονόμηση ενέργειας.



*Σχήμα 4 - Βασική hardware αρχ*ιτεκτονική ασύρματου κόμβου [7]

4.3 Παράμετροι σχεδίασης των Ασύρματων Δικτύων Αισθητήρων

Η σχεδίαση ενός ΑΔΑ εξαρτάται από πλήθος παραμέτρων που σχετίζονται τόσο με την εφαρμογή του δικτύου όσο όμως και με τις γενικές λειτουργίες ενός κόμβου, τη δυνατότητα αίσθησης, τη δυνατότητα επεξεργασίας, τη δυνατότητα επικοινωνίας, τη συντήρηση, την τοποθέτηση κόμβων (localization), το συγχρονισμό και την ασφάλεια. Παρακάτω γίνεται ανάλυση όλων αυτών των παραμέτρων που παίζουν ρόλο στη σχεδίαση ενός ΑΔΑ:

1. Γενικές λειτουργίες ενός κόμβου: Η εφαρμογή προς υλοποίηση θέτει τις απαιτήσεις στον τρόπο με τον οποίο ο αισθητήρας του κόμβου θα πάρει μετρήσεις από την περιοχή επίβλεψης. Ωστόσο ο σχεδιαστής της εφαρμογής πρέπει να έχει υπόψη του τις παρακάτω γενικές λειτουργίες που μπορεί να εκτελέσει ένας κόμβος [6]:
    a. Μέτρηση ενός φυσικού μεγέθους όπως θερμοκρασία, ατμοσφαιρική πίεση, ποσότητα φωτός, σχετική υγρασία κ.α. σε μια δεδομένη τοποθεσία.
    b. Αντίληψη γεγονότων και εκτίμηση παραμέτρων τους όπως ανίχνευση διέλευσης ενός οχήματος και εκτίμηση της ταχύτητας και κατεύθυνσής του.
    c. Ανίχνευση αντικειμένου και ταυτοποίηση του όπως ανίχνευση εισβολής στην παρατηρούμενη από το δίκτυο περιοχή και πιθανότατα κατηγοριοποίηση αντικειμένου.
2. Δυνατότητα Αίσθησης: Τα ασύρματα δίκτυα αισθητήρων μπορούν να καταταχθούν ανάλογα με τον τρόπο που συλλέγουν και αποστέλλουν δεδομένα σε:
    a. Συνεχή: όταν οι κόμβοι συλλέγουν συνεχώς δεδομένα από το περιβάλλον.

b. Αντιδραστικά (reactive): όταν οι κόμβοι συλλέγουν και αποστέλλουν δεδομένα έπειτα από ανάλογο σήμα που θα πάρουν από τον συντονιστή του δικτύου ή έπειτα από κάποια μεταβολή στον περιβάλλοντα χώρο για την οποία υπάρχει οδηγία αντίδρασης στο λογισμικό του κόμβου.

c. Περιοδικά: όταν οι κόμβοι συλλέγουν δεδομένα κατά περιοδικά χρονικά διαστήματα τα οποία ορίζονται στο λογισμικό της εφαρμογής.

Τα συστήματα τα οποία ενσωματώνουν έναν αριθμό από τις παραπάνω λειτουργίες ονομάζονται υβριδικά. Ανάλογα με τη δυνατότητα αίσθησης των αισθητήρων μπορούν να ταξινομηθούν σε παθητικές συσκευές (μέτρηση σεισμικών δονήσεων, υγρασίας, θερμοκρασίας, ακουστικών κυμάτων), συνήθως χαμηλής ενέργειας, ή ενεργητικές (ραντάρ, σόναρ), που τείνουν να είναι υψηλής ενέργειας συστήματα.

Ο ορισμός της αίσθησης μπορεί να αναλυθεί σε όρους όπως η έκθεση (exposure) (ο χρόνος έκθεσης σε συνδυασμό με την απόσταση του κόμβου από το προς παρατήρηση φαινόμενο), η προσαρμογή (calibration) και η κάλυψη (sensing coverage). Οι έρευνες που γίνονται στο χώρο των ασύρματων δικτύων αισθητήρων επικεντρώνονται στην εξοικονόμηση ενέργειας σε συνάρτηση με τον χώρο κάλυψης, είτε με εύρεση του ελάχιστου αριθμού ενεργών κόμβων για την κάλυψη μιας περιοχής, είτε με προτάσεις τοποθέτησης των κόμβων για κατανεμημένη ανίχνευση σε μεγάλης κλίμακας ασύρματα δίκτυα αισθητήρων. Η συνεχής ενεργή κατάσταση των κόμβων είναι συνήθως μη αποδοτική, ανάλογα πάντα με τις απαιτήσεις που θέτει η κάθε εφαρμογή. Είναι αποδεκτό και συνηθίζεται να υπάρχουν πλεονασματικοί κόμβοι (redundancy), δηλαδή επικαλύψεις στην περιοχή εποπτείας ώστε να επιτυχαίνεται μεγαλύτερη ακρίβεια.

3. Δυνατότητα Επεξεργασίας: Η μονάδα επεξεργασίας δεδομένων ενός ασύρματου κόμβου αποτελείται από τη μνήμη και τον επεξεργαστή, ο οποίος είναι προγραμματιζόμενος και εκτελεί βασικούς υπολογισμούς επεξεργασίας σήματος και πιθανότατα διεργασίες συσχέτισης δεδομένων. Ο σχεδιασμός αυτής της μονάδας είναι προσανατολισμένος σε λύσεις όπου το κόστος και η κατανάλωση ενέργειας θα κρατηθούν χαμηλά. Επεξεργασίες δεδομένων που πιθανόν να απαιτηθούν από την εφαρμογή είναι:

    a. Η συγχώνευση δεδομένων (data fusion): ένα η περισσότερα πακέτα που έχουν ληφθεί συνδυάζονται για την δημιουργία ενός μεγαλύτερου πακέτου με σκοπό την εξοικονόμηση ενέργειας
    b. η συμπίεση δεδομένων
    c. η επεξεργασία κώδικα ασφάλειας

    Η επεξεργασία των δεδομένων, όπως έχει ήδη αναφερθεί, μπορεί να υλοποιείται από κάθε κόμβο χωριστά ή με συνεργασία των κόμβων προσεγγίζοντας κατανεμημένα συστήματα. Στην πρώτη περίπτωση οι κόμβοι διεξάγουν υπολογισμούς τοπικά και αποστέλλουν ένα υποσύνολο των διατιθέμενων δεδομένων ή/και των επεξεργασμένων πληροφοριών, ενώ στη δεύτερη η επεξεργασία υλοποιείται σε διαδοχικά επίπεδα, έως ότου η πληροφορία που αφορά τα γεγονότα ενδιαφέροντος καταφθάσει στο σημείο διαχείρισης [6].

4. Δυνατότητα Επικοινωνίας: Η επικοινωνία σε ένα ασύρματο δίκτυο αισθητήρων μπορεί να χωριστεί σε επικοινωνία υποδομής και επικοινωνία εφαρμογών. Η επικοινωνία υποδομής είναι η επικοινωνία που πραγματοποιείται για τον καθορισμό, την διατήρηση και την βελτιστοποίηση της λειτουργίας του δικτύου, του οποίου η τοπολογία πιθανόν να μεταβάλλεται συχνά. Σε ένα στατικό δίκτυο ασύρματων

αισθητήρων απαιτείται μια αρχική προεργασία για τη δημιουργία του δικτύου ενώ αργότερα η επικοινωνία υποδομής είναι απαραίτητη μόνο για τον επαναπροσδιορισμό του. Στα δίκτυα πουπεριλαμβάνουν κινούμενους κόμβους, είναι απαραίτητη η επικοινωνία υποδομής γιατην εύρεση των διαδρομών επικοινωνίας και τονεπαναπροσδιορισμό του δικτύου. Όσο αφορά την επικοινωνία εφαρμογών, διακρίνονται οι παρακάτω μορφές οι οποίες αναπαριστώνται και στην Εικόνα 4 [6]:

a. Άμεση σύνδεση (direct connected WSN): είναι η άμεση επικοινωνία του κάθε κόμβου με το δέκτη δεδομένων (data sink). Λόγω του μεγάλου αριθμού κόμβων και του πιθανότητα περιορισμένου εύρους μετάδοσης κάθε κόμβου εξαιτίας ενεργειακών περιορισμών, είναι γενικά ασύμφορη, έως και αδύνατη. Συνεπώς αυτή η μορφή επικοινωνίας δεν ενδείκνυται για ασύρματα δίκτυα αισθητήρων ευρείας κλίμακας.

b. Peer to peer πολλαπλών αλμάτων (multi-hop) επικοινωνία: η επικοινωνίαπολλαπλών αλμάτων σε μικρές αποστάσεις οδηγεί σε μικρότερη κατανάλωση ενέργειας, σε σχέση με μια αντίστοιχη μεγάλων αλμάτων (large-hop) μετάδοση μεταξύ ενός ζεύγους αποστολέα παραλήπτη.

c. Επίπεδη ad hoc multi-hop επικοινωνία: στην επικοινωνία αυτού του τύπου κάποιοι κόμβοι έχουν την αρμοδιότητα δρομολόγησης πακέτων, εκτός από την αίσθηση και αποστολή των δικών τους δεδομένων. Η μορφή αυτή παρέχει εξοικονόμηση ενέργειας στην επικοινωνία, όμως οι κόμβοι που βρίσκονται πιο κοντά στο δέκτη δεδομένων (data sink) είναι υπεύθυνοι για τη δρομολόγηση προς αυτόν, των πακέτων των υπόλοιπων κόμβων, με αποτέλεσμα, την ανομοιόμορφη κατανάλωση της ενέργειάς τους σε σχέση μετους υπόλοιπους κόμβους.

d. Συστάδες πολλαπλών αλμάτων (cluster based multi-hop) επικοινωνία: η μορφή της επικοινωνίας αυτού του τύπου βασίζεται σε συστάδες που συνθέτουν οι κόμβοι και ορίζονται σύμφωνα με κανόνες ‘’ένας επικεφαλής για κάθε συστάδα’’. Εκτός από τις συστάδες ενός επιπέδου, υπάρχουν και σχήματα επικοινωνίας τα οποία βασίζονται σε συστάδες οργανωμένες κατά ιεραρχία, όπου οι επικεφαλείς συστάδων (cluster heads) χαμηλότερου επιπέδου επικοινωνούν με τους επικεφαλείς συστάδων υψηλότερου επιπέδου. Η συγχώνευση δεδομένων (data fusion) τοπικά στους επικεφαλείς συστάδων μειώνει τον όγκο της αποστελλόμενης πληροφορίας στο δέκτη δεδομένων (data sink) με επακόλουθη μείωση της καταναλισκόμενης ενέργειας. Μειονέκτημα του σχήματος είναι ότι όγκος των δεδομένων επιβαρύνει τους επικεφαλείς συστάδων, με αποτέλεσμα την ασύμμετρη μείωση των ενεργειακών τους αποθεμάτων σε σχέση με τους υπόλοιπους κόμβους και τον αυξημένο φόρτο στους επικεφαλείς συστάδων ανώτερων επιπέδων.

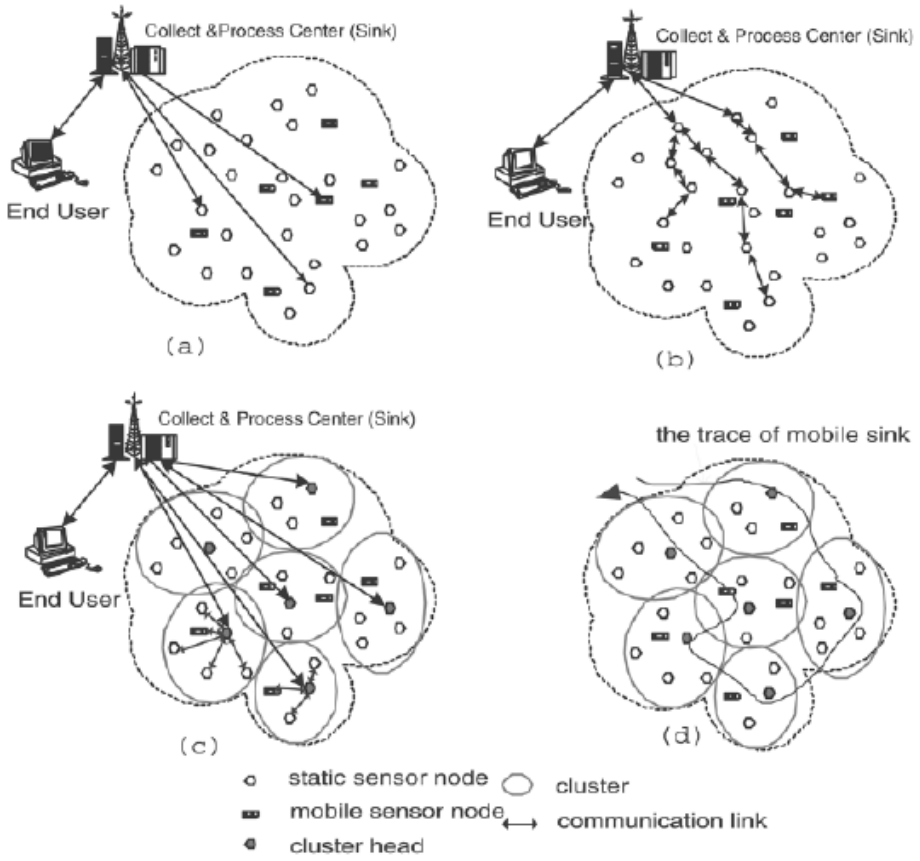
Τα ασύρματα δίκτυα αισθητήρων ταξινομούνται βάση του τρόπου αποστολής δεδομένων ως εξής:

a. Συνεχή: στα δίκτυα αυτά οι κόμβοι συλλέγουν και αποστέλλουν αδιαλείπτως δεδομένα προς τον δέκτη δεδομένων (data sink).

b. Κατ’ αίτηση (on demand): οι κόμβοι αποστέλλουν δεδομένα έπειτα από ανάλογο σήμα που θα λάβουν από τον συντονιστή του δικτύου.

c. Καθοδηγούμενα από γεγονότα: οι κόμβοι αποστέλλουν δεδομένα αφού συμβεί κάποια μεταβολή στον περιβάλλοντα χώρο.

d. Προγραμματισμένα: οι κόμβοι αποστέλλουν δεδομένα βάση συνθηκών προκαθορισμένων στο λογισμικό της εφαρμογής.



Σχήμα 5 - Μορφές επικοινωνίας ΑΔΑ [7]

5. Συντήρηση: Ο όρος αυτός αναφέρεται στα ασύρματα δίκτυα αισθητήρων τα οποία μπορούν να εκτελέσουν λειτουργίες όπως ο αυτοπροσδιορισμός, η αυτοπροστασία και η επαναφορά χωρίς να απαιτείται ουσιαστική συμμετοχή του ανθρώπινου παράγοντα. Η διαδικασία συντήρησης αφορά την ανίχνευση αποτυχιών ή την μείωσης της απόδοσης του δικτύου, καθώς και τις διαδικασίες διάγνωσης και επανόρθωσης. Η ανίχνευση αλλαγών στην κατάσταση του δικτύου παρέχει ευελιξία, σθεναρότητα, ανεξαρτησία και δυνατότητα βελτιστοποίησης της συμπεριφοράς του δικτύου. Οι τύποι συντήρησης διακρίνονται στους εξής [6]:

a. corrective: το δίκτυο επανορθώνει τις αποτυχίες
b. adaptive: το δίκτυο προσαρμόζεται στις μεταβολές
c. preventive: το δίκτυο μαθαίνει να αναμένει την επίδραση των αλλαγών
d. proactive: το δίκτυο μαθαίνει να επεμβαίνει ώστε να προλαμβάνει τις αποτυχίες

Ένα παράδειγμα συντήρησης στα ασύρματα δίκτυα αισθητήρων αφορά την πυκνότητα των κόμβων του δικτύου. Σε περίπτωση που δεν απαιτείται υψηλή πυκνότητα κόμβων μπορεί να πραγματοποιηθεί παροδική απενεργοποίηση ορισμένων κόμβων.

6. Τοποθέτηση κόμβων: Τα ασύρματα δίκτυα αισθητήρων μπορούν να ταξινομηθούν σε δομημένα ή μη με κριτήριο αν υπήρξε προσχεδιασμένη ή όχι τοποθέτηση των κόμβων. Συνήθως ένα μη δομημένο ασύρματο δίκτυο αισθητήρων αποτελείται από ένα πυκνό σύνολο κόμβων, οι οποίοι είναι τυχαία τοποθετημένοι στον χώρο επίβλεψης. Αφού εγκατασταθεί το δίκτυο, εκτελεί τις λειτουργίες της επιτήρησης και της αναφοράς δεδομένων χωρίς καμία παρέμβαση. Σε ένα δομημένο ασύρματο δίκτυο αισθητήρων, το σύνολο των κόμβων ή μόνο κάποιοι από αυτούς τοποθετούνται με προσχεδιασμένο τρόπο. Τα δομημένα δίκτυα έχουν πλεονέκτημα στην ευκολία συντήρησης στο κόστος διαχείρισης, καθώς επίσης χρειάζονται λιγότεροι κόμβοι σε συγκεκριμένες θέσεις για την κάλυψη μιας περιοχής. Αντίθετα με την τυχαία τοποθέτηση των κόμβων μπορεί να μείνουν ακάλυπτες περιοχές ή να υπάρξουν πλεονασματικοί κόμβοι. Το πρόβλημα καθορισμού του σημείου τοποθέτησης των κόμβων ονομάζεται localization. Μέθοδοι για την επίλυση του προβλήματος είναι το σύστημα GPS, οι beacon κόμβοι, localization βάσει εγγύτητας αλλά και κάποιοι αλγόριθμοι [3].

7. Συγχρονισμός: Για να υπάρξει υποστήριξη χρονικά συσχετισμένων δεδομένων στο δίκτυο από τους διαφορετικούς κόμβους του, απαιτείται η ύπαρξη μιας μεθόδου συντονισμού που θα παρέχει μεγάλη ακρίβεια. Υπάρχουν αρκετές μέθοδοι άμεσου ή έμμεσου συγχρονισμού. Πιθανά σφάλματα στο χρονισμό των κόμβων κάνουν αναξιόπιστο το συσχετισμό των δεδομένων, προσβάλλοντας έτσι και τη συνολική αξιοπιστία του δικτύου [3].

8. Ασφάλεια: Η ύπαρξη ασφάλειας στα ασύρματο δίκτυα αισθητήρων επιβαρύνει τους κόμβους με την εκτέλεση πολύπλοκων αλγόριθμων αυθεντικότητας και κρυπτογράφησης. Λόγω πιθανώνυποκλοπών και παρεμβολών στο ασύρματο κανάλι μετάδοσης των ΑΔΑ, η κρυπτογράφηση κάθε εκπομπής αλλά και η πρόβλεψη κατά την κατασκευή και τοποθέτηση των κόμβων είναι απαραίτητα, ώστε να παραμείνουν τα δεδομένα αναλλοίωτα και να εξασφαλίζεται η αντοχή στη φυσική παραβίαση (tamper resilience) [3].

Η χρήση τεχνικών αυθεντικότητας και κρυπτογράφησης επιδρούν αρνητικά τόσο στην κατανάλωση ισχύος όσο και στο διαθέσιμο εύρος ζώνης του δικτύου, ενώ η ενσωμάτωση επιπλέον bits στα μεταφερόμενα πακέτα, τα οποία περιέχουν τις πληροφορίες αυθεντικότητας, μειώνουν τον αριθμό των πραγματικών δεδομένων που μπορούν να μεταφερθούν από ένα κόμβο [1].

4.4 Σχεδιαστικοί περιορισμοί των Ασύρματων Δικτύων Αισθητήρων

Κατά την σχεδίαση των ασύρματων κόμβων πρέπει να ληφθούν υπόψη ορισμένοι περιορισμοί που απορρέουν από τις ιδιαιτερότητες των ασύρματων δικτύων αισθητήρων. Τα σχεδιαστικά αυτά ζητήματα περιγράφονται παρακάτω[6][7]:

1. Περιορισμένοι πόροι (υπολογιστική ισχύς, μνήμη, ενέργεια, εύρος ζώνης): Συνήθως οι κόμβοι τοποθετούνται σε περιοχές όπου είναι δύσκολη η πρόσβαση τους, με αποτέλεσμα να είναι δύσκολη και η αντικατάσταση της πηγής ενέργειας. Αυτό έχει ως ο αποτέλεσμα ο χρόνος ζωής του κάθε κόμβου να καθορίζεται συνήθως από τη ζωή της μπαταρίας του. Η ενέργεια του κόμβου καταναλώνεται κυρίως κατά την αποστολή και λήψη δεδομένων με αποτέλεσμα να απαιτείται χρήση πρωτοκόλλων εξοικονόμησης ενέργειας για την επέκταση της ζωής του συστήματος. Επιπλέον, αλγόριθμοι χαμηλής πολυπλοκότητας οδηγούν στη μείωση του υπολογιστικού χρόνου και της καταναλισκόμενης ισχύος. Επίσης αποδοτικές τεχνικές στον καθορισμό του εύρους ζώνης επιταχύνουν την παράδοση των δεδομένων.
2. Δυναμική τοπολογία και περιβάλλον λειτουργίας: Σε ένα ασύρματο δίκτυο αισθητήρων η τοπολογία του ενδέχεται να μεταβάλλεται, λόγω της αναξιοπιστίας κάποιων κόμβων του. Ένας κόμβος μπορεί να παρουσιάσει σφάλματα ή και να σταματήσει να λειτουργεί, χωρίς να ενημερώσει τους υπόλοιπους κόμβους, λόγω εξάντλησης της ενέργειάς του. Επιπλέον, καινούριοι κόμβοι είναι πιθανό να τοποθετηθούν στην περιοχή επίβλεψης. Επίσης, καθώς το περιβάλλον όπου είναι τοποθετημένοι οι κόμβοι είναι ευμετάβλητο, μπορεί να προκληθεί δυσλειτουργία των κόμβων ή αχρήστευση των ήδη συγκεντρωμένων

πληροφοριών τους. Για την αντιμετώπιση αυτών των συνθηκών ενδείκνυται η υποστήριξη ευελιξίας και επεκτασιμότητας (flexibility scalability) μέσω της ομαδοποίησης (clustering) και της επικοινωνίας πολλαπλών αλμάτων (multi-hop).

3. Πυκνή και τυχαία τοποθέτηση των κόμβων: Τα ασύρματα δίκτυα αισθητήρων αποτελούνται από μεγάλο αριθμό κόμβων, συνήθως τυχαία τοποθετημένων σε δυσπρόσιτες περιοχές. Για την εξοικονόμηση ενέργειας ο κάθε κόμβος δε βρίσκεται σε συνεχή ενεργή κατάσταση αλλά εναλλάσσει την λειτουργία του ανάλογα με τις απαιτήσεις σε: off, sleep, idle, εκπομπής, λήψης και αστοχίας. Το δίκτυο πρέπει λοιπόν να δημιουργεί συνδέσεις αυτόνομα, ανεξαρτήτως δηλαδή της κατάστασης των κόμβων του. Επιπλέον ενδείκνυται η ανακατεύθυνση των πακέτων μέσω διαδρομών, όπου οι κόμβοι διαθέτουν μεγαλύτερα αποθέματα ενέργειας, ώστε να επιτυγχάνεται η συμμετρική εξασθένηση ενέργειας του δικτύου. Όλα τα παραπάνω συνιστούν το λεγόμενο αυτοπροσδιορισμό του δικτύου (self configuration)

4. Ad hoc αρχιτεκτονική και λειτουργία χωρίς ανθρώπινη παρέμβαση: Η μη ύπαρξη δομής και η λειτουργία χωρίς την ανθρώπινη παρέμβαση απαιτεί από το δίκτυο να πραγματοποιεί συνδέσεις και να τις συντηρεί αυτόνομα.

5. Πλεονασμός δεδομένων: Η πυκνή τοποθέτηση των κόμβων οδηγεί σε φαινόμενα πλεονασμού δεδομένων. Για την αποφυγή διακίνησης επιπλέον όγκου δεδομένων από τους κόμβους απαιτείται η συνεργατική επεξεργασία των πληροφοριών, συγχώνευση δεδομένων (data fusion) και υπολογισμοί εντός του δικτύου αισθητήρων. Αντί για την άμεση αποστολή των δεδομένων προς τον δέκτη δεδομένων, ο κάθε κόμβος επεξεργάζεται μερικώς, με απλούς υπολογισμούς, τα δεδομένα και αποστέλλει μόνο τα αποτελέσματα.

6. Ασύρματο μέσο επιρρεπές σε σφάλματα: Πολλές φορές το περιβάλλον όπου τοποθετούνται οι κόμβοι έχει υψηλό θόρυβο, με αποτέλεσμα να

παρουσιάζονται φαινόμενα εξασθένησης του σήματος, χαμηλής αξιοπιστίας και QoS, αλλά και περιορισμένης ασφάλειας. Σε αυτούς τους χώρους εφαρμογής απαιτείται η εξακρίβωση των δεδομένων σε κάθε επίπεδο του δικτύου και οι λειτουργίες συντήρησης.

7. Ανάγκη ειδικών μηχανισμών δρομολόγησης και μετάδοσης δεδομένων: Η ύπαρξη διαφορετικών αναγκών δρομολόγησης από τα παραδοσιακά δίκτυα απαιτεί διαφορετικά πρωτόκολλα και σχεδιασμό δικτύου. Μπορούμε να χωρίσουμε τις εξής κατηγορίες σχεδιασμού δικτύων: εστιασμένα στα δεδομένα (data centric), εστιασμένα στην ταυτότητα των κόμβων (address centric), ιεραρχικά με επικοινωνία πολλαπλών αλμάτων (cluster based),δομημένης τοποθέτησης κόμβων (location based) και προσανατολισμένα στην παροχή εξασφαλισμένης ποιότητας επικοινωνίας (QoS oriented).

4.5 Κόστος Παραγωγής των Ασύρματων Δικτύων Αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται από πολλούς κόμβους, με αποτέλεσμα το κόστος του κόμβου να επηρεάζει σημαντικά την διαμόρφωση του συνολικού κόστους του δικτύου. Πρέπει το κόστος του κάθε κόμβου να κρατηθεί χαμηλά ώστε το συνολικό κόστος του δικτύου να είναι μικρότερο από το κόστος ενός συμβατικού δικτύου αντίστοιχων δυνατοτήτων.

Ένας επιπλέον παράγοντας που επηρεάζει το τελικό κόστος είναι η ευκολία ανάπτυξης του δικτύου. Η ανάπτυξη του δικτύου, στο χώρο λειτουργίας του, πρέπει να είναι εφικτή και από μη εξειδικευμένο προσωπικό. Μια τέτοια δυνατότητα προϋποθέτει την ικανότητα αυτορρύθμισης από το ίδιο το δίκτυο. Στην ιδεατή περίπτωση, το σύστημα θα πρέπει να είναι ικανό να ρυθμίζεται αυτόματα, ανεξάρτητα από την κατάσταση που επικρατεί στο περιβάλλον όπου τοποθετείται [1].

5 Πρότυπα και τοπολογία Ασύρματων Δικτύων Αισθητήρων

Ο οργανισμός της IEEE (Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών) αναπτύσσεται ταχύτατα δημιουργώντας διαρκώς νέα πρωτόκολλα οδηγιών οδηγώντας με αυτό τον τρόπο στην γιγάντωση της βιομηχανίας κατασκευαστών αντίστοιχων συσκευών, όπου πλέον κρίνεται αναγκαία η διασφάλιση της συμβατότητας μεταξύ των διάφορων συσκευών για την προστασία του αγοραστή. Οι οικογένειες πρωτοκόλλων που αναπτύσσονται αποτελούν το καθιερωμένο πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων. Το πρώτο πρότυπο ασύρματων τοπικών δικτύων είναι το IEEE 462.11 και όπως προαναφέραμε είναι υπεύθυνο για τον έλεγχο πρόσβασης στα ασύρματα δίκτυα και υιοθετήθηκε το 1997. Εκτός των παραπάνω εκδόσεων έχουν προταθεί και κάποιες άλλες επεκτάσεις τους, οι οποίες όμως δεν έχουν υλοποιηθεί σε εμπορικά προϊόντα και έχουν περισσότερο ακαδημαϊκό ενδιαφέρον (IEEE 462.11 WG: 462.11e ή QoS, 462.11n). Όταν γίνεται αναφορά στην "τοπολογία του 462.11", ουσιαστικά εννοούνται στοιχεία που αλληλεπιδρούν ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο το οποίο παρέχει τη δυνατότητα μετακίνησης των σταθμών χωρίς να γίνεται αντιληπτή στα ανώτερα στρώματα. Κατ’ ‘όπως γίνεται αντιληπτό υπάρχει συσχέτιση της τοπολογίας και των προτύπων, η ανάλυση των οποίων θα πραγματοποιηθεί σε αυτό το κεφάλαιο.

5.1 Τοπολογία Ασύρματων Δικτύων Ασφαλείας

Ένα ΑΔΑ αποτελείται, βασικά, από δύο δομικά στοιχεία. Αυτά που παράγουν πληροφορία, όπως είναι ο κάθε κόμβος στο δίκτυο, και ονομάζονται πηγές (sources) και από τα στοιχεία που συλλέγουν την πληροφορία από τις πηγές και ονομάζονται αποδέκτες (sinks), σε κάποια συγγράμματα συναντώνται και

ως καταβόθρες. Η διασύνδεση και ο τρόπος που επικοινωνούν μεταξύ τους οι πηγές και οι αποδέκτες καθορίζουν την τοπολογία του δικτυού. Υπάρχουν τέσσερεις δημοφιλής τοπολογίες [8,9]:

1. **Peer-to-Peer** (Ίσο προς ίσο): Ένα peer to peer δίκτυο είναι ένα δίκτυο που επιτρέπει στους κόμβους του να μοιράζονται ισοδύναμα τους πόρους τους και ταυτόχρονα μπορεί να χρησιμοποιήσει την συνολική επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το bandwidth για υλοποίηση μιας εφαρμογής. Οι κόμβοι μεταξύ τους είναι ίσος προς ίσο, έχουν δηλαδή τα ίδια δικαιώματα στο δίκτυο και ο κάθε κόμβος έχει πρόσβαση στους υπολοίπους κόμβους. Τα δίκτυα peer-to-peer χωρίζονται σε τρεις κατηγορίες:
    a. Συγκεντρωτικά p2p δίκτυα:Στα συγκεντρωτικά p2p δίκτυα (συχνά 1 ης γενιάς p2p δίκτυα) υπάρχει ένα κεντρικός κόμβος, ονομαζόμενος index server ο οποίος κρατάει κατάσταση ποιος κόμβος έχει και τι. Άρα αν κάποιος κόμβος επιθυμεί κάτι από ένα άλλο κόμβο θα πρέπει να αιτηθεί στον index server ο οποίος αφού βρει ποιος το έχει μετά δημιουργεί μια σύνδεση μεταξύ του αιτητή και αυτού που έχει το δεδομένο.
    b. Αποκεντρικά p2p δίκτυα: Σε αυτή τη λογική κάθε κόμβος είναι servent (κόμβοι που ταυτόχρονα είναι και server και client, λέξη προκύπτει από την συνένωση των client και server) και έτσι ταυτόχρονα μπορεί να εξυπηρετήσει ή να εξυπηρετηθεί. Σε αυτή την περίπτωση μόλις ένα κόμβος εισέλθει στο δίκτυο θα πρέπει να δηλώσει την παρουσία του στους υπόλοιπους κόμβους που είναι κοντά του και αυτοί με την σειρά τους στο συνολικό δίκτυο.
    c. p2p δίκτυα 3ης γενιάς: Το βασικό χαρακτηριστικό της τοπολογίας είναι η ανωνυμία, έχουν αποκεντρικό χαρακτήρα η φιλοσοφία αυτών των δικτύων είναι η υψηλή βιωσιμότητα στο συνεχή διαμοιρασμό πληροφορίας και στην κωδικοποίηση της έτσι, ώστε

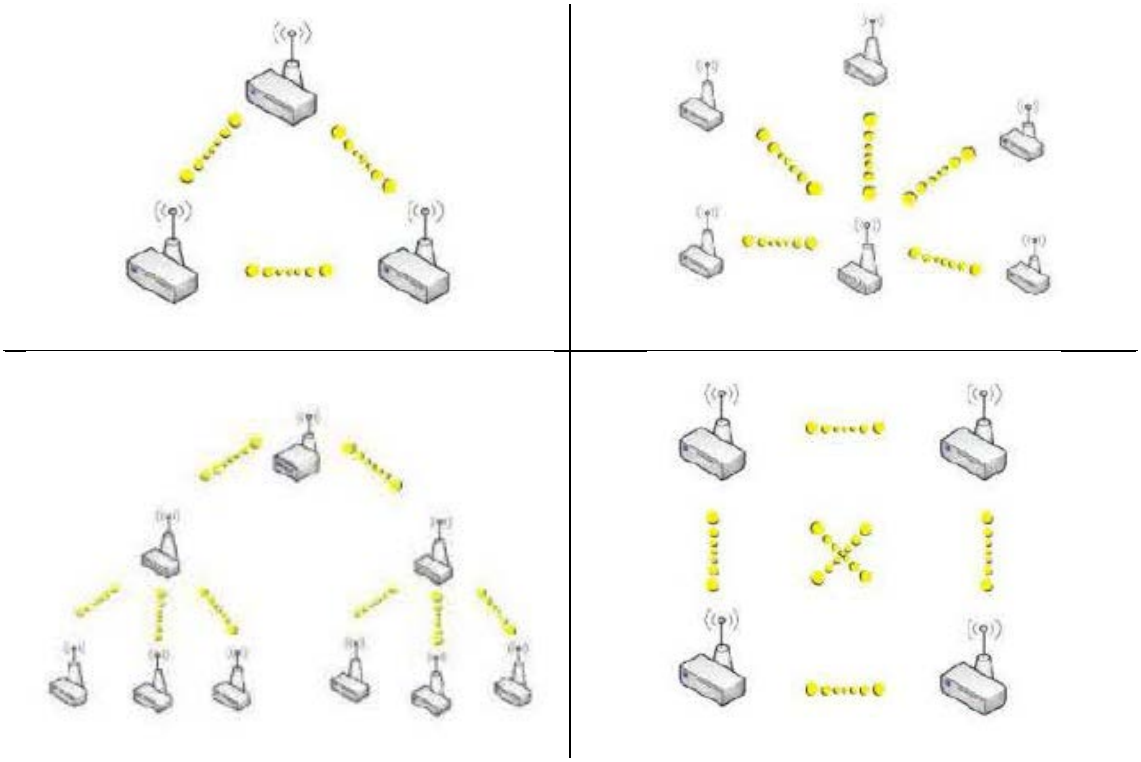
να μην μπορεί ο κόμβος να αποκτήσει έλεγχο σε αυτήν, εφόσον δεν παραχωρηθούν δικαιώματα.

2. **Star** (αστέρα): Είναι μια από τις πιο διαδεδομένες τοπολογίες διασύνδεσης υπολογιστών. Σε κάθε τέτοια τοπολογία υπάρχει ο κεντρικός κόμβος ο οποίος λειτουργεί σαν μεσολαβητής και μεταφέρει μηνύματα μεταξύ των κόμβων που βρίσκονται γύρω του μέσω αυτού. Η συγκεκριμένη τοπολογία μειώνει την πιθανότητα σφάλματος δικτύου ενώνοντας όλους τους κόμβους με τον κεντρικό κόμβο. Ο κεντρικός κόμβος μεταδίδει (broadcast) ό.τι δεδομένα λαμβάνει, με αποτέλεμσα όλοι οι κόμβοι λαμβάνουν το μήνυμα που στέλνει ένας κόμβος(σε κάποιες περιπτώσεις και ο ίδιος) και είναι ευθύνη του λαμβάνοντα κόμβου να αποφασίσει εάν το πακέτο πληροφοριας που λαμβάνει είναι δικό του και πώς θα το αξιοποιήσει. Σε περίπτωση που ο ένας κόμβος (πλην του κεντρικού) καταρρεύσει το δίκτυο δεν καταστρέφεται παρά μόνο απομονώνεται ο συγκεκριμένος κόμβος. Πέρα αυτού του πλεονεκτήματος η απόδοση είναι επίσης καλύτερη, λόγω του ότι για τη μεταφορά ενός μηνύματος μεταξύ δύο κόμβων θα παρεμβάλλονται πάντα 3 συσκευές (αποστολέας ► κεντρικός►παραλήπτης) και δύο μέσα μεταφοράς (καλώδιο, ασύρματο κτλ). Η κεντρικοποιήση που προσφέρει η τοπολογία αστέρα κάνει εύκολη την διαδικασία επέκτασης του δικτύου αφού μόνο ο κεντρικός κόμβος θα χρειάζεται να ενημερωθεί κατά κάποιο τρόπο. Επίσης αφού όλη η πληροφορία περνάει από τον κεντρικό κόμβο ο έλεγχος σχετικά με το τι είδους πληροφορία διακινείται στο δίκτυο είναι σαφώς ευκολότερη. Σημαντικό πλεονέκτημα είναι ακόμα η απλότητα της τοπολογίας που κάνει εύκολη την δημιουργία star networks, τη συντήρηση κτλ. Ένα τέτοιο δίκτυο, ωστόσο έχει και αρκετά μειονεκτήματα όπως την εξ' ολοκλήρου εξάρτηση από το κεντρικό κόμβο από την πηγάζουν πολλά προβλήματα: η επέκταση του δικτύου μπορεί να γίνει για παράδειγμα μέχρι το σημείο που μπορεί να εξυπηρετεί ο κεντρικός κόμβος.

3. **Tree** (Δέντρου): Σε αυτή την μορφή πρώτο στην ιεραρχία βρίσκουμε το root note, πιο κάτω από αυτό είναι τα central hub τα οποία το καθένα ξεχωριστά δημιουργεί μια δική του τοπολογία τύπου αστέρα. Συνεπώς, αυτή η τοπολογία είναι μια συνδυαστική τοπολογία των δυο προαναφερθέντων τοπολογιών και για αυτό ονομάζεται και hybrid (υβριδικό). Τα πλεονεκτήματα αυτής της τοπολογίας είναι πως είναι μια πολύ διαδεδομένη τοπολογία, υποστηρίζεται από πολλούς κατασκευαστές, η διασύνδεση δυο σημείων είναι εφικτή, όλοι οι κόμβοι έχουν πρόσβαση στο δικό τους μικρό δίκτυο αλλά και στο μεγαλύτερο δίκτυο που υλοποιείται από τους «γονείς» τους. Τα μειονεκτήματα είναι το γεγονός πως εφόσον ολόκληρο το δίκτυο βασίζεται στον main κόμβο αν αυτός καταρρεύσει τότε θα ακολουθήσει η κατάρευση ολόκληρου του δίκτυου και η δυσκολία εγκατάστασης λόγω της πολυπλοκότητάς της τοπολογίας.
4. **Mesh** (Πλέγματος): Σε αυτή την τοπολογία ο κάθε κόμβος δεν παραλαβμάνει και μεταδίδει τα δικά του δεδομένα μόνο αλλά ταυτόχρονα συνεργάζεται με τους υπόλοιπους κόμβους και λειτουργεί σαν συνδετικός κρίκος για να υπάρξει συνολική μεταφορά δεδομένων στο δίκτυο. Ο σχεδιασμός ενός τέτοιου δικτύου μπορεί να επιτευχθεί με δύο τρόπους: με καθορισμένη δρομολόγηση ή με «πλημμύρισμα» του δικτύου. Με την τεχνική δρομολόγησης τα δεδομένα ξέρουν εκ των προτέρων ότι θα ακολουθήσουν συγκεκριμένο μονοπάτι και για να φτάσουν στο τελικό προορισμό ίσως χρειαστεί να περάσουν μέσα από άλλους κόμβους κάνοντας κάθε φορά μικρά άλματα (hops). Ώστε να είναι υλοποιήσιμη αυτή η τεχνική θα πρέπει να λειτουργούν συνεχώς αλγόριθμοι που θα αποκαθιστούν καινούργια μονοπάτια και θα «θεραπεύουν» το δίκτυο σε περίπτωση καταστροφής κόμβων. Στην περίπτωση του «πλημμυρίσματος» του δικτύου, ο κάθε κόμβος κάνει μεταδίσει την προς μεταφορά πληροφορία και στη συνέχεια οι παραλήπτες αναμεταδίδουν τα δεδομένα με αποτέλεσμα το δίκτυο να

κατακλίζεται με τη συγκεκριμένη πληροφορία , η οποία κάποια στιγμή σίγουρα θα καταλήξει στον επιθυμητό κόμβο (αν βέβαια υπάρχει επικοινωνία αυτού το κόμβου με το υπόλοιπο δίκτυο) με αυτόν τον τρόπο. Fully connected network ονομάζεται ένα δίκτυο στο οποίο όλοι οι κόμβοι του είναι διασυνδεδεμένοι μεταξύ τους. Τέλος, τα mesh δίκτυα μπορούν να θεωρηθούν ως ένα είδος ad hoc network.

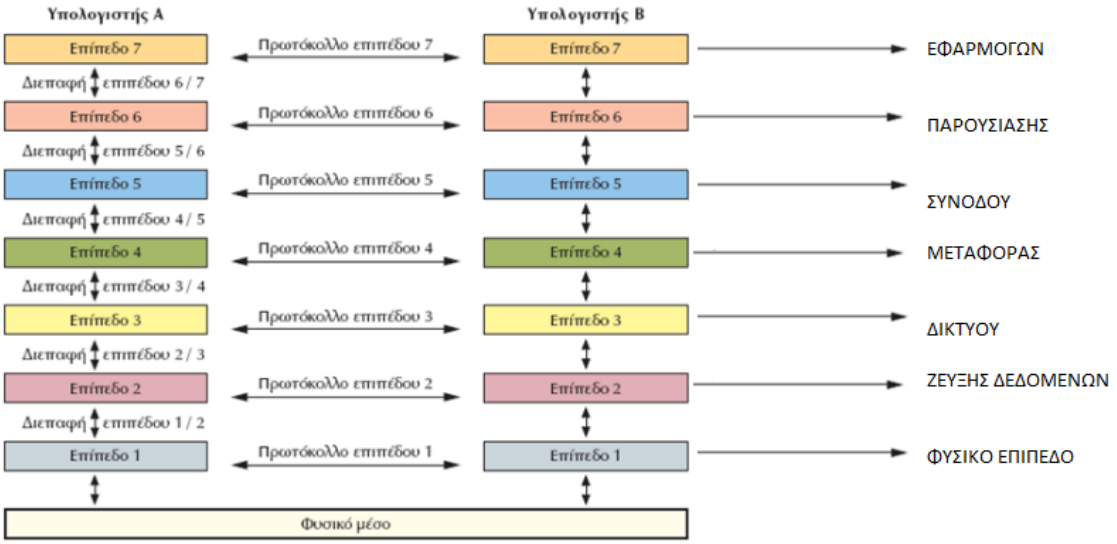
Στην Εικόνα 6 ακολουθεί η σχηματική επεξήγηση όλων των προαναφερθάντων τοπολογιών.



Σχήμα 6 – Τοπολογία α. ίσο-προς-ίσο, β. αστέρα, γ.δέντρου , δ.πλέγματος[8]

5.2 Μοντέλο OSI

Δεν θα μπορούσε να ολοκληρωθεί η τοπολογία δικτύου χωρίς να γίνει αναφορά στο μοντέλο OSI. Το μοντέλο OSI (Open Systems Interconnection) είναι ένα πρότυπο μοντέλο επτά επιπέδων και καθορίζει την διασύνδεση μεταξύ των δικτύων. Το μοντέλο OSI υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια κατακόρυφη στοίβα 7 επιπέδων, όπως φαίνεται και στην Εικόνα 7, όπου για κάθε στρώμα ένα συγκεκριμένο πρωτόκολλο είναι υπεύθυνο να παρέχει στο προηγούμενο και στο επόμενο στρώμα την αναμενόμενη μορφή δεδομένων. Συγκεκριμένα, τα επίπεδα έχουν ως εξής [I] :



Σχήμα 7 – Επεξήγηση μοντέλου OSI [I]

1. **Physical Layer** (Φυσικό επίπεδο): Στο χαμηλότερο επίπεδο του μοντέλου βρίσκεται το hardware, όπου γίνεται η δυαδική μετάδοση των δεδομένων (ενσύρματη, ασύρματη ...). Σε αυτό το επίπεδο υπάρχουν συσκευές όπως διανεμητές (Hub), επαναλήπτες(repeaters), κάρτες

δικτύου, προσαρμοστείς δίαυλου. Βασικές λειτουργίες που εκτελούνται σε αυτό το στρώμα είναι:

a. Η έναρξη ή ο τερματισμός της ηλεκτρικής διασύνδεσης μεταξύ δύο επικοινωνιακών συσκευών.
b. Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων έτσι ώστε να είναι εφικτή η μετάδοση τους αλλά και κατανοητή από τις επικοινωνιακές συσκευές.
c. Υλοποίηση πολύπλεξης όταν οι επικοινωνιακές συσκευές εξυπηρετούν περισσότερους από έναν πελάτη (clients).

2. **Data Link Layer** (Επίπεδο Ζεύξης Δεδομένων): Είναι και γνωστό ως MAC layer και είναι υπεύθυνο για την αξιόπιστη μεταφορά δεδομένων μεταξύ της σύνδεσης που το φυσικό επίπεδο καθόρισε (παράδειγμα πρωτοκόλλου σε αυτό το επίπεδο είναι το Ethernet, το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών). Σε αυτό το επίπεδο οι διευθύνσεις των συσκευών είναι εργοστασιακά προκαθορισμένες και είναι φυσικές διευθύνσεις (MAC address). Κάποια παραδείγματα πρωτοκόλλου εκτός από το Ethernet, είναι τα HDLC και ADCCP για συνδέσεις από σημείο-σε-σημείο και το 462.11, όπως έχει αναφερθεί, για ασύρματα τοπικά δίκτυα. Αυτό το επίπεδο σε κάποια πρωτόκολλα, όπως το 462.11, μπορεί να υποδιαιρεθεί σε μικρότερα υποεπίπεδα όπως:
    a. Υποεπίπεδο MAC: στο οποίο γίνεται έλεγχος πρόσβασης στο κοινό μέσο.
    b. Υποεπίπεδο LLC (logical link control): στο οποίο γίνεται έλεγχος λογικών συνδέσεων. Σε αυτό το στρώμα επικρατέστερο πρωτόκολλο είναι το 462.2.

Τέλος, αναφέρεται πως κάποιες συσκευές που λειτουργούν σε αυτό το επίπεδο είναι δικτυακές γέφυρες και δικτυακοί διακόπτες.

3. **Network Layer** (Επίπεδο Δικτύου): Είναι υπεύθυνο για την διακίνηση των δεδομένων στο δίκτυο εκτελώντας λειτουργίες όπως μεταγωγής στους κόμβους, δρομολόγησης, ελέγχου ροής και αποκατάστασης σφαλμάτων διατηρώντας, πάντα την ποιότητα εξυπηρέτησης που απαιτεί το επόμενο επίπεδο (Επίπεδο Μεταφοράς). Σύνηθες πρωτοκόλλου σε αυτό το επίπεδο είναι το IP22. Τέλος, σε αυτό το επίπεδο λειτουργούν οι δρομολογητές (routers).

4. **Transport Layer** (Επίπεδο Μεταφοράς): Είναι το ανώτερο επίπεδο που έχει σχέση με την παροχή τηλεπικοινωνιακών υπηρεσιών προσφέροντας τις έξης υπηρεσίες: Διαχείριση συνδέσεων, Μεταβίβαση δεδομένων, Έλεγχο ροής. Σύνηθες πρωτόκολλο σε αυτό το επίπεδο είναι το TCP (Transmission Control Protocol - πρωτόκολλο ελέγχου μεταφοράς). Στην ουσία αυτό το επίπεδο διεκπεραιώνει την μεταφορά των δεδομένων από χρήστη σε χρήστη, το οποίο έχει σαν αποτέλεσμα τα ανώτερα επίπεδα σε σχέση με αυτό (δηλαδή με το Επίπεδο Μεταφοράς), να μην ενδιαφέρονται για την αξιοπιστία της μεταφοράς των δεδομένων. Η αξιοπιστία αφορά στο Επίπεδο Μεταφοράς και για να εξασφαλιστεί χρησιμοποιούνται οι εξής τακτικές: Έλεγχος ροής, Κατάτμηση και αποτμηματοποιήση, Έλεγχος σφαλμάτων.

   Το επίπεδο είναι δυνατό να μπορεί να γνωρίζει ποια πακέτα δεν παραδόθηκαν, ώστε να ξαναπροσπαθεί την αποστολή τους.

5. **Sessíon Laver** (Επίπεδο Συνόδου): Το επίπεδο αυτό δίνει τη δυνατότητα στους χρήστες να πραγματοποιούν συνόδους οργανώνοντας και συγχρονίζοντας την ανταλλαγή μηνυμάτων. Οι λειτουργίες που αντιμετωπίζει είναι: FDX (full duplex, όταν οι δύο που συνομιλούν μιλούν ταυτόχρονα δεσμεύοντας δύο κανάλια), HDX (half duplex, όταν υπάρχει

ένα διαθέσιμο κανάλι το οποίο πρέπει να μοιραστούν δύο συνομιλητές και έτσι μιλάει ο καθένας με τη σειρά). Σε αυτό το στρώμα υποστηρίζονται διαδικασίες όπως: Αποθήκευση κατάστασης (checkpoint), Αναβολή (adjournment), Τερματισμός (termination), Επανεκκίνηση (restart).

6. **Presentatíon Layer** (Επίπεδο παρουσίασης): Το επίπεδο αυτό είναι υπεύθυνο για τον μετασχηματισμό των δεδομένων στην αναμενόμενη, από το επόμενο επίπεδο, τυπική μορφή. Σε αυτό το επίπεδο τα δεδομένα κρυπτογραφούνται, συμπιέζονται, κωδικοποιούνται και γενικά επεξεργάζονται ανάλογα με τις απαιτήσεις του συγκεκριμένου πρωτόκολλου της κάθε εφαρμογής. Για παράδειγμα σε αρκετές εφαρμογές τα δεδομένα έρχονται σε μορφή XML(XML - extensible Markup Language - είναι μια γλώσσα σήμανσης που περιέχει ένα σύνολο κανόνων για την ηλεκτρονική κωδικοποίηση κειμένων και γενικά δεδομένων) και μετατρέπονται σε αρχεία αναγνωρίσιμα από την εφαρμογή που υπάρχει στο πιο πάνω στρώμα.

7. **Applícatíon Laver** (Επίπεδο εφαρμογής): Αυτό το επίπεδο είναι το ανώτατο επίπεδο του μοντέλου και είναι στο επίπεδο όπου ο χρήστης αλληλεπιδρά με τα δεδομένα και γενικότερα με το δίκτυο. Κάθε εφαρμογή που επεξεργάζεται δεδομένα του δικτύου και επικοινωνεί με τον χρήστη θα βρίσκεται σε αυτό το επίπεδο. Μερικά παραδείγματα πρωτοκόλλων στο επίπεδο αυτό είναι:

a. Telnet: -Telecommunication NETwork - πρωτόκολλο επικοινωνίας διασυνδεδεμένων υπολογιστών
b. FTP: - File Transfer Protocol - ευρέως χρησιμοποιούμενο πρωτόκολλο μεταφοράς αρχείων.
c. SMTP: - Simple Mail Transfer Protocol – καθιερωμένο πρωτόκολλο για τη μετάδοση μηνυμάτων ηλεκτρικού ταχυδρομείου στο internet.

d. HTTP: - HyperText Transfer Protocol - το πιο διαδεδομένο πρωτόκολλο μεταφοράς υπερκειμένου στο διαδίκτυο.

Η αρχιτεκτονική ενός ΑΔΑ απαιτεί την ύπαρξη των τελευταίων τριών κατωτέρων επιπέδων (φυσικού, ζεύξης δεδομένων, δικτύου) για αυτό και θα κάνουμε μια πιο εκτενή αναφορά στα πρωτόκολλα που έχουν κατά καιρούς προταθεί για τα τρία αυτά επίπεδα.

5.3 Πρωτόκολλο στο φυσικό επίπεδο

Όπως έχει ήδη αναφερθεί το Φυσικό επίπεδο είναι το χαμηλότερο επίπεδο στο οποίο βρίσκεται το hardware του δικτύου. Η ποιότητα του φυσικού επιπέδου σε ένα κόμβο εξαρτάται άμεσα από το κόστος και την κατανάλωση ενέργειας, για αυτό και τα πρωτόκολλα σε αυτό το επίπεδο προσπαθούν να μειώσουν την κατανάλωση ενέργειας και να μειώσουν ταυτόχρονα το κόστος των ηλεκτρονικών/αναλογικών μερών. Συνήθως, η βέλτιστη λύση μπορεί να επιτευχθεί με διάφορους συμβιβασμούς (trade-offs), όπου ο αρχιτέκτονας του υλικού καλείται να πραγματοποιήσει.

Τα πιο διαδεδομένα πρωτόκολλα είναι της κατηγόριας 802.11, γνωστή και ως Wi-Fi (Wireless Fidelity, στα ελληνικά «ασύρματη πιστότητα»), τα οποία αναφέρονται σε μια οικογένεια προτύπων που έχουν να κάνουν με τα ασύρματα τοπικά δίκτυα. Τα πρότυπα δουλεύουν στις συχνότητες των 2.4, 3.6 και 5 GHz και πλέον αποτελούν τα καθιερωμένα πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων. Εφαρμογές του πρότυπου είναι παροχή πρόσβασης στο διαδίκτυο, VoIP (voice over ip, τηλεφωνία μέσω internet), ασύρματη διασύνδεση ηλεκτρονικών συσκευών μεταξύ τους κτλ.

Η πρώτη έκδοση του Wi-Fi εμφανίστηκε το Ιούνιο του 1997, λειτουργούσε στην συχνότητα των 2.4GHz με FHSS (frequency hopping) και κατόρθωνε να φτάνει ταχύτητες μέχρι 1 Mbps. Ο ρυθμός μετάδοσης αυξήθηκε στα 2 Mbps, εφόσον έγινε χρήση DSSS (direct sequence), με την εμβέλεια να φτάνει τα 20 μέτρα σε εσωτερικούς χώρους και τα 100 μέτρα σε εξωτερικούς χώρους. Το Σεπτέμβριο του 1999 παρουσιάστηκε η έκδοση 462.11a, η οποία λειτουργούσε σε συχνότητες των 5 και 3.7GHz και χρησιμοποιούσε OFDM (orthogonal frequency division rnultiplexing), με αποτέλεσμα η συγκεκριμένη έκδοση να πετύχαινει ταχύτητες 6, 9, 12, 18, 24, 36, 48, 54 Mbps και εξωτερική εμβέλεια εως και 5km. Τον ίδιο μήνα παρουσιάστηκε και η έκδοση 462.11b με συχνότητα στα 2.4GHz, η οποία χρησιμοποιώντας DSSS είχε ρυθμό μετάδοσης δεδομένων 5.5 και 11 Mbps και με εμβέλεια 38m σε εσωτερικούς χώρους και 140m σε εξωτερικούς χώρους. Τον Ιούνιο του 2003 η έκδοση 462.11g με συχνότητα στα 2.4GHz και χρήση OFDM και DSSS χαρακτηριζόταν από ρυθμούς μετάδοσης όπως και της έκδοσης 462.11a ενώ είχε εμβέλεια όπως η έκδοση 462.11b. Η έκδοση 462 .11n, η οποία δουλεύει στα 2.4/5GHz με OFDM, εμφανίστηκε τον Οκτώβριο του 2009 και μπορεί να έχει ρυθμό μετάδοσης έως και 150Mbps και εμβέλεια 36m εσωτερικά και 250m εξωτερικά. Η πιο πρόσφατη έκδοση παρουσιάστηκε το 2016 με την ονομασία 462.11ah με συχνότητα λειτουργίας στα 900 MHz, με αποτέλεσμα την πολύ χαμηλή κατανάλωση ισχύος (η κατανάλωση ισχύος συγκρίνεται με αυτή της τεχνολογίας Bluetooth) και υψηλή ταχύτητα στα 43.3 Mbps [10].

5.4 Πρωτόκολλο στο Επίπεδο Ζεύξης Δεδομένων

Στο δεύτερο επίπεδο του OSI μοντέλου, γνωστό και ως MAC επίπεδο, τα πιο γνωστά πρωτόκολλα είναι βασισμένα σε λογική CSMA (carrier sense multiple

access : MAC πρωτόκολλο στο οποίο ένας κόμβος πρέπει να σιγουρέψει ότι δεν υπάρχει μετάδοση άλλου σήματος στο μέσο, πχ BUS, στο οποίο μεταδίδει τα δεδομένα ώστε να στείλει το πακέτο του) και λογική TDMA (time division multiple access: μέθοδος η όποια επιτρέπει την παραχώρηση κάποιου καναλιού συγκεκριμένης συχνότητας σε περισσότερους από έναν πελάτη – clients- διαμελίζοντας το σήμα σε διάφορα χρονικά κομμάτια). Το πιο γνωστό πρωτόκολλο είναι το Mac πρωτόκολλο IEEE 462.15.4, η ανάλυση του οποίου ακολουθεί παρακάτω [II,III,IV,11,V, 12, VI, VII, VIII].

1. **CSMA**
    a. S-MAC (sense - mac, υποστηρίζεται από το tiny0S)
       (tiny0S: λειτουργικό σύστημα σχεδιασμένο ειδικά για ασύρματα δίκτυα αισθητήρων)
    b. T-MA C (timeout - mac)
    c. B-MAC (Berkley- mac, υποστηρίζεται από το tinyOS)
    d. P-MAC (pattern-mac)

2. **TDMA**
    a. E-MAC
    b. L-MAC
    c. RI-MAC

3. **IEEE 802.15.4**

Το IEEE 802.15.4 είναι ένα πρότυπο που καθορίζει τις προδιαγραφές που θα πρέπει να έχει το φυσικό και το MAC επίπεδο των κόμβων για την υλοποίηση ασύρματων δικτύων χαμηλού ρυθμού μετάδοσης (LR-WPAN, low rate wireless personal area network). Βασικά χαρακτηριστικά του πρωτύπου είναι η ικανότητα να ελαχιστοποιεί την κατανάλωση ενέργειας, η παροχή αξιοπιστίας, η όχι ιδιαίτερη πολυπλοκότητά του, η ικανότητα υλοποίησης ασύρματων δικτύων

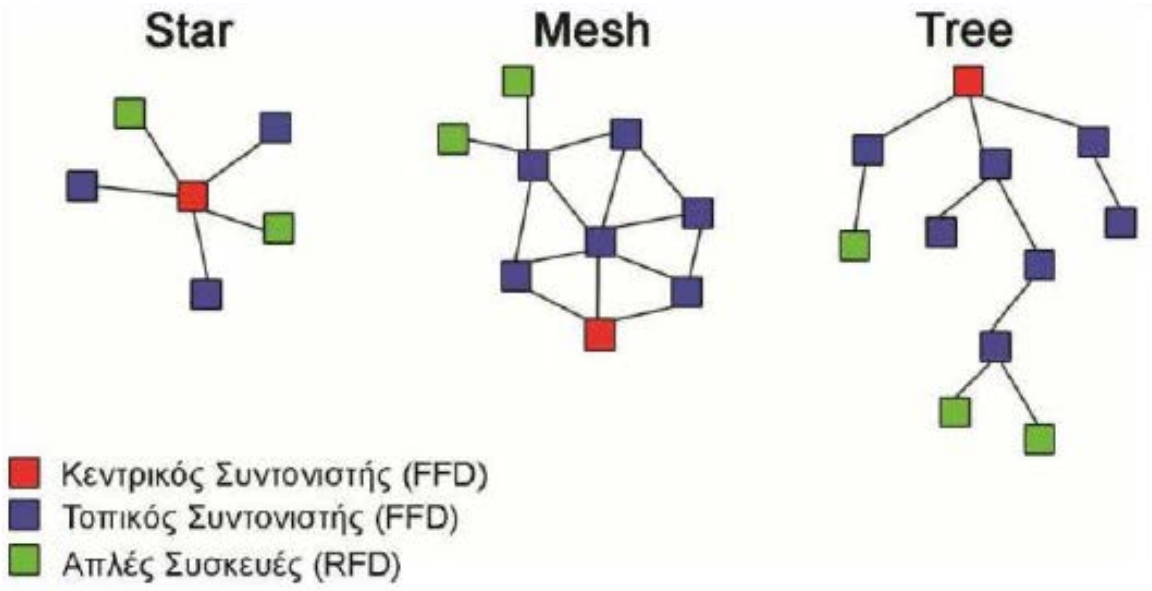
γρήγορα, εύκολα και ευέλικτα. Το πρότυπο καθορίζει τρείς μπάντες συχνοτήτων στις οποίες μπορεί να λειτουργήσει:

a. **Ευρώπη**: 868-868,6 MHz, με 1 κανάλι και με ρυθμό μετάδοσης 20kbps.
b. **Αμερική**: 905-928 MHz, με 10 κανάλια και με ρυθμό μετάδοσης 40kbps.
c. **Παγκοσμίως:** 2,4-2,485 GHz, με 16 κανάλια των 5MHz και με ρυθμό μετάδοσης 250kbps.

Ένα δίκτυο βασισμένο σε αυτό το πρότυπο ορίζει δύο είδη κόμβων στο επίπεδο MAC και είναι:

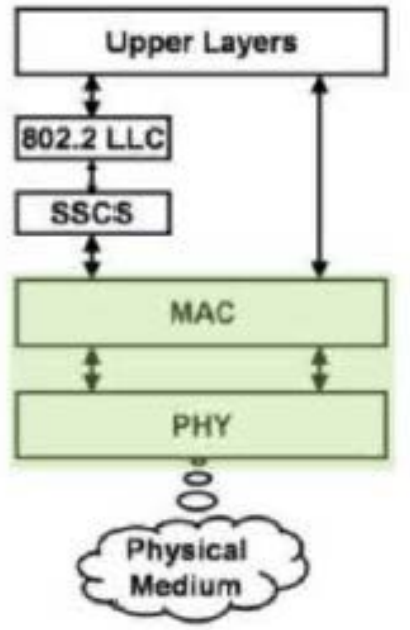
a. **FFD** (Full Function Device): Ένα κόμβος που είναι FFD σε ένα PAN (Personal Area Network - προσωπικό τοπικό δίκτυο) δίκτυο μπορεί να είναι κεντρικός συντονιστής του δικτύου, τοπικός συντονιστής οπουδήποτε στο δίκτυο ή και μια απλή συσκευή του δικτύου. Οι FFD έχουν τη δυνατότητα να επικοινωνούν με οποιοδήποτε κόμβο εντός της εμβέλειας τους. Οι FFD είναι ο βασικός κορμός του δικτύου
b. **RFD** (Reduce Function Device): Απλές συσκευές στο δίκτυο που προορίζονται για μικρές εργασίες και επικοινωνούνε μόνο με τον πλησιέστερο FFD κόμβο.

Ένα τέτοιο δίκτυο σχηματίζεται από FFD και RFD κόμβους σχηματίζοντας δίκτυα με τοπολογίες peer to peer, star, rnesh, όπως αναφέρθηκαν στην αρχή αυτού το κεφαλαίου. Στην Εικόνα 8 φαίνονται τρεις χαρακτηριστικές τοπολογίες και το είδος των αντίστοιχων κόμβων τους.



Σχήμα 8 – Τοπολογίες 462.15.4 [11]

Το πρωτόκολλο 802.15.4 αποτελείται από ένα σύνολο επιπέδων (όπως και το OSI) με το κάθε επίπεδο εκτελεί ένα μέρος του συνολικού έργου που επιτελεί το πρωτόκολλο. Μια συσκευή που είναι συμβατή με το 802.15.4 έχει δύο επίπεδα, το φυσικό επίπεδο, που είναι ο πομποδέκτης μαζί με κάποιους μηχανισμούς ελέγχου, και το επίπεδο του MAC, το όποιο είναι υπεύθυνο να παρέχει πρόσβαση στο φυσικό κανάλι για όλους τους τύπους μετάδοσης. Τα δύο επίπεδα φαίνονται στην Εικόνα 9 και ονομάζονται αντίστοιχα PHY και MAC.



Σχήμα 9 – Αρχιτεκτονική συσκευής LR-WPAN [V]

Παρακάτω γίνεται η ανάλυση των δύο επιπέδων:

1. **Φυσικό επίπεδο** (PHY): Στο φυσικό επίπεδο η τεχνική μετάδοσης που χρησιμοποιείται είναι η DSSS με διαμόρφωση BPSK (- Binary Phase-Shift Keying - η πιο απλή μορφή διαμόρφωσης μετατόπισης φάσης) ή QPSK (- Quadrature Phase Shift Keying - είναι ένας αλγόριθμος διαμόρφωσης φάσης) Στο φυσικό επίπεδο εκτελούνται οι πιο κάτω διεργασίες:
    a. **Ανίχνευση ενέργειας στον δέκτη** (ED, Receive Energy Detection): Στη συγκεκριμένη διεργασία γίνεται εκτίμηση της ισχύος τους σήματος που λαμβάνεται χωρίς να επιχειρείται η αποκωδικοποιήση του σήματος ή η αναγνώριση οτιδήποτε άλλου πέρα του σήματος. Η εκτίμηση φυλάσσεται ώστε να μπορεί να χρησιμοποιηθεί και από άλλα επίπεδα.

b. **Ένδειξη ποιότητας συνδέσμου** (LQI, link quality Indicator): Κατά την παραλαβή ενός πακέτου σε αυτό το επίπεδο γίνεται πρώτα μια εκτίμηση για την ποιότητα του με βάση την τιμή του ED και η αποθήκευση της εκτίμησης αυτής ώστε να χρησιμοποιηθεί και από άλλα επίπεδα.
c. **Έλεγχος αδράνειας καναλιού** (CCA, Clear Channel Assessment): Κατά τη διεργασία αυτή γίνεται έλεγχος για το κατά πόσο υπάρχει κίνηση στο κανάλι. Αυτό μπορεί να επιτευχθεί είτε ελέγχοντας αν η ED έχει ξεπεράσει κάποιο συγκεκριμένο όριο, είτε με ανίχνευση φέροντος, είτε με την ανίχνευση σήματος που χαρακτηρίζεται με την αναμενόμενη διαμόρφωση στο κανάλι.

Στο φυσικό επίπεδο γίνεται η επιλογή της συχνότητας του καναλιού που θα χρησιμοποιηθεί και η αποστολή/λήψη των πακέτων. Τα πακέτα στο φυσικό επίπεδο έχουν τη δομή, όπως αυτή παρουσιάζεται στον Πίνακα 4:

		Octets		
		1		Variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

ΠΙΝΑΚΑΣ 5 – [12]

Το preamble σήμα που χρησιμεύει για τον συγχρονισμό και το πεδίο SFD (Start of Frame Delimiter) -που καθορίζει την αρχή του υπόλοιπου πακέτου -

αποτελούν την κεφαλίδα SHR (Synch Header). Στη συνέχεια, η κεφαλίδα PHR δηλώνει το μέγεθος του πλαισίου PSDU (PHY Service Data Unit), το οποίο μεταβάλλεται και είναι η χρήσιμη πληροφορία.

2. **Επίπεδο MAC**: Το επίπεδο MAC χρησιμοποιεί τον αλγόριθμο CSMA - CA (Carrier Sense Multiple Access with Collision Avoidance) και με βάση αυτόν επιλέγεται ποια συσκευή θα ξεκινήσει να εκπέμπει ή θα σταματήσει και θα μπει σε αναμονή.Υπάρχουν δύο εκδοχές του CSMA:

    a. **Slotted CSMA**: Σε αυτή την περίπτωση η συσκευή που θα εκτελέσει την αποστολή παρακολουθεί το κανάλι αν είναι αδρανές και εφόσον το επιβεβαιώσει στέλνει το πακέτο σε μικρά κομμάτια του (slots). Το slotted CSMA είναι ιδανικό για τοπολογίες που υπάρχει διαφοροποίηση των κόμβων μεταξύ τους σε θέματα ιεραρχίας (master, slave).
    b. **Unslotted CSMA - CA**: Ο αλγόριθμος αυτός, όπως και ο πιο πάνω, ανιχνεύει την κίνηση στο κανάλι. Εφόσον το κανάλι είναι αδρανές αρχίζει η μετάδοση ολόκληρου του πακέτου. Στην περίπτωση που στο κανάλι υπάρχουν συγκρούσεις, ο αλγόριθμος οπισθοχώρησης του Ethernet καθυστέρει τις συσκευές για ένα τυχαίο χρονικό διάστημα ώσπου να επιχειρήσουν ξανά τη διαδικασία.

Τα πακέτα στο MAC επίπεδο έχουν την πιο κάτω μορφή:

ΠΙΝΑΚΑΣ 6 – [12]

Octets: 2	**1**	**0/2**	**0/2/8**	**0/2**	**0/2/8**	**0/5/6/10/ 14**	**Variable**	**2**
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Auxiliary Security Server	Frame payload	FCS
		Addressing Fields						
MHR							MAC payload	MFR

Ένα πακέτο στο επίπεδο MAC αποτελείται από το MHR, το MAC payload και το MFR. Η κεφαλίδα MHR περιέχει πληροφορίες σχετικά με την διευθυνσιοδότηση του πακέτου, τον τύπο του υπόλοιπου πακέτου (το είδος του payload) και την αρίθμηση του πακέτου.

5.5 Πρωτόκολλο στο επίπεδο δικτύου

Στο επίπεδο δικτύου θα αναφέρουμε κάποια πρωτόκολλα που αναλαμβάνουν την δρομολόγηση των δεδομένων [13,14].

1. **Network structure based protocols**:
    a. **Flat routing:** Ο κάθε κόμβος είναι ίσος με τον δίπλα του (p2p) και θα πρέπει να συνεργαστούν για να μεταφέρουν δεδομένα. Η λογική αυτών των πρωτοκόλλων θέτει ως κέντρο τα δεδομένα (data centric) και όχι τους κόμβους, αφού έτσι και αλλιώς ο κάθε κόμβος δεν μπορεί να ξεχωρίσει από τον άλλον. Ακολουθούν σχετικά παραδείγματα:

I. **SPIN** (Sensor protocols for in forrnations vía negotiation)

II. **Directed diffusion**

III. **Energy aware routing**

b. **Hierarchical Routing:** Σε αυτή την οικογένεια πρωτοκόλλων δημιουργείται ιεραρχία μεταξύ των κόμβων. Οι κόμβοι με περισσότερη ενέργεια καλούνται να εκτελέσουν την επεξεργασία και την αποστολή των δεδομένων σε αντίθεση με τους υπόλοιπους κόμβους.

I. **LEACH** (low energy adaptive clustering)

II. **PEGASIS** (power efficient gatherinq in sensor inforrnation systerns)

III. **TEEN** (threshold sensitive energy efficient protocol)

IV. **SMECN** (srnall rninirnurn energy cornrnunication network)

V. **SOP** (self organized protocol)ví. Virtual qrid architecture

VI. **TTDD** (two tier data dissernination)

c. **Location based routing:** Σε αυτή την οικογένεια οι κόμβοι καθορίζονται από την γεωγραφική τους θέση η οποία μπορεί να καθοριστεί είτε από GPS είτε από την ισχύ του σήματος των γειτονικών κόμβων.

I. **GAF** (geographic adaptive fidelity)

II. **GEAR** (geographic energy aware routing)

III. **SPAN**

2. **Protocol operation based protocols:**

    a. **Multipath:** Σε αυτή την οικογένεια η πηγή και ο προορισμός συνδέονται με περισσότερο από ένα μονοπάτι, με αποτέλεσμα να αυξάνεται η αξιοπιστία αλλά να μεγαλώνει η συνολική κατανάλωση.
    b. **Query based:** Σε αυτή την οικογένεια ο προορισμός διαδίδει στο δίκτυο το αίτημα (query) και οι συγκεκριμένοι κόμβοι ανταπαντούνε.
    c. **Negotiation based**: Σε αυτή την οικογένεια γίνεται προσπάθεια να εξαλείφθούν οι επιπλέον μεταδόσεις των κόμβων για διαπραγμάτευση.
    d. **Quality of Service (QoS):** Σε αυτή την οικογένεια το πακέτο παραδίδεται στο σταθμό βάσης έγκαιρα, με χαμηλή συνολική κατανάλωση.

Τα πρωτόκολλα δρομολόγησης θα μπορούσαν να κατηγοριοποιηθούν ως εξής:

1. Proactive: Τα πρωτόκολλα στα οποία οι διαδρομές που θα ακολουθήσουν τα μηνύματα είναι προκαθορισμένες.
2. Reactive: Τα πρωτόκολλα με δυναμικές διαδρομές δρομολόγησης, οι οποίες υλοποιούνται όταν το δίκτυο χρειαστεί να μεταφέρει δεδομένα.
3. Hybrid: Τα πρωτόκολλα που αποτελούν συνδυασμό των δύο πιο πάνω.

5.6 Λειτουργικό σύστημα των Ασύρματων Δικτύων Αισθητήρων

Το λειτουργικό σύστημα είναι η διεπαφή του χρήστη με το υλικό. Ένα λειτουργικό σύστημα που απευθύνεται σε ΑΔΑ είναι πολύ πιο απλό από τα συνηθισμένα λειτουργικά (Windows, Linux, Solaris κτλ). Αυτό οφείλεται στο γεγονός ότι το ίδιο το υλικό (δηλαδή το hardware) δεν μπορεί να υποστηρίξει πολύπλοκες εφαρμογές, καθώς οι κόμβοι είναι σχεδιασμένοι για συγκεκριμένες

εφαρμογές και έχουν ως στόχο την χαμηλή κατανάλωση (περιορισμοί που δεν υπάρχουν στην αρχιτεκτονική ενός επεξεργαστή τις οικογένειας, για παράδειγμα, x86 της Intel). Πιο κάτω αναφέρονται μερικά από τα πιο γνωστά λειτουργικά που έχουν σχεδιασθεί για ΑΔΑ [15,16]:

1. **MANTIS OS** (Multímodal of in-sítu sensors): Multithreading (Τεχνική λειτουργικών συστημάτων κατά την οποία κάποιες διεργασίες μπορούν να τρέχουν σε διάφορα νήματα, δίνοντας την αίσθηση της παράλληλης επεξεργασίας αυξάνοντας την αποδοτικότητα των εφαρμογών) λειτουργικό σύστημα σχεδιασμένο ασύρματους αισθητήρες με περιορισμένους πόρους.

2. **TnutOS**

3. **Nano RK OS**: Πραγματικού χρόνου λειτουργικό σύστημα κατασκευασμένο για μικροελεγκτές που χρησιμοποιούν διάφοροι κόμβοι των ΑΔΑ.

4. **LíteOS**: Πραγματικού χρόνου λειτουργικό σχεδιασμένο για ΑΔΑ.

5. **Contíkí OS**: Λειτουργικό ανοιχτού κώδικα, πολυδιεργασιακό ή αλλιώς Multitasking (Η χρήση δύο ή περισσότερων κεντρικών μονάδων επεξεργασίας –CPU - σε ένα ενιαίο σύστημα υπολογιστή) με υψηλή μεταφερσιμότητα, σχεδιασμένο για δικτυωμένα ενσωματωμένα συστήματα και ασύρματα δίκτυα αισθητήρων με περιορισμούς μνήμης. Παρέχει ταυτόχρονα μηχανισμούς πλήρους IP δικτύωσης (και για τις δύο εκδόσεις 1Pv4 και 1Pv6) και χαμηλής κατανάλωσης ενέργειας ραδιοεπικοινωνία.

6. **TínvOS**: Λειτουργικό ανοικτού κώδικα ΛΣ και ίσως το πιο διαδεδομένο για ασύρματα δίκτυα αισθητήρων. Η τελευταία έκδοση είναι η 2.1.1, η οποία παρουσιάσθηκε τον Απρίλιο του 2010. Η εγκατάσταση του λειτουργικού σε

κόμβους με περιορισμένους πόρους και με απαίτηση βέλτιστης κατανάλωσης ενέργειας προϋποθέτει ότι το λειτουργικό θα πρέπει:

a. Να έχει αρκετά μικρό μέγεθος.
b. Να είναι ικανό να ελαχιστοποιεί την κατανάλωση ενέργειας.
c. Να είναι αξιόπιστο (μεταφορά πακέτων, επεξεργασία κτλ) .
d. Να υποστηρίζει την δυνατότητα επαναπρογραμματισμού.
e. Να υποστηρίζει ποικίλες εφαρμογές.
f. Να μπορεί να εφαρμόσει μιας μορφής παραλληλισμού

Χαρακτηριστικό του tinyOS είναι η απουσία του Multithreading. Αντί αυτού γίνεται χρήση του Event-Driven μοντέλου (Η παραγωγή, ανίχνευση και αντίδραση σε γεγονότων σηματοδείται με την αλλαγή της παρούσας κατάστασης του συστήματος). Το Event-Driven μοντέλο εξασφαλίζει παράλληλη εκτέλεση διεργασιών χρησιμοποιώντας ελάχιστη ενέργεια και μνήμη (βασικές απαιτήσεις).

6 Εφαρμογές Ασύρματων Δικτύων Αισθητήρων

6.1 Παράγοντες υλοποίησης εφαρμογών και κατηγορίες εφαρμογών

Όπως και με πολλές άλλες τεχνολογίες, η έρευνα στην περιοχή των ασύρματων δικτύων αισθητήρων ξεκίνησε από στρατιωτικές εφαρμογές και χάρη στην δημιουργικότητα των χρηστών πολλές νέες εφαρμογές έχουν προκύψει, οι απαιτήσεις των οποίων δίνουν διαρκώς ώθηση για την ανάπτυξη περισσότερων εφαρμογών, στην εξέλιξη των αισθητήρων και άρα κάνοντας επιτακτική την ανάγκη ενσωμάτωσής τους σε άλλους τεχνολογικούς κλάδους.

Τα ασύρματα δίκτυα αισθητήρων παρέχουν ένα τρόπο εποπτείας και κατά επέκταση ελέγχου του περιβάλλοντα χώρου ή επίβλεψης ενός συγκεκριμένου μέρους ενός συστήματος. Η θεώρηση αυτή δεν έχει να κάνει μόνο με την παρατήρηση ενός φαινομένου, αλλά και με την ανάλυση, την επεξεργασία και την παρουσίαση των δεδομένων που λαμβάνονται από τα ΑΔΑ. Συγκεκριμένα, τα ΑΔΑ παρουσιάζουν τη δυνατότητα δειγματοληψίας με μεγαλύτερη συχνότητα απ' ότι άλλες παραδοσιακές μέθοδοι, οι οποίες πάσχουν από έλλειψη διάρκειας τόσο στον χρόνο όσο και στον χώρο που περιγράφουν το δείγμα. Οι παραδοσιακές προσεγγίσεις για την μελέτη πολύπλοκων φαινομένων στο σύνολο τους βασίζονται σε ένα μικρό, αντιπροσωπευτικό και ικανό αριθμό δεδομένων προκειμένου να εξαχθεί μια γενική εικόνα. Ωστόσο, σε μια εφαρμογή χρειάζεται ένας ικανός αριθμός αισθητήρων, σωστά κατανεμημένων στον χώρο, οι οποίοι παίρνουν μετρήσεις με τέτοια συχνότητα ώστε να μπορούν να εποπτεύσουν το φαινόμενο. Επιπλέον, χρειάζεται μια τεχνολογική υποδομή για τη συλλογή αυτών των δεδομένων και τη μετάδοση τους σε έναν

ανθρώπινο παρατηρητή. Τέλος, απαιτείται μια τεχνική ανάλυσης η οποία μπορεί να κάνει αυτά τα δεδομένα πιο κατανοητά, ώστε να εξαχθεί κάποιο συμπέρασμα καθώς επίσης και να δώσει την ευκαιρία εκμετάλλευσης τους σε πλήθος εφαρμογών [1][3][17][18].

Η ασύρματη δικτύωση και η δυνατότητα αυτό-οργάνωσης των δικτύων χωρίς την ανάγκη ανθρώπινης παρέμβασης, κάνει δυνατή την εξάπλωση τους σε περιβάλλοντα που είναι δύσκολο ή ακόμη και αδύνατο να πλησιάσει ο άνθρωπος. Η έλλειψη καλωδίωσης για την επίτευξη της μεταξύ τους επικοινωνίας αποτελεί τον κυρίαρχο παράγοντα που συμβάλλει σε αυτό. Αποτέλεσμα αυτών των πλεονεκτημάτων είναι η δυνατότητα παρατήρησης του φαινομένου από μεγάλη ή ασφαλή απόσταση. Συμπληρωματικά πλεονεκτήματα των ασύρματων δικτύων αισθητήρων που συμβάλλουν καθοριστικά στην υλοποίηση πολλών εφαρμογών είναι[7][17]:

1. Η δυνατότητα να δουλεύουν σε ακραίες συνθήκες.
2. Η δυνατότητα υποστήριξης πολλών αισθητήρων σε ένα δίκτυο, η οποία επιδρά στη δυνατότητα υψηλής συχνότητας δειγματοληψίας και στην υψηλή ανάλυση πολύπλοκων μετρήσεων.
3. Η αυξημένη χωρική πυκνότητα της διάταξης, η οποία βελτιώνει τα ποσοστά σφάλματος με πλεονασμό πληροφοριών από γειτονικούς κόμβους για την ίδια περιοχή κάλυψης.
4. Η χαμηλή ενεργειακή κατανάλωση.
5. Το χαμηλό κόστος.

Καθοριστικός, επίσης παράγοντας στην υλοποίηση εφαρμογών είναι η μεγάλη ποικιλία των τύπων των αισθητήρων για φαινόμενα και καταστάσεις όπως:

1. Θερμοκρασία
2. Πίεση
3. Ένταση φωτός
4. Υγρασία

5. Κίνηση
6. Επιτάχυνση
7. Ένταση Θορύβου
8. Μέτρησης όγκου αντικειμένων
9. Σύσταση εδάφους κ.α.

Με βάση τα παραπάνω γίνεται εύλογο πως οι πρώτες εφαρμογές των ασύρματων δικτύων αισθητήρων είχαν σχέση με τη συλλογή δεδομένων σε περιβάλλοντα που είναι δύσκολο να ελεγχθούν ή που είναι δύσκολο να υφίσταται ανθρώπινη παρουσία, όπως τα περιβάλλοντα φυσικών πόρων. Σημαντική επίσης υπήρξε και η χρήση τους για τον εντοπισμό συμβάντων ή θέσης, όπως σεισμικών δραστηριοτήτων ή κινούμενων αντικειμένων, γεγονός που εισήγαγε την έννοια του εντοπισμού συμβάντος ως μια επιπλέον δυνατότητα στη χρήση των δικτύων αυτών. Μια τρίτη εφαρμογή των δικτύων αυτών, η ανίχνευση καταστάσεων, κινείται κάπου μεταξύ της παρακολούθησης, συλλογής δεδομένων και του εντοπισμού συμβάντος. Αυτός ο τύπος δικτύου καταγράφει συγκεκριμένα πράγματα στο χώρο, τα οποία αξίζουν παρακολούθησης, και επίσης είναι σε θέση να αξιολογήσει και να εντοπίσει μη ομαλές τιμές ή και να προσδιορίσει καταστάσεις. Τα ασύρματα δίκτυα αισθητήρων μπορούν να καταταγούν σε δυο βασικές κατηγορίες [1][3], όπως φαίνεται και στην Εικόνα 10:

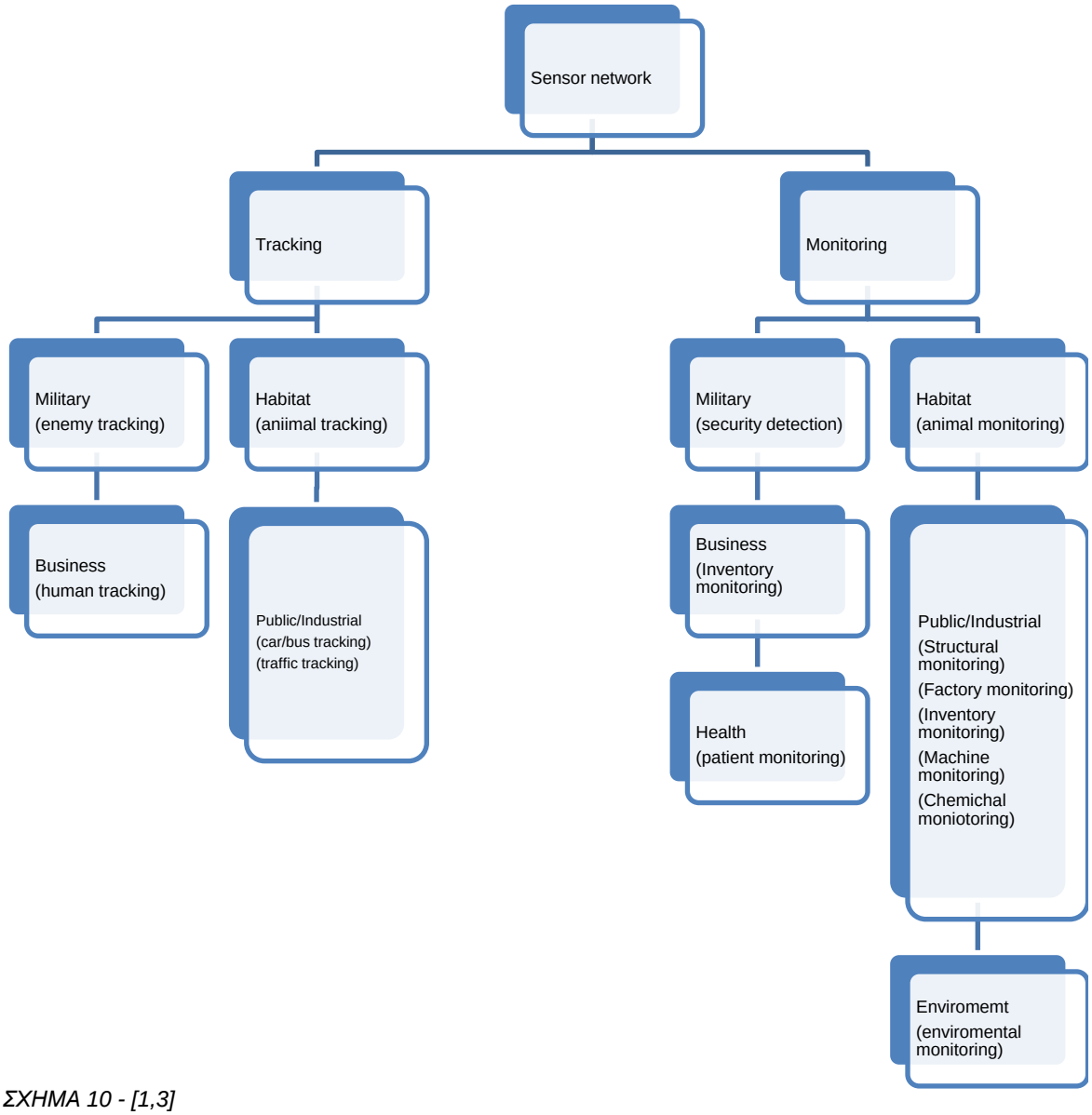
1. της επίβλεψης (monitoring)
2. της ανίχνευσης (tracking)

Αυτές με την σειρά τους μπορούν να χωριστούν σε:

1. Παρακολούθηση χώρου
2. Παρακολούθηση αντικειμένων
3. Παρατήρηση της αλληλεπίδρασης των αντικειμένων και περιβάλλοντος χώρου

Ενδεικτικά, ορισμένες εφαρμογές αναφέρονται ακολούθως [7]:

1. Περιβαλλοντικές εφαρμογές,
2. Γεωργικές εφαρμογές
3. Εφαρμογές πρόληψης καταστροφών και παροχής βοήθειας
4. Οικιακές εφαρμογές
5. Επιτήρηση μηχανών και βιομηχανικές εφαρμογές
6. Επιτήρηση αντικειμένων
7. Εφαρμογές ασφαλείας
8. Στρατιωτικές εφαρμογές
9. Τηλεματική - έλεγχος μεταφορών και συγκοινωνιών
10. Ιατρικές εφαρμογές και Υγιεινή
11. Άλλες εμπορικές εφαρμογές


Sensor network
Tracking
Monitoring
Military
(enemy tracking)
Habitat
(aniimal tracking)
Military
(security detection)
Habitat
(animal monitoring)
Business
(human tracking)
Public/Industrial
(car/bus tracking)
(traffic tracking)
Business
(Inventory
monitoring)
Public/Industrial
(Structural
monitoring)
(Factory monitoring)
(Inventory
monitoring)
(Machine
monitoring)
(Chemichal
moniotoring)
Health
(patient monitoring)
Enviromemt
(enviromental
monitoring)

ΣΧΗΜΑ 10 - [1,3]

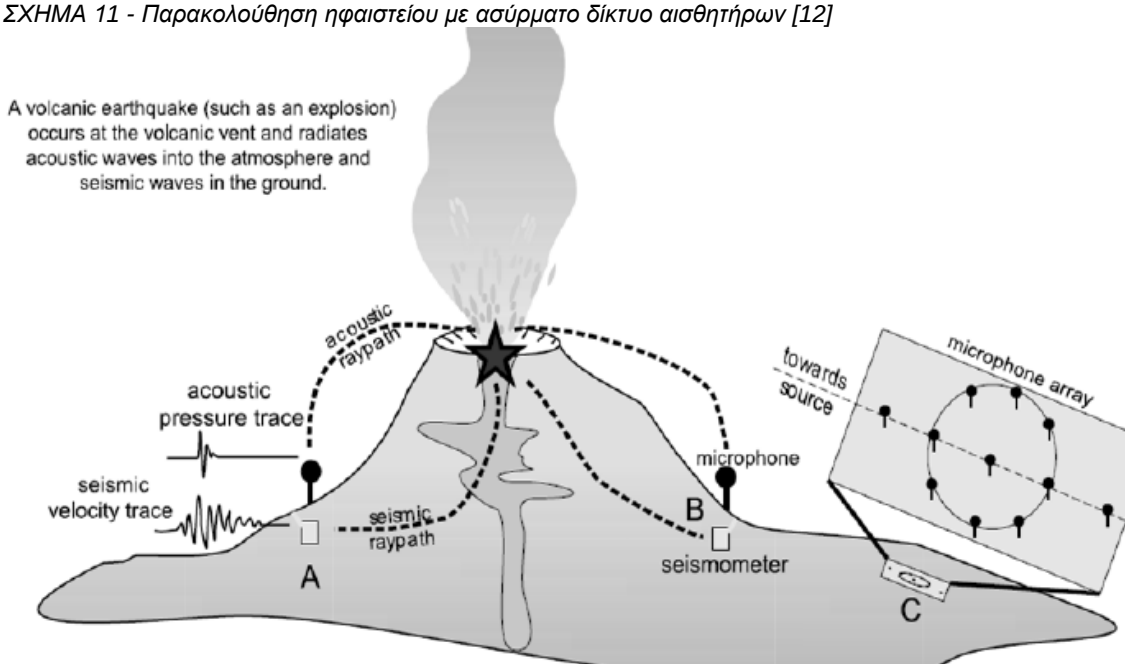
6.2 Περιβαλλοντικές εφαρμογές

Σήμερα υπάρχει ένας μεγάλος αριθμός περιβαλλοντολογικών εφαρμογών ασύρματων δικτύων αισθητήρων για την καταγραφή της εξελικτικής διαδικασίας ενός οικοσυστήματος υδάτινου, χερσαίου, δασικού ή αστικού. Στις εφαρμογές αυτές χρησιμοποιούνται συνήθως αισθητήρες βροχόπτωσης, στάθμης νερού και αισθητήρες καιρού για μετεωρολογική, γεωφυσική έρευνα και μελέτη της ρύπανσης. Υπάρχουν επίσης εφαρμογές για την ρύθμιση των κλιματικών συνθηκών στα μεγάλα κτήρια ώστε να εξασφαλίζεται ένα περιβάλλον εργασίας ευχάριστο και κυρίως υγιές. Επιπλέον, υπάρχουν, περιβαλλοντικές εφαρμογές για την παρατήρηση και καταγραφή του ζωικού βασιλείου όπως είναι η παρακολούθηση της κίνησης των πουλιών, των μικρών ζώων και των εντόμων, η καταγραφή κρίσιμων περιβαλλοντικών παραμέτρων και συνθηκών που επηρεάζουν το κλίμα της γης, η καταγραφή μετρήσεων σε θάλασσα, ξηρά και αέρα, ο εντοπισμός πυρκαγιάς σε δάση, ο εντοπισμός πλημμυρών, η μελέτη της μόλυνσης και τέλος η γεωφυσική και μετεωρολογική έρευνα [1][17][19].

Μια από τις πιο διαδεδομένες οικολογικές εφαρμογές είναι το πρόγραμμα Great Duck Island κοντά στην ακτή του Maine των ΗΠΑ. Στη συγκεκριμένη εφαρμογή το επιστημονικό προσωπικό χρησιμοποιεί ένα πρότυπο δίκτυο αισθητήρων για τη μελέτη του μικροκλίματος στο δυσπρόσιτο δίκτυο υπογείων φωλιών των θαλασσοπουλιών του είδους Storm-Petrel. Στα πλαίσια του προγράμματος τοποθετήθηκαν αισθητήρες για τη συνεχή μέτρηση μεγεθών, όπως η φωτεινότητα, η θερμοκρασία και η βαρομετρική πίεση. Η αναμετάδοση των μετρήσεων γίνεται σε τοπικούς υπολογιστές και κατόπιν, σε πραγματικό χρόνο, γίνεται η επεξεργασία στο εργαστήριο και η εξαγωγή συμπερασμάτων. Με τον τρόπο αυτό, οι βιολόγοι λαμβάνουν τις επιθυμητές πληροφορίες για την παρατήρηση των πουλιών και την προστασία του βιότοπου, με την ελάχιστη δυνατή ανθρώπινη παρέμβαση [17][20].

Εφαρμογές ασύρματων δικτύων αισθητήρων υλοποιήθηκαν ακόμα και σε ακραία περιβάλλοντα, όπου η συνεχής ανθρώπινη πρόσβαση είναι αδύνατη. Η παρακολούθηση ηφαιστείου είναι ένα παράδειγμα τέτοιων ακραίων εφαρμογών, όπου ένα δίκτυο αισθητήρων μπορεί εύκολα να αναπτυχθεί κοντά σε ένα ενεργό ηφαίστειο για τη συνεχή παρακολούθηση της ηφαιστειακής δραστηριότητας, παρέχοντας πληροφόρηση που με τα μέχρι πρότινος εργαλεία δεν ήταν εφικτή. Χαρακτηριστικά, δυο τέτοιες εφαρμογές έλαβαν χώρο σε δυο ηφαίστεια του Εκουαδόρ κατά την περίοδο 2004-2005 [17][21] με τρόπο που σχηματικά αναπαρίσταται στην Εικόνα 11.

ΣΧΗΜΑ 11 - Παρακολούθηση ηφαιστείου με ασύρματο δίκτυο αισθητήρων [12]



Ένα άλλο παράδειγμα εφαρμογής για την καλύτερη κατανόηση οικολογικών προβλημάτων είναι το δάσος Redwood στο Berkeley, το πρόβλημα του οποίου αφορά στην κατανόηση δυναμικών διεργασιών που συμβαίνουν μέσα στα δέντρα, με συνέπεια η συγκεκριμένη εφαρμογή να είναι έτσι σχεδιασμένη ώστε να λαμβάνει δείγματα από ένα πυκνό πλέγμα αισθητήρων τοποθετημένων στα δέντρα του δασικού συστήματος [17][22].

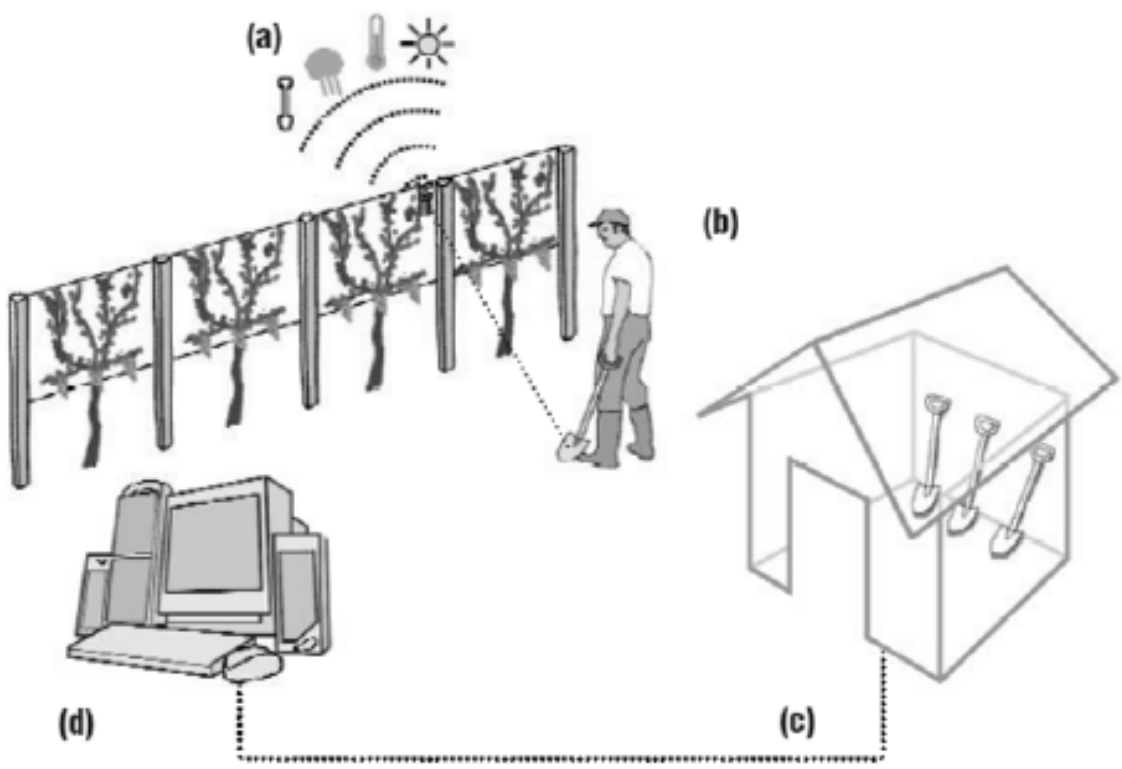
Τέλος, μια ακόμα σχετική εφαρμογή αφορά στο πανεπιστημίο του Princeton και συγκεκριμένα το πρόγραμμα ZebraNet με το οποίο παρακολουθείται η μετανάστευση, η συνύπαρξη με άλλα είδη και η νυχτερινή συμπεριφορά των πληθυσμών ζέβρας στην Αφρική [17][23].

6.3 Αγροτικές εφαρμογές

Μερικές σημαντικές εφαρμογές των ασύρματων δικτύων αισθητήρων στη γεωργία σχετίζονται με την ποιοτική και ποσοτική αναβάθμιση της αγροτικής παραγωγής. Στο πλαίσιο αυτών των εφαρμογών μπορούν να χρησιμοποιούνται αισθητήρες, που επιτρέπουν την παρακολούθηση των ακριβών επιπέδων του πόσιμου νερού, της διάβρωσης του εδάφους, της θερμοκρασίας, της υγρασίας και το βαθμό μόλυνσης του αέρα σε πραγματικό χρόνο.
Η παραπάνω παρακολούθηση επιτρέπει να παίρνονται αποφάσεις για την ορθολογική ρίψη λιπασμάτων, εντομοκτόνων, νερού στις φυτείες, όποτε, όπου και σε όση ποσότητα κρίνεται αναγκαίο [1].

Μια σχετική εφαρμογή στην αμπελουργία είναι γνωστή για την παγίωση του «έξυπνου αμπελώνα». Συγκεκριμένα, στον έξυπνο αμπελώνα, οι αισθητήρες ελέγχουν τις θρεπτικές ουσίες σε φυτά και έδαφος, κρατούν τις αμπέλους απαλλαγμένες από τα παράσιτα, εντοπίζουν την υγρασία και ειδοποιούν για τις

περιοχές όπου απαιτείται πότισμα. Επίσης, το πρόγραμμα λαμβάνει πληροφορίες από εκείνους που φροντίζουν τα αμπέλια, καλλιεργούν το χώμα και μαζεύουν τα σταφύλια καθώς και δεδομένα για τις ανάγκες των ιδιοκτητών των αμπελώνων, των οινοπαραγωγών και των πωλητών κρασιού. Με τον τρόπο αυτό επιτυγχάνεται, τόσο η αύξηση της παραγωγής, όσο και η ποιοτική βελτίωση του παραγόμενου κρασιού [24]. Στην Εικόνα 12 γίνεται σχηματική αναπαράσταση της λειτουργίας του έξυπνου αμπελώνα.



Σχήμα 12 - Εφαρμογή ασύρματου δικτύου αισθητήρων στην αμπελουργία [24]

6.4 Εφαρμογές πρόληψης καταστροφών και παροχής βοήθειας

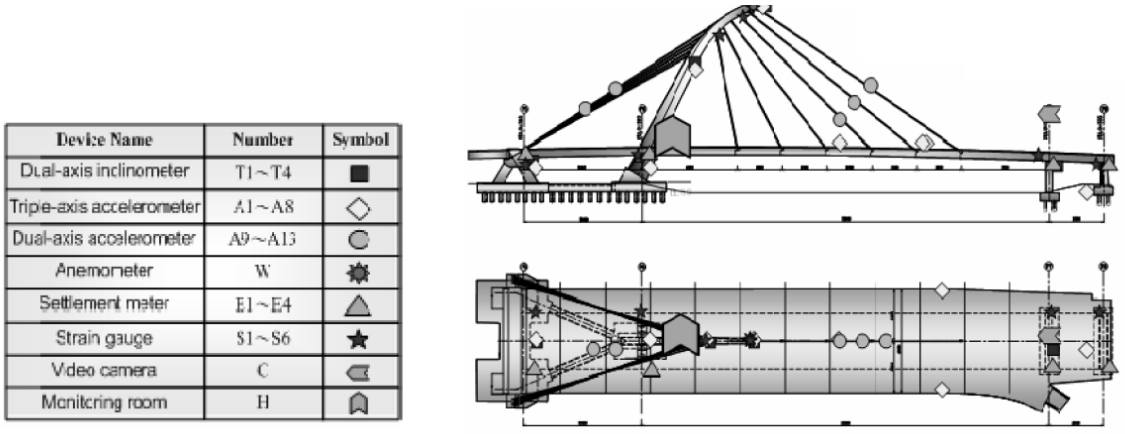
Τα ασύρματα δίκτυα αισθητήρων μπορούν να βρουν εφαρμογή σε μια σειρά από επείγουσες καταστάσεις εποπτεύοντας περιοχές με αυξημένο κίνδυνο εκδήλωσης κάποιας καταστροφής. Τυπικές εφαρμογές είναι η πυρανίχνευση, ο έλεγχος πλημυρών και ο έλεγχος τεχνικών κατασκευών[1][17][25].

Στον τομέα της πρόληψης εκδήλωσης πυρκαγιών η συμβολή των ασύρματων δικτύων αισθητήρων μπορεί να σώσει εκατοντάδες στρέμματα δάσους αλλά και ανθρώπινων ζωών. Εφόσον οι καιρικές συνθήκες που μπορούν να προκαλέσουν πυρκαγιά είναι προβλέψιμες, έχουν αναπτυχθεί σχετικές τεχνικές ανίχνευσης τέτοιων συνθηκών σε περιοχές που είναι επιρρεπείς σε πυρκαγιές. Η τοποθέτηση των αισθητήρων σε δύσβατες περιοχές είναι δυνατό να γίνει με ρίψη από αεροσκάφος, ενώ η τροφοδοσία επιτυγχάνεται για μεγάλα χρονικά διαστήματα με τη χρήση μπαταριάς ή και με ηλιακή ενέργεια, λαμβάνοντας υπόψη ότι εφαρμογές τέτοιου τύπου παραμένουν αδρανείς για μεγάλο χρονικό διάστημα και συνεπώς δεν αποτελούν ενεργοβόρα συστήματα.

Μια άλλη επείγουσα κατάσταση μπορεί να προκληθεί από πλημμύρες ύστερα από παρατεταμένες βροχοπτώσεις μιας θύελλας ή μιας καταιγίδας, τη γρήγορη τήξη μεγάλων ποσοτήτων χιονιού, φουσκωμένους ποταμούς εξαιτίας μεγάλων βροχοπτώσεων στις πηγές αυτών, καθώς και από κατάρρευση φραγμάτων ή αναχωμάτων κατασκευασμένων από τον άνθρωπο. Ανάλογα με το πιθανό αίτιο πρόκλησης μίας πλημμύρας σε κάποια συγκεκριμένη γεωγραφική περιοχή, μπορεί να εγκατασταθεί σε αυτήν ένα ασύρματο δίκτυο αισθητήρων για την έγκαιρη ανίχνευσή κι αντιμετώπισή της. Ένα παράδειγμα συστήματος ανίχνευσης πλημμύρων είναι το σύστημα ALERT, το οποίο και αναπτύχθηκε στις ΗΠΑ και για το οποίο χρησιμοποιήθηκαν διάφοροι τύποι αισθητήρων, όπως μέτρησης της στάθμης της βροχόπτωσης, της θερμοκρασίας, της

υγρασίας και της στάθμης του νερού. Τα δεδομένα από αυτές τις μετρήσεις αποστέλλονται σε μία ή περισσότερες κεντρικές αποθήκες δεδομένων, όπου και υφίστανται επεξεργασία για την αποτελεσματική πρόληψη, καθώς και την αντιμετώπιση των πλημμύρων[1].

Ένα άλλο παράδειγμα στον τομέα της πρόληψης καταστροφών είναι ο έλεγχος μεγάλων δημοσίων έργων και υποδομών. Οι κατασκευές υπόκεινται σε μακροπρόθεσμες καταπονήσεις λόγω εκτεταμένης λειτουργικής ζωής, διαβρώσεων, τριβών μεταξύ τους και σεισμικών δονήσεων. Συνεπώς, είναι σημαντική η επέκταση της ενεργής ζωής των υποδομών, μέσω της συλλογής ποιοτικών πληροφοριών για την κατάστασή τους. Με αυτό τον τρόπο γίνεται δυνατό για τους μηχανικούς να πραγματοποιούν προληπτικές επισκευές βασιζόμενοι περισσότερο σε μετρήσεις απόδοσης και λιγότερο σε προγραμματισμένες συντηρήσεις [26]. Στην Εικόνα 13 φαίνεται πως γίνεται η παρακολούθηση καταπόνησης μιας γέφυρας σε διάφορα σημεία της.



Device Name	Number	Symbol
Dual-axis inclinometer	T1~T4	■
Triple-axis accelerometer	A1~A8	◇
Dual-axis accelerometer	A9~A13	○
Anemometer	W	✹
Settlement meter	E1~E4	△
Strain gauge	S1~S6	★
Video camera	C	⊂
Monitoring room	H	⌂

Σχήμα 13 - Παρακολούθηση καταπόνησης ΑΔΑ σε γέφυρα [26]

6.5 Οικιακές εφαρμογές

Στις εφαρμογές για οικιακή χρήση τα ασύρματα δίκτυα αισθητήρων συμβάλλουν στην προώθηση των οικιακών αυτοματισμών, στην υλοποίηση έξυπνων σπιτιών με περιβάλλοντα που προσαρμόζονται ανάλογα με τις εξωτερικές συνθήκες ή τις επιλογές του χρήστη. Στόχος είναι η μείωση της σπατάλης σε ενέργεια με τον έλεγχο των συνθηκών στο εσωτερικό των κτιρίων όσο αφορά στην υγρασία, στον εξαερισμό και στον κλιματισμό (humidity, ventilation, air-conditioning - HVAC). Με αυτό τον τρόπο όχι μόνο πετυχαίνεται η εξοικονόμηση ενέργειας, αλλά βελτιώνεται και το βιοτικό επίπεδο των κατοίκων. Είναι επίσης δυνατός ο έλεγχος των μηχανικών επιπέδων πίεσης στις σεισμικά ενεργές ζώνες εξακριβώνοντας έτσι εάν το κτίριο είναι ασφαλές ή βρίσκεται στα όρια της κατάρρευσης καθώς επίσης και η ενσωμάτωση ασύρματων αισθητήρων σε συσκευές ώστε να δημιουργηθεί ένα αυτόνομο έξυπνο δίκτυο [1][17].

6.6 Βιομηχανικές εφαρμογές

Στην βιομηχανία τα ασύρματα δίκτυα αισθητήρων σε συνδυασμό με συστήματα ελέγχου μπορούν να εποπτεύουν όλη την γραμμή παραγωγή; για την ορθή λειτουργία της παραγωγής και την ασφάλεια του προσωπικού. Το περιβάλλον στο οποίο βρίσκουν εφαρμογή τα ΑΔΑ μπορεί να είναι επικίνδυνο για τον άνθρωπο ή ακόμα να είναι αδύνατη σε αυτό η ανθρώπινη πρόσβαση.

Υπάρχουν πολλά παραδείγματα βιομηχανικών εφαρμογών που σχετίζονται με τον έλεγχο διαφόρων δυσπρόσιτων παραγωγικών περιοχών, όπως έλεγχος στο εσωτερικό μηχανών και σε υπόγειες παραγωγικές διαδικασίες, οι οποίες για

προφανής λόγους είναι αρκετά επικίνδυνες και δύσκολες στον χειρισμό. Τα διυλιστήρια είναι ένας χώρος όπου τα ασύρματα δίκτυα αισθητήρων χρησιμοποιούντα για μέτρηση και καταγραφή στα διάφορα στάδια των διεργασιών. Ο έλεγχος της παραγωγής επιτυγχάνεται με ειδικά σήματα συναγερμών που εκπέμπουν ασύρματοι αισθητήρες με αποτέλεσμα να ειδοποιούνται οι τεχνικοί όταν η θερμοκρασία ή η πίεση βγαίνει εκτός ορίων.

Μια ακόμη σχετική εφαρμογή είναι η μέτρηση των μη φυσιολογικών δονήσεων κατά τη διάρκεια γεωτρήσεων και η προειδοποίηση των μηχανικών για πιθανή επερχόμενη βλάβη του εξοπλισμού. Τέλος, αξίζει να αναφερθεί μία ακόμη εφαρμογή σχετική με τον έλεγχο διαφόρων υπογείων αγωγών από τα ασύρματα δίκτυα αισθητήρων, είτε πρόκειται για αποχετευτικούς ή υδρευτικούς αγωγούς, είτε δεξαμενές και αγωγούς φυσικού αερίου [27], όπου η ανθρώπινη πρόσβαση μπορεί να χαρακτηριστεί από εξαιρετικά δύσκολη έως ανέφικτη.

6.7 Εφαρμογές στην υγεία

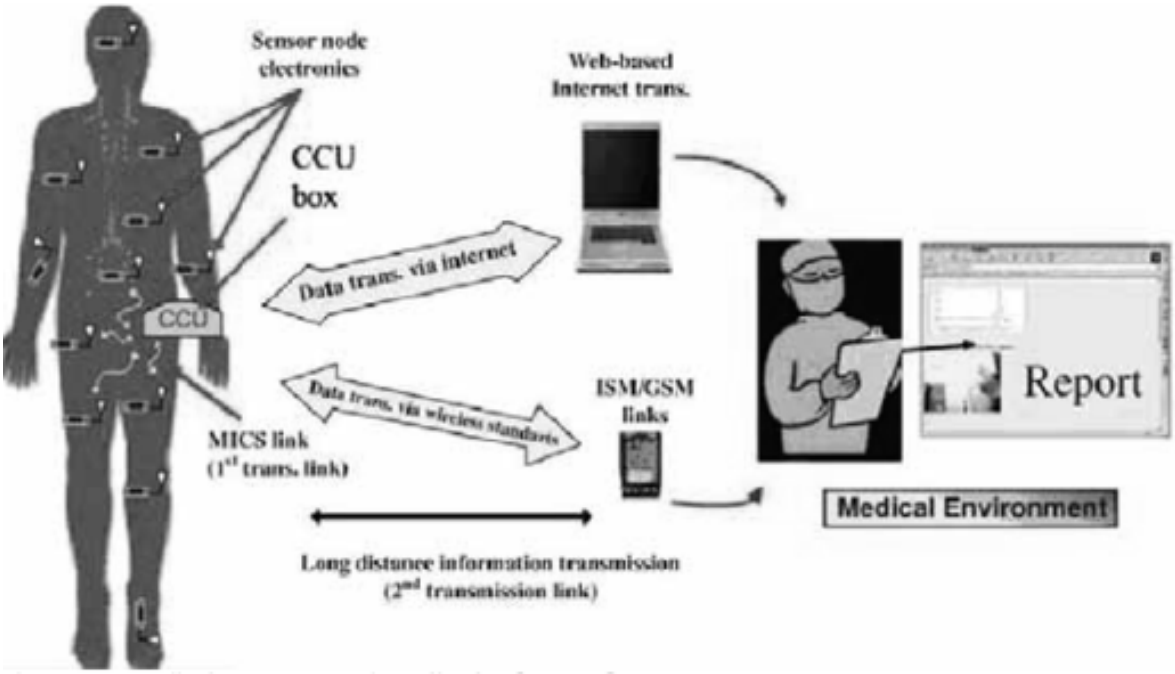
Οι εφαρμογές στον τομέα της υγείας είναι μια ιδιαίτερη και ξεχωριστή κατηγορία των εφαρμογών ασύρματων αισθητήρων που συνήθως τη συναντάμε με το όνομα BSN (Body Sensor Network). Η δυσκολία και το σημείο διαφοροποίησης τους είναι ότι αφορούν μετρήσεις στο ανθρώπινο σώμα. Η ανάγκη για την πρόληψη και αποφυγή οποιουδήποτε λάθους καθώς και η πολυπλοκότητα του ανθρώπινου σώματος, καθιστούν την ανάπτυξη του τομέα αρκετά αργή.

Η τάση σε αυτό τον τομέα είναι η παρακολούθηση ασθενών στην εντατική ή η κατά την μετά-εγχειρητική περίοδο από απομακρυσμένη, κατ' οίκον παρακολούθηση, σε περιπτώσεις χρόνιων παθήσεων ή ηλικιωμένων. Η καινοτομία των ΑΔΑ εφαρμογών έγκειται στις συνθήκες πλήρους κινητικότητας

που παρέχουν στους χρήστες τους σε συνδυασμό με την αίσθηση ασφάλειας που συνεπάγεται η διαρκής αλλά ταυτόχρονα διακριτική και μη παρεμβατική παρακολούθηση της υγείας τους. Έτσι, μέσω της τηλεϊατρικής επιτυγχάνεται η κατά το δυνατόν αποδέσμευση του ασθενούς από τους νοσοκομειακούς περιορισμούς.

Βασική επιδίωξη των υπηρεσιών που προσφέρονται από τα ΑΔΑ στον τομέα τηε υγείας, είναι ο διαρκής και εξ αποστάσεως έλεγχος της κατάστασης της υγείας μέσω της συλλογής, επεξεργασίας, αξιολόγησης, αξιοποίησης και αποθήκευσης της κατάλληλης ιατρικής πληροφορίας. Έτσι, είναι δυνατή η επίτευξη ενός καλύτερου επιπέδου ζωής αλλά και πιο φθηνού κόστους ιατρικής περίθαλψης για όλους.

Συμπληρωματικά, αξίζει να αναφερθεί πως στο μέλλον τα ΑΔΑ μπορούν να χρησιμοποιηθούν ακόμα και για την πρόληψη δυσάρεστων καταστάσεων με τη βοήθεια των ανιχνευτικών συστημάτων καταγραφής θέσης και κατάστασης ασθενών [1][6][17][28][29].



Σχήμα 14 - Εφαρμογές ΑΔΑ στην ιατρική [21]

6.8 Εφαρμογές στις συγκοινωνίες

Τα τελευταία χρόνια στο χώρο των μεταφορών και συγκοινωνιών έχει παρατηρηθεί μεγάλη αξιοποίηση των τεχνολογιών της ηλεκτρονικής και πληροφορικής, όπως τα ασύρματα δίκτυα αισθητήρων. Συγκεκριμένα, υπάρχουν πολλές έρευνες για το πώς τα ασύρματα δίκτυα αισθητήρων δύνανται να χρησιμοποιηθούν για τον καλύτερο έλεγχο της κυκλοφορίας οχημάτων στις λεγόμενες έξυπνες λεωφόρους καθώς και μια αυξανόμενη τάση για τα οχήματα να ενσωματώνουν όλο και περισσότερους αισθητήρες.

Η αρχή λειτουργίας τέτοιων εφαρμογών βασίζεται στο ότι τα οχήματα ανταλλάσουν πληροφορίες για τις διάφορες συνθήκες που συναντά ο προπορευόμενος όπως: ολισθηρό οδόστρωμα, απότομο φρενάρισμα, μποτιλιαρίσματα, έργα στο οδόστρωμα κτλ. με σκοπό την προώθηση της ασφαλούς οδήγησης, της μείωσης των ατυχημάτων, του ελέγχου των ορίων ταχύτητας του συγκοινωνιακού φόρτου, αλλά και της πιο ξεκούραστης οδήγησης.

Οι προαναφερθείσες λειτουργίες αφορούν στο παρόν την εξυπηρέτηση του οδηγού, αλλά το προσδοκώμενο αποτέλεσμα για το εγγύς μέλλον είναι το κάθε όχημα να μετακινείται από μόνο του χωρίς να χρειάζεται η ανθρώπινη παρέμβαση σε συνεργασία όμως πάντα με τα υπάρχοντα δίκτυα GPS [1][17].

6.9 Εφαρμογές επιτήρησης

Τα ασύρματα δίκτυα αισθητήρων έχοντας την δυνατότητα να αντιλαμβάνονται μεταβολές φυσικών φαινομένων όπως: η μεταβολή της επιτάχυνσης, η καταγραφή της θέσης και άλλες, καθιστούν εφικτή την ανάπτυξη εφαρμογών σχετικές με την επίβλεψη κιβωτίων, δεμάτων και άλλων αντικειμένων. Σε αυτή την κατηγορία εφαρμογών ανήκουν και εκείνες που αναφέρονται στην παρακολούθηση χώρων για λόγους ασφάλειας και στην ενημέρωση κάποιας εποπτεύουσας εφαρμογής σε τακτά χρονικά διαστήματα. Η εποπτεύουσα εφαρμογή μπορεί μέσω των κόμβων να ενημερωθεί για την εκδήλωση ενός περιστατικού ενδιαφέροντος, όπως για παράδειγμα την παραβίαση ενός χώρου [1][17].

6.10 Στρατιωτικές εφαρμογές

Τα δίκτυα ασύρματων αισθητήρων αναπτύχτηκαν όπως και πολλές άλλες επιστημονικές και τεχνολογικές ανακαλύψεις από την τάση που δημιουργούν οι στρατιωτικοί ανταγωνισμοί, καθώς πολλές ανακαλύψεις αναδύθηκαν είτε από κάποιο πόλεμο είτε στα στρατιωτικά εργαστήρια και αργότερα βρήκαν εφαρμογή σε τομείς που προάγουν και εξυπηρετούν άλλες καθημερινές ανάγκες του ανθρώπου.

Από όσα είναι δυνατόν να είναι γνωστά λόγω του στρατιωτικού απόρρητου, τα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται για την επιτήρηση στρατιωτικών εγκαταστάσεων, των συνόρων ενός κράτους, όπως επίσης και για την αναγνώριση των φίλιων πυρών στο πεδίο της μάχης, την εκτίμηση των ζημιών μετά από μία μάχη, τη στόχευση, την παρακολούθηση του πεδίου της μάχης, την αναγνώριση των εχθρικών δυνάμεων και του εδάφους, την ανίχνευση πυρηνικών, βιολογικών και χημικών απειλών και πολλά άλλα.

Ένα ασύρματο δίκτυο αισθητήρων μπορεί να χρησιμοποιηθεί στο πεδίο της μάχης για τη συλλογή δεδομένων που αφορούν την κατάσταση, τη θέση και τον οπλισμό των στρατευμάτων σε πραγματικό χρόνο. Τα δεδομένα αυτά αποστέλλονται στους αρχηγούς και επικεφαλείς του στρατεύματος, βοηθώντας στη λήψη των κατάλληλων αποφάσεων, κατά τη διάρκεια μιας εμπόλεμης κατάστασης [1][17].

7 Ασφάλεια Ασύρματων Δικτύων Αισθητήρων

7.1 Εισαγωγή

Στο παρόν κεφάλαιο, θα αναφερθούμε συγκεκριμένα στην ασφάλεια των ασύρματων δικτύων αισθητήρων. Όπως είναι αντιληπτό, το πρόβλημα της ασφάλειας είναι ιδιαίτερα σημαντικό στα ασύρματα δίκτυα αισθητήρων καθώς πλέον είναι ένας καθοριστικός παράγοντας για μια σειρά από εφαρμογές. Χαρακτηριστικά παραδείγματα είναι οι στρατιωτικές εφαρμογές, οι εφαρμογές βιομηχανικού ελέγχου, οι ιατρικές εφαρμογές και γενικά οπουδήποτε κρίσιμες αποφάσεις εξαρτώνται από πληροφορίες οι οποίες συγκεντρώνονται και επεξεργάζονται στα δίκτυα αυτά.

Η έννοια της ασφάλειας ενός ασύρματου δικτύου αισθητήρων σχετίζεται με την ικανότητα της προστασίας των πληροφοριών του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στις εξουσιοδοτημένες οντότητες όταν τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Αν και η ασφάλεια στα δίκτυα υπολογιστών είναι μια καλά εδραιωμένη επιστημονική περιοχή, με πρωτόκολλα και πρότυπα τα οποία τυγχάνουν ευρείας αναγνώρισης, η προσαρμογή και χρησιμοποίηση αυτών στα δίκτυα ασυρμάτων αισθητήρων, είναι τις περισσότερες φορές, αν όχι αδύνατη, πάρα πολύ δύσκολη, εξαιτίας των ιδιαίτερων χαρακτηριστικών των δικτύων αισθητήρων τόσο εξαιτίας των περιορισμών των κόμβων που τα απαρτίζουν,

όσο και εξαιτίας των ιδιαίτερων χαρακτηριστικών των εφαρμογών στις οποίες χρησιμοποιούνται.

7.2 Απαιτήσεις ασφαλείας

Σε ότι έχει να κάνει με την ασφάλεια, είναι άξιο αναφοράς να τονίσουμε πως αποτελεί ίσως το σημαντικότερο κομμάτι κατά τη δημιουργία και ανάπτυξη ενός ασύρματου δικτύου. Για τον λόγο αυτό πρέπει κατά την σχεδίαση να ληφθεί μέριμνα ώστε το ασύρματο δίκτυο να μπορεί να αντιμετωπίσει ένα πλήθος πιθανών επιθέσεων ανάλογα πάντα με τις απαιτήσεις, τις ιδιαιτερότητες, τις τεχνικές προδιαγραφές της εκάστοτε εφαρμογής. Για την αντιμετώπιση των απειλών ένα ασύρματο δίκτυο πρέπει να μπορεί να τηρεί τις αρχές ασφαλείας. Οι σημαντικότερες απαιτήσεις ασφαλείας περιγράφονται παρακάτω.

1. **Διαθεσιμότητα**: Ορίζοντας την Διαθεσιμότητα, θα λέγαμε πως ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Με τον όρο διαθεσιμότητα εννοούμε ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργούν, παρά τις όποιες τυχόν διαταραχές, όπως διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες καθώς και οι κόμβοι του δικτύου δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (Denial of Service - DoS) όταν επιθυμούν να προσπελάσουν τους πόρους του δικτύου. Τα συστήματα που εξασφαλίζουν τη διαθεσιμότητα προσπαθούν να καταπολεμήσουν τις επιθέσεις κατανάλωσης ενέργειας, καθώς επίσης την παρεκτροπή των κόμβων και την εγωιστική συμπεριφορά τους κατά την προώθηση μηνυμάτων [33].
2. **Εμπιστευτικότητα**: Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από

μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των κόμβων ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένες οντότητες. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Η συνήθης τακτική για να κρατηθούν ευαίσθητα δεδομένα ασφαλή είναι η κρυπτογράφηση των δεδομένων με ένα μυστικό κλειδί, το οποίο μόνο οι επίδοξοι λήπτες κατέχουν. Επειδή η κρυπτογράφηση δημόσιου κλειδιού είναι πολύ ενεργοβόρα στα δίκτυα αισθητήρων, τα περισσότερα από τα προτεινόμενα πρωτόκολλα χρησιμοποιούν μεθόδους κρυπτογράφησης συμμετρικού κλειδιού.

3. **Ακεραιότητα**: Η ακεραιότητα είναι ουσιαστικά η επιβεβαίωση ότι τα δεδομένα που έχουν αποσταλεί, παραληφθεί ή αποθηκευτεί είναι πλήρη και δεν έχουν υποστεί αλλοίωση. Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι, δηλαδή σημαίνει πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων. Επομένως η μετατροπή, διαγραφή και δημιουργία των δεδομένων εντός ενός ασύρματου δικτύου αισθητήρων, πρέπει να γίνεται μόνο από εξουσιοδοτημένα μέρη. Κάπου εδώ να προσθέσουμε ότι ένα καλό και ασφαλές σύστημα θα ήταν ικανό να ανιχνεύσει οποιοδήποτε πρόβλημα ακεραιότητας ώστε αν μια παράβαση διαπιστωθεί, τότε άμεσα η υπηρεσία να αναφέρει αυτό το πρόβλημα. Εάν έχει εφαρμοσθεί ένας εύρωστος μηχανισμός εμπιστευτικότητας, η ακεραιότητα πληροφορίας είναι τόσο απλή, όπως η προσθήκη κατατεμαχισμών πριν την κρυπτογράφηση των μηνυμάτων [34].

4. **Αυθεντικότητα** Η αυθεντικότητα επιτρέπει σε ένα κόμβο να διασφαλίσει την ταυτότητα του επικοινωνούντα κόμβου. Χωρίς την αυθεντικότητα, ένας αντίπαλος μπορεί να μεταμφιέσει έναν κόμβο και έτσι να κερδίσει μη

εξουσιοδοτημένη πρόσβαση σε πηγές του δικτύου, σε ευαίσθητες πληροφορίες και να παρέμβει στις λειτουργίες άλλων κόμβων. Έτσι, η αυθεντικότητα είναι απαραίτητη για πολλούς εκτελεστικούς σκοπούς του προγράμματος, όπως εκ νέου προγραμματισμός του δικτύου, έλεγχος κύκλου ασφαλείας σ' ένα κόμβο κ.ά. Η αυθεντικότητα πληροφορίας επιτρέπει στον δέκτη να επιβεβαιώσει ότι η πληροφορία στάλθηκε τοπικά από τον πραγματικό αποστολέα. Σε επικοινωνία δύο μερών, η αυθεντικότητα μπορεί να επιτευχθεί με έναν καθαρά συμμετρικό μηχανισμό: Ο αποστολέας και ο λήπτης μοιράζονται ένα μυστικό κλειδί με το οποίο υπολογίζουν έναν κώδικα αυθεντικότητας μηνύματος (message authentication code-MAC) για όλα τα αποστελλόμενα δεδομένα. Όταν ένα μήνυμα με τον σωστό MAC φτάσει, ο λήπτης ξέρει ότι στάλθηκε από τον αποστολέα. Όμως, κατά την εκπομπή μηνύματος προς πολλούς αποδέκτες, χρειάζονται ισχυρότεροι δεσμοί εμπιστοσύνης. Σε αυτή την περίπτωση, μπορούν να χρησιμοποιηθούν άλλες τεχνικές όπως είναι τα πρωτόκολλα SPINS (Security Protocols for Sensor Networks - SPINS) και LEAP (Localized Encryption and Authentication Protocols - LEAP) [35-37].

5. **Μη αποποίηση** Σχετικά με την απαίτηση της μη αποποίησης, να αναφέρουμε ότι αυ Υπάρχουν ορισμένα χαρακτηριστικά των δικτύων τα οποία έχουν συγκεκριμένες επιπτώσεις. Παρακάτω παρουσιάζονται αναλυτικά αυτά τα χαρακτηριστικά και οι επιπτώσεις τους στην ασφάλεια [32][36][51].

6. **Φρεσκάδα πληροφοριών (data freshness):** Δηλώνει ότι οι πληροφορίες και τα μηνύματα που ανταλλάσσονται είναι πρόσφατα και διαβεβαιώνει ότι δεν επαναλαμβάνεται αναμετάδοση παλαιών μηνυμάτων. Σε όλα τα μηνύματα, συνήθως, παρέχεται ένας καταμετρητής χρόνου. Βάσει αυτού του μετρητή μπορούμε να διασφαλίσουμε ότι ένα μήνυμα είναι φρέσκο. Με αυτό τον τρόπο

εξασφαλίζεται η προστασία από τις επιθέσεις επανεκπομπής μηνυμάτων, καθώς επίσης και από την άσκοπη κατανάλωση ενεργειακών πόρων στους κόμβους από μηνύματα τα οποία για κάποιο λόγο κυκλοφορούν σε ατέρμονες βρόχους [35][36].

7.3 Κενά ασφαλείας και ευπάθειες στα ασύρματα δίκτυα αισθητήρων

Σχετικά με τα κενά ασφαλείας και τις ευπάθειες στα ασύρματα δίκτυα αισθητήρων, να πούμε ότι τα χαρακτηριστικά των ασύρματων δικτύων αισθητήρων που εξετάζουμε, όπως η χαμηλή υπολογιστική ισχύς, η περιορισμένη ικανότητα αποθήκευσης, η περιορισμένη διαθέσιμη ενέργεια και ο μεγάλος αριθμός κόμβων. Έτσι λοιπόν, και οι ιδιαιτερότητες της κάθε εφαρμογής, στις οποίες χρησιμοποιούνται, μεταξύ των οποίων μπορεί να είναι η λειτουργία σε αφιλόξενα περιβάλλοντα, η ελλιπής γνώση της τοπολογίας στην περιοχή ανάπτυξης, οι δυνατότητες αυτό οργάνωσης και αυτόματης διόρθωσης δυσλειτουργιών και η λειτουργία χωρίς ανθρώπινη επιτήρηση, κάνουν μη πρακτική την χρήση των περισσότερων αλγορίθμων ασφαλείας. Για παράδειγμα, η μνήμη ενός αισθητήρα είναι ανεπαρκής στην αποθήκευση των απαραίτητων μεταβλητών που χρειάζονται στους αλγόριθμους ασύμμετρης κρυπτογράφησης[35].

Υπάρχουν ορισμένα χαρακτηριστικά των δικτύων τα οποία έχουν συγκεκριμένες επιπτώσεις. Παρακάτω παρουσιάζονται αναλυτικά αυτά τα χαρακτηριστικά και οι επιπτώσεις τους στην ασφάλεια [32][36][51].

1. **Ασύρματές συνδέσεις:** Η χρήση ασύρματων συνδέσεων καθιστά τα δίκτυα αισθητήρων ευαίσθητα σε επιθέσεις. Σε αντίθεση με τα ενσύρματα

δίκτυα στα οποία ένας αντίπαλος πρέπει να κερδίσει φυσική πρόσβαση στα καλώδια των δικτύων ή να περάσει διαμέσου αρκετών γραμμών άμυνας στα firewalls και στις πύλες εξόδου, οι επιθέσεις στα ασύρματα δίκτυα μπορούν να έρθουν από όλες τις κατευθύνσεις και να στοχεύσουν οποιοδήποτε κόμβο. Γι' αυτό, τα δίκτυα αυτά δεν θα έχουν μια καθαρή γραμμή άμυνας και κάθε κόμβος πρέπει να είναι προετοιμασμένος για να αμυνθεί στις επιθέσεις.

2. **Έλλειψη υποδομής:** Τα ασύρματα δίκτυα αισθητήρων οργανώνονται με τέτοιο τρόπο ώστε οι κεντρικοί επεξεργαστές, το ειδικευμένο λογισμικό και οι σταθεροί δρομολογητές είναι απόντες. Η έλλειψη αυτής της υποδομής αποκλείει την ανάπτυξη κεντρικής διαχείρισης. Οι κόμβοι υποστηρίζουν ισόνομες σχέσεις και έτσι οποιοδήποτε σχήμα ασφαλείας στηρίζεται σε κατανεμημένα συνεργατικά σχήματα και όχι σε κεντρικά σχήματα ασφαλείας.

3. **Πολλαπλά άλματα**: Η έλλειψη κεντρικών δρομολογητών επιβάλει στους κόμβους να είναι από μόνοι τους δρομολογητές. Τα πακέτα περνούν από πολλούς κόμβους-δρομολογητές πριν φτάσουν στον τελικό προορισμό. Λόγω της πιθανής αναξιοπιστίας αυτών των κόμβων, το χαρακτηριστικό αυτό αποτελεί ένα σημείο κενού ασφάλειας των δικτύων αισθητήρων.

4. **Μη σταθεροί κόμβοι**: Κάπου εδώ να αναφέρουμε ότι αρκετές εφαρμογές απαιτούν οι κόμβοι να μην είναι σταθεροί αλλά να μετακινούνται ανάλογα με την προς εποπτεία περιοχή. Οι διαδρομές που θα ακολουθήσουν δεν μπορούν να προκαθοριστούν. Αυτό σημαίνει ότι η ανίχνευση ενός συγκεκριμένου κόμβου σ' ένα δίκτυο ευρείας κλίμακας δεν μπορεί να γίνει εύκολα. Επιπλέον να προσθέσουμε πως η κινητικότητα των κόμβων και η ασύρματη διασύνδεση επιτρέπει τους κόμβους να εισέρχονται και να φεύγουν από ένα δίκτυο. Έτσι, η τοπολογία του δικτύου δεν είναι σταθερή ως προς το σχήμα και το μέγεθος, αλλά αλλάζει συνεχώς. Για να δημιουργηθεί ένα καλό σύστημα

ασφαλείας πρέπει να ληφθεί υπ' όψιν αυτό το χαρακτηριστικό των δικτύων ώστε να επιτραπεί η δημιουργία ασφαλούς σύνδεσης με οποιοδήποτε κόμβο εισέρχεται στο δίκτυο.

5. **Περιορισμένη ενέργεια**: Η περιορισμένη συνήθως ενέργεια θα μπορούσαμε να πούμε πως είναι ένα από τα μεγαλύτερα προβλήματα ασφάλειας στα ασύρματα δίκτυα αισθητήρων. Συνήθως τα δίκτυα αυτά διαθέτουν περιορισμένη ενέργεια που προέρχεται από συσσωρευτές. Η αντικατάσταση ή επαναφόρτιση των συσσωρευτών αυτών κρίνεται είτε αδύνατη λόγω τοποθεσίας είτε αντιοικονομική. Έτσι, οι συσκευές παροχής ενέργειας που έχουν μαζί τους οι κόμβοι πρέπει να προφυλάσσονται για να παρατείνουν τον χρόνο ζωής των κόμβων αλλά και του δικτύου. Όταν εφαρμόζεται μια κρυπτογραφική λειτουργία ή ένα πρωτόκολλο σε έναν κόμβο, πρέπει να λαμβάνεται υπ' όψιν η επιπλέον ενεργειακή επιβάρυνση από τον κώδικα ασφαλείας. Όταν θέλουμε να εφαρμόσουμε ένα σύστημα ασφαλείας, μας ενδιαφέρει να μην μειώνεται ο μέγιστος χρόνος ζωής των κόμβων από το σύστημα.
6. **Περιορισμένη μνήμη**: Συνήθως να σημειώσουμε ότι οι κόμβοι των δικτύων αισθητήρων απαιτείται να έχουν μικρό μέγεθος και χαμηλή τιμή, δεδομένου ότι χρειάζονται αρκετοί για την υλοποίηση μιας εφαρμογής. Αποτέλεσμα είναι οι κόμβοι να διαθέτουν περιορισμένη μνήμη από την οποία ένα ποσοστό θα καταναλώσει ο κώδικας της εφαρμογής. Επομένως, για να δημιουργηθεί ένας αποτελεσματικός μηχανισμός ασφαλείας, είναι αναγκαίο να περιοριστεί ο κώδικας του αλγόριθμου ασφαλείας.
7. **Δρομολόγηση** Πολύ χρήσιμο θα ήταν να ειπωθεί πως η δρομολόγηση και η προώθηση των δεδομένων είναι βασικές λειτουργίες ενός δικτύου για την επικοινωνία. Σε αντίθεση με τα παραδοσιακά δίκτυα όπου η λειτουργία της δρομολόγησης εκτελείται από συγκεκριμένους κόμβους και δρομολογητές, στα δίκτυα αισθητήρων η δρομολόγηση συνήθως

εκτελείται από όλους τους κόμβους. Επιπλέον, οι κοινοί μηχανισμοί ασφάλειας κατά τη δρομολόγηση που αποτελείται από την αυθεντικότητα του κόμβου και του μηνύματος, αναφέρονται σε ένα εκ τον προτέρων μοντέλο εμπιστοσύνης στο οποίο νόμιμοι δρομολογητές πιστεύεται ότι εκτελούν τις σωστές εργασίες. Όμως η αυθεντικότητα του κόμβου ή των μηνυμάτων του δεν εγγυάται τη σωστή εκτέλεση της δρομολόγησης σε ανοιχτά περιβάλλοντα με έλλειψη εμπιστοσύνης.

7.4 Επιθέσεις

Επειδή τα δίκτυα αισθητήρων τις περισσότερες φορές αναπτύσσονται σε περιβάλλοντα, στα οποία δεν μπορεί να γίνει εύκολα η συντήρηση του δικτύου, θα πρέπει να πούμε πως είναι αναγκαίο λοιπόν, να λάβουμε μέριμνα ώστε το δίκτυο να γνωρίζει τις πιθανές απειλές καθώς επίσης και τους μηχανισμούς ώστε να προστατευτεί από τις επιθέσεις. Οι απειλές που δέχεται ένας κόμβος του δικτύου μπορούν να χωριστούν, στις επιθέσεις και στην κακή συμπεριφορά [33].

Σαν Επίθεση ορίζουμε οποιαδήποτε πράξη που σκόπιμα προσπαθεί να προκαλέσει ζημιά στο δίκτυο. Μπορούμε να τις χωρίσουμε ανάλογα με την προέλευση τους και την φύση τους. Μια κατηγοριοποίηση με βάση την προέλευση χωρίζει τις επιθέσεις σε εξωτερικές και εσωτερικές.

1. Εξωτερικές επιθέσεις: είναι οι επιθέσεις όπου ένας κόμβος εκτός του δικτύου μπορεί να παρακολουθήσει πακέτα που αποστέλλονται από τους κόμβους του δικτύου για κακόβουλους σκοπούς και να εισάγει στο δίκτυο μη έγκυρα πακέτα με σκοπό την διατάραξη της λειτουργιάς του δικτύου.
2. Εσωτερικές επιθέσεις: είναι οι επιθέσεις που προκαλούνται από μέλη του δικτύου και είναι αρκετά δύσκολο να ανιχνεύουν αφού η προτεινόμενη

άμυνα για τις εξωτερικές επιθέσεις είναι άχρηστη εναντίον εσωτερικών εχθρών [38].

Οι επιθέσεις μπορούν να ταξινομούνται και ανάλογα με την φύση τους. Έτσι χωρίζονται σε παθητικές και ενεργητικές επιθέσεις.

1. Παθητικές επιθέσεις: είναι οι επιθέσεις κατά τις οποίες κάποια μη εξουσιοδοτημένη οντότητα κάνει ακρόαση και συλλέγει πληροφορίες από το κανάλι επικοινωνίας. Λόγω της φύσης του μέσου διάδοσης των ασύρματων επικοινωνιών που είναι ευρέως διαμοιραζόμενο, είναι εύκολο για έναν επιτιθέμενο να εκκινήσει μια τέτοια επίθεση σε αυτό το περιβάλλον, παρά σε ένα κλασικό ενσύρματο περιβάλλον.
2. Ενεργητικές επιθέσεις: είναι οι επιθέσεις κατά τις οποίες οι επιτιθέμενοι παρακολουθούν ακούν και τροποποιούν τη ροή των δεδομένων στο κανάλι επικοινωνίας [39].

Σαν απειλές κακής συμπεριφοράς ορίζονται οι αυθαίρετες συμπεριφορές εσωτερικών κόμβων που μπορούν να οδηγήσουν αθέλητα σε καταστροφή άλλων κόμβων. Ο στόχος του κόμβου δεν είναι να επιτεθεί σε έναν άλλο κόμβο, αλλά μπορεί να έχει άλλους στόχους, όπως να αποκτήσει ένα άδικο πλεονέκτημα σε σύγκριση με άλλους κόμβους. Για παράδειγμα, ένας κόμβος μπορεί να μην εκτελέσει σωστά το πρωτόκολλο MAC με σκοπό να λάβει μεγαλύτερο εύρος ζώνης ή μπορεί να αρνηθεί να προωθήσει πακέτα για άλλους για να μην καταναλώσει κομμάτι της ενέργειάς του, ενώ χρησιμοποιεί την ενέργειά του και ζητά από άλλους κόμβους να προωθούν τα δικά του πακέτα.

7.4.1 Επιθέσεις στα διάφορα επίπεδα δικτύου

Οι επιθέσεις στα ασύρματα δίκτυα αισθητήρων στοχεύουν σε διαφορετικές λειτουργίες του δικτύου ανάλογα με τα χαρακτηριστικά και τον τρόπο δράσης της απειλής. Για το λόγο αυτό τα αντίμετρα και η συνολική πολιτική ασφάλειας πρέπει να σχεδιάζονται όχι μεμονωμένα και ανεξάρτητα, αλλά με μια πολυεπίπεδη προοπτική και αρχιτεκτονική. Παρακάτω περιγράφουμε τα κενά ασφαλείας, τις συνήθεις επιθέσεις και τρόπους αντιμετώπισης κατηγοριοποιημένα με βάση το επίπεδο του δικτύου [31].

7.4.1.1 Επιθέσεις στο φυσικό επίπεδο

Οι επιθέσεις στο φυσικό επίπεδο πραγματοποιούνται μέσο μετάδοσης ή στους κόμβους. Στις επιθέσεις προς το μέσο μετάδοσης, ο επιτιθέμενος προσπαθεί να σταματήσει τη λειτουργία του δικτύου, μέσω παρεμβολών στο ραδιοφωνικό φάσμα εκπομπής (jamming attack). Η χρήση ισχυρών παρεμβολών, οι οποίες κατακλύζουν την περιοχή του ραδιοφωνικού φάσματος συχνοτήτων που χρησιμοποιεί το δίκτυο με θόρυβο, επιφέρει αδυναμία ανταλλαγής μηνυμάτων ανάμεσα στους κόμβους. Ένα αντίμετρο το οποίο αντιμετωπίζει ικανοποιητικά την παραπάνω απειλή είναι η χρήση τεχνικών διαμόρφωσης εύρους φάσματος στο σήμα και μεταπήδησης συχνότητας για τη μετάδοση. Οι τεχνικές αυτές επιτρέπουν την επικοινωνία μόνο σε κόμβους οι οποίοι γνωρίζουν εκ των προτέρων το χρησιμοποιούμενο μοντέλο επικοινωνίας, αποκρύπτοντας την ύπαρξη και λειτουργία των κόμβων στην περιοχή ανάπτυξής τους.

Στις επιθέσεις ενάντια στους κόμβους (tampering attack), ο επιτιθέμενος εκμεταλλεύεται τη λειτουργία των κόμβων σε περιοχές μη ελεγχόμενες και στοχεύει στην φυσική καταστροφή τους καθώς και στην απόκτηση τυχόν πολύτιμων δεδομένων, τα οποία είναι αποθηκευμένα σε αυτούς. Η κύρια προστασία ενάντια σε αυτού του είδους την επίθεση, είναι η χρήση μηχανισμών

προστασίας ενάντια στην παραβίαση, καθώς και το μικρότερο δυνατό μέγεθος και η χρήση τεχνικών φυσικής απόκρυψης των κόμβων [31][36][40].

7.4.1.2 Επιθέσεις στο επίπεδο ζεύξης δεδομένων

Στο επίπεδο της ζεύξης δεδομένων μπορούμε να εντοπίσουμε δύο είδη επιθέσεων, τις επιθέσεις οι οποίες προκαλούν σύγκρουση των μεταδιδόμενων πακέτων δεδομένων και τις επιθέσεις οι οποίες στοχεύουν στην εξάντληση των αποθεμάτων ενέργειας των συσσωρευτών.

Οι πρώτες στοχεύουν σε δίκτυα τα οποία χρησιμοποιούν MAC πρωτόκολλα τα οποία λειτουργούν με το σχήμα Ready-To-Send/Clear-To-Send (RTS/CTS). Στα δίκτυα αυτά ο επιτιθέμενος τοποθετεί στην περιοχή τού δικτύου κόμβους οι οποίοι λαμβάνουν τα μηνύματα (RTS/CTS), υποδύονται ότι είναι οι νόμιμοι αποδέκτες του αιτήματος και χωρίς να επιβεβαιώνουν ότι έχει γίνει επιτυχής λήψη μηνύματος με CTS με αποτέλεσμα να εξαναγκάζεται ο κόμβος να εκπέμπει συνεχώς RTS πακέτα, καταργώντας ουσιαστικά τη δυνατότητα επικοινωνίας του με το υπόλοιπο δίκτυο. Η βασικότερη μέθοδος αντιμετώπισης της παραπάνω επίθεσης, είναι με τη χρήση πρωτοκόλλων MAC τα οποία δεν επιτρέπουν τις συγκρούσεις πακέτων δεδομένων καθώς και η χρήση κωδίκων διόρθωσης λαθών.

Οι δεύτερες επιθέσεις στοχεύουν στην εξάντληση των ενεργειακών αποθεμάτων των κόμβων την οποία επιτυγχάνουν με τη δρομολόγηση μεγάλων μηνυμάτων, με συνεχή χρήση του υποσυστήματος μετάδοσής, το οποίο, καταναλώνει την περισσότερη ενέργεια από όλα τα υποσυστήματα του κόμβου. Η κύρια άμυνα σε αυτού του είδους την επίθεση είναι η δρομολόγηση μηνυμάτων μόνο μετά από αυθεντικοποίηση του αποστολέα και η φραγή μηνυμάτων με μέγεθος

μεγαλύτερο από το μέγεθος των τυπικών μηνυμάτων της εφαρμογής, που εξυπηρετεί το δίκτυο [31][36][41].

7.4.1.3 Επιθέσεις στα επίπεδα δικτύου και μεταφοράς

Σε αυτό το σημείο να αναφέρουμε ότι επίπεδο δικτύου μπορούν να πραγματοποιηθούν μια σειρά από επιθέσεις οι οποίες σχετίζονται με την εκμετάλλευση αδυναμιών των πρωτοκόλλων δρομολόγησης. Έτσι ένας επιτιθέμενος μπορεί να συμμετέχει στην αλυσίδα δρομολόγησης των μηνυμάτων και να καταστρέφει όσα πακέτα φτάνουν σε αυτόν (black hole attacks), ή όσα μηνύματα λαμβάνει να τα κρατά και να τα εκπέμπει ετεροχρονισμένα (grey hole attacks) ή να τα προωθεί σε λαθεμένες κατευθύνσεις δημιουργώντας ατέρμονες βρόχους (misdirections attacks), προκαλώντας με αυτό τον τρόπο κατανάλωση ενέργειας στους κόμβους που συμμετέχουν στη δρομολόγηση.

Μια άλλη κατηγορία επιθέσεων στο επίπεδο δικτύου είναι η επίθεση τύπου homing. Η επίθεση αυτή βασίζεται στην ανάλυση της κίνησης του δικτύου ώστε να βρεθούν κομβόι οι οποίοι είναι κρίσιμοι για τη λειτουργία του δικτύου. Έπειτα με κάποιου άλλου τύπου επίθεση, προς αυτούς τους κόμβους, γίνεται προσπάθεια ώστε να εξουδετερωθούν.

Η καλύτερη άμυνα ενάντια σε αυτού του είδους τις επιθέσεις στηρίζεται σε πρωτόκολλα δρομολόγησης, τα οποία παρακολουθούν συνεχώς τη λειτουργία του δικτύου, εντοπίζουν μη φυσιολογικές συμπεριφορές, τις απομονώνουν και είναι σε θέση να παρέχουν εναλλακτικά μονοπάτια δρομολόγησης, ώστε να αποφεύγονται οι περιοχές στις οποίες δρουν οι επιτιθέμενοι. Όμως η σημαντικότερη ενέργεια η οποία θωρακίζει το δίκτυο απέναντι σε αυτού του

είδους τις επιθέσεις είναι η συμμετοχή στη δρομολόγηση μόνο εξουσιοδοτημένων κόμβων [31][36][42].

7.4.2 Είδη και τύποι επιθέσεων

Στο κομμάτι αυτό θα γίνει μία αναφορά σχετικά με τα είδη επιθέσεων. Συνήθως κατά την εκτέλεση μιας επίθεσης, οι επιτιθέμενοι διαθέτουν μεγαλύτερη ενέργεια από τους κόμβους του δικτύου. Με το πλεονέκτημα αυτό μπορούν να αναγκάσουν κόμβους του δικτύου να καταναλώσουν όλη τους την ενέργεια και να βγουν εκτός λειτουργίας. Έτσι, είναι αναγκαία η άμεση πρόληψη και γνώση μιας απειλής. Παρακάτω περιγράφουμε τις απειλές που δέχεται ένα δίκτυο. Οι επιθέσεις σε ένα ασύρματο δίκτυο δεν περιορίζονται σε επιθέσεις άρνησης υπηρεσίας αλλά περιλαμβάνουν μια ποικιλία τεχνικών όπως κατάληψη κόμβου, επιθέσεις εναντίον του πρωτόκολλου δρομολόγησης και επιθέσεις στην φυσική ασφάλεια ενός κόμβου.

7.4.2.1 Επιθέσεις άρνησης εξυπηρέτησης

Επίθεση άρνησης εξυπηρέτησης (Denial of Service - DoS) ορίζεται οποιοδήποτε γεγονός μειώνει ή εξαλείφει την ικανότητα ενός δικτύου να εκτελέσει τις αναμενόμενες λειτουργίες. Υπάρχουν πολλές τεχνικές που χρησιμοποιούνται στα συμβατικά δίκτυα υπολογιστών και ανταπεξέρχονται σε κάποιες μορφές άρνησης εξυπηρέτησης. Το πρόβλημα στα δίκτυα αισθητήρων είναι ότι οι περιορισμοί ενέργειας, αποθηκευτικού χώρου και υπολογιστικών πόρων αποτρέπουν την εφαρμογή των συνήθων τεχνικών άμυνας.

Συνήθως μια επίθεση άρνησης εξυπηρέτησης αποτελείται το θύμα (victim), τον υπαίτιο της επίθεσης (attack daemon agent), το πρόγραμμα συντονισμού

επίθεσης (control master program) και τον πραγματικά επιτιθέμενο (real attacker).

Στο φυσικό επίπεδο μια συνήθης επίθεση σε ένα δίκτυο είναι η συμφόρηση (jamming) ενός κόμβου ή μιας ομάδας κόμβων. Η συμφόρηση, σ' αυτή την περίπτωση, είναι η μετάδοση ενός σήματος που παρεμβάλλεται στις συχνότητες που χρησιμοποιούνται από το δίκτυο. Η συμφόρηση σ' ένα δίκτυο μπορεί να πραγματοποιείται συνεχόμενα ή διακοπτόμενα. Μια άλλη μορφή επίθεση άρνησης εξυπηρέτησης στο φυσικό επίπεδο των δικτύων είναι η επίθεση της πλαστογράφησης(tampering). Η πλαστογράφηση μπορεί να οδηγήσει σε εκτεθειμένους κόμβους οι οποίοι μπορούν να εξάγουν ευαίσθητα δεδομένα για να κερδίσουν μη απεριόριστη πρόσβαση σε υψηλότερα επίπεδα επικοινωνίας.

Στο επίπεδο ζεύξης μια πιθανότητα επίθεσης άρνησης εξυπηρέτησης είναι ο επιτιθέμενος να προσπαθήσει να παραβιάσει το πρωτόκολλο επικοινωνίας και να μεταδίδει συνεχώς μηνύματα σε μια προσπάθεια να προκαλέσει συγκρούσεις (collisions). Τέτοιες συγκρούσεις απαιτούν την αναμετάδοση οποιουδήποτε πακέτου επηρεάζεται από αυτές. Ένα αποτέλεσμα των συγκρούσεων είναι η εξάντληση των κόμβων του δικτύου από την ισχύ τους.

Στο επίπεδο δικτύου, οι συνηθέστερες επιθέσεις που μπορούν να δημιουργηθούν είναι η αμέλεια (neglect), η επίθεση αποστολής σε λάθος διεύθυνση (misdirection) και οι μαύρες τρύπες (black holes). Στις επιθέσεις αμέλειας ένας κόμβος αυθαίρετα αμελεί να δρομολογήσει ορισμένα μηνύματα. Ο υπονομευμένος ή κακόβουλος κόμβος μπορεί να συμμετέχει σε χαμηλών επιπέδων πρωτόκολλα και μπορεί να γνωρίζει ότι λαμβάνει δεδομένα από έναν άλλο κόμβο αλλά δεν τα αποστέλλει. Μια πιο ενεργή μορφή επίθεσης, η

αποστολή μηνυμάτων σε λάθος διεύθυνση, προωθεί τα μηνύματα σε λάθος διαδρομές, δημιουργώντας λάθος πληροφορίες δρομολόγησης. Στις επιθέσεις μαύρης τρύπας, οι κόμβοι διαφημίζουν μηδενικού κόστους δρομολόγηση σε κάθε άλλο κόμβο, δημιουργώντας δρομολόγηση μαύρης τρύπας στο δίκτυο. Όσο η διαφήμισή τους διαδίδεται, το δίκτυο δρομολογεί περισσότερη κίνηση προς την κατεύθυνσή τους. Αυτό προκαλεί έντονη διαμάχη πηγών γύρω από τους κακόβουλους κόμβους, καθώς οι γείτονες συναγωνίζονται για περιορισμένο εύρος ζώνης. Οι γείτονες μπορούν να εξαντληθούν δημιουργώντας μια τρύπα ή ένα χώρισμα στο δίκτυο.

Στο επίπεδο μεταφοράς οι επιθέσεις άρνησης εξυπηρέτησης μπορούν να είναι επιθέσεις πλημμύρας (flooding) και αποσυγχρονισμού (desynchronization). Η πλημμύρα είναι τόσο απλή όσο το να στέλνεις πολλές αιτήσεις σύνδεσης σε έναν ευάλωτο κόμβο. Κάθε αίτηση προκαλεί το θύμα να δεσμεύσει πηγές που διατηρεί γι' αυτήν τη σύνδεση και τελικά την εξάντλησή του από άποψη πηγών. Κατά την επίθεση του αποσυγχρονισμού, ο επιτιθέμενος επανειλημμένα πλαστογραφεί τα μηνύματα των σημείων τερματισμού. Αυτά τα μηνύματα έχουν νούμερα ακολουθίας ή σημαίες ελέγχου που αναγκάζουν τα σημεία τερματισμού να αιτηθούν αναμετάδοση των χαμένων κομματιών [32][41][43].

7.4.2.2 Σιβυλλική επίθεση

Η σιβυλλική επίθεση (Sybil attack) ορίζεται ως μια κακόβουλη συσκευή η οποία προσλαμβάνει πολλαπλές ταυτότητες. Οι επιπλέον ταυτότητες που προσλαμβάνει η συσκευή ονομάζονται σιβυλλικοί κόμβοι. Έτσι, ένας κακόβουλος κόμβος συμπεριφέρεται σαν να είναι ένας μεγάλος αριθμός κόμβων, για παράδειγμα μιμούμενος άλλους κόμβους ή παρουσιάζοντας λάθος ταυτότητες. Στην χειρότερη περίπτωση, ο επιτιθέμενος μπορεί να παράγει έναν

αυθαίρετο αριθμό επιπλέον κόμβων, χρησιμοποιώντας μόνο μια φυσική συσκευή [32][44].

7.4.2.3 Επιθέσεις ανάλυσης κίνησης

Τα δίκτυα αισθητήρων συνήθως αποτελούνται από πολλές συσκευές μικρής ισχύος που επικοινωνούν με τους σταθμούς βάσης, συσκευές αυξημένων δυνατοτήτων. Είναι πιθανό λοιπόν, τα δεδομένα να συγκεντρώνονται από τους ξεχωριστούς κόμβους και να δρομολογούνται στον σταθμό βάσης. Συχνά, ένας επιτιθέμενος για να καταστήσει το δίκτυο άχρηστο, μπορεί να απενεργοποιήσει το σταθμό βάσης. Υπάρχουν δύο μορφές επιθέσεων αυτού του τύπου προς το σταθμό βάσης. Μια επίθεση καταγραφής του ρυθμού απλά χρησιμοποιεί την ιδέα ότι οι κόμβοι πλησίον των σταθμών βάσεων τείνουν να προωθούν περισσότερα πακέτα από αυτούς που βρίσκονται μακρύτερα από τους σταθμούς βάσης. Ένας επιτιθέμενος χρειάζεται να παρακολουθεί ποιος κόμβος στέλνει πακέτα και να ακολουθήσει αυτούς τους κόμβους που στέλνουν τα περισσότερα πακέτα. Σε μια επίθεση συσχέτισης χρόνου, ένας επιτιθέμενος απλά παράγει γεγονότα και παρακολουθεί σε ποιόν τα στέλνει ένας οποιοδήποτε κόμβος. Για να δημιουργήσει ένα γεγονός, ο επιτιθέμενος απλά παράγει ένα φυσικό γεγονός που μπορεί να καταγραφεί από τους κόμβους του δικτύου [32][52].

7.4.2.4 Επιθέσεις αναπαραγωγής κόμβου

Η επίθεση αναπαραγωγής κόμβου με έναν επιτιθέμενο που προσπαθεί να προσθέσει έναν κόμβο στο υπάρχον δίκτυο αντιγράφοντας την ταυτότητα ενός υπάρχοντος κόμβου. Ένας κόμβος που παράγεται με αυτόν τον τρόπο μπορεί να διαταράξει την ομαλή λειτουργία του δικτύου: τα πακέτα μπορεί να αλλοιώνονται ή να οδηγούνται σε λάθος διαδρομή. Αυτό μπορεί να οδηγήσει ένα δίκτυο που δεν συνδέεται ομαλά, να παρέχει λάθος δεδομένα. Αν ένας

επιτιθέμενος κερδίσει φυσική πρόσβαση στο δίκτυο, μπορεί να αντιγράψει τα κρυπτογραφικά κλειδιά και μπορεί να εισάγει αναπαραγόμενους κόμβους σε στρατηγικά σημεία του δικτύου. Εισάγοντας νέους κόμβους σε συγκεκριμένα σημεία, ο επιτιθέμενος μπορεί να ελέγχει ένα συγκεκριμένο κομμάτι του δικτύου και να εκτελεί επιθέσεις στο υπόλοιπο υγιές δίκτυο [32][45].

7.4.2.5 Επιθέσεις εναντίον του απορρήτου

Στα δίκτυα αισθητήρων διακινούνται πληροφορίες που προέρχονται από συλλογή στην υπό επιτήρηση περιοχή Αν και οι πληροφορίες αυτές είναι φαινομενικά ακίνδυνες, οι επιτιθέμενοι μπορούν να τις χρησιμοποιήσουν για να αποκομίσουν ευαίσθητα δεδομένα αν ξέρουν πώς να συσχετίσουν τα πολλαπλά μηνύματα που καταφθάνουν στους κόμβους.

Το πρόβλημα απορρήτου επιδεινώνεται επειδή στο δίκτυο διακινείται εύκολα διαθέσιμος ένας μεγάλος όγκος δεδομένων μέσω απομακρυσμένης πρόσβασης. Συνεπώς, οι επιτιθέμενοι δεν χρειάζεται να είναι παρόντες για να διατηρήσουν επαφή. Μπορούν να συγκεντρώνουν δεδομένα με απομακρυσμένη πρόσβαση, η οποία επιτρέπει σε έναν επιτιθέμενο να παρακολουθεί πολλαπλά σημεία του δικτύου ταυτόχρονα. Οι συνηθέστερες επιθέσεις εναντίον του απορρήτου είναι η παρακολούθηση και κρυφάκουσμα, η ανάλυση κίνησης και η παραλλαγή (camouflage) [32][46][47].

7.4.2.6 Φυσικές επιθέσεις

Τα δίκτυα αισθητήρων συχνά λειτουργούν σε εχθρικά περιβάλλοντα όπου, η έλλειψη επιτήρησης των κόμβων καθιστά το δίκτυο ευάλωτο σε φυσικές επιθέσεις. Ως φυσικές επιθέσεις θεωρούνται απειλές που επιφέρουν την φυσική καταστροφή των κόμβων. Σε αντίθεση με τις επιθέσεις που αναφέρθηκαν

παραπάνω, οι φυσικές επιθέσεις καταστρέφουν τον κόμβο μόνιμα και οι απώλειες είναι μη αναστρέψιμες. Επίσης, οι επιτιθέμενοι μπορούν να εξάγουν κρυπτογραφικά μυστικά, να μελετήσουν τη διάταξη των κυκλωμάτων των κόμβων, να τροποποιήσουν τον προγραμματισμό των κόμβων ή να αντικαταστήσουν κόμβους με άλλους κακόβουλους [48].

7.4.2.7 Επιθέσεις καταβόθρας

Κατά την επίθεση καταβόθρας (sinkhole attack) στόχος του επιτιθέμενου είναι να παρασύρει όλη την κίνηση μιας συγκεκριμένης περιοχής του δικτύου μέσω ενός εκτεθειμένου κόμβου, δημιουργώντας μια μεταφορική καταβόθρα με τον επιτιθέμενο στο κέντρο. Επειδή οι κόμβοι δίπλα ή πάνω στη διαδρομή που ακολουθούν τα πακέτα έχουν μεγάλες δυνατότητες να απασχολούνται με δεδομένα εφαρμογών, οι επιθέσεις καταβόθρας μπορούν να ενεργοποιήσουν και άλλες επιθέσεις (για παράδειγμα επιλεκτική προώθηση). Οι επιθέσεις καταβόθρας συνήθως δουλεύουν κάνοντας έναν εκτεθειμένο κόμβο να φαίνεται ελκυστικός στους γειτονικούς κόμβους ως προς τον αλγόριθμο δρομολόγησης. Εξασφαλίζοντας ότι όλη η κίνηση στην περιοχή ενδιαφέροντος ρέει μέσω ενός εκτεθειμένου κόμβου, ένας επιτιθέμενος μπορεί επιλεκτικά να τροποποιήσει ή να απορρίψει πακέτα που προέρχονται από οποιοδήποτε κόμβο του δικτύου [32][49].

7.4.2.8 Σκουληκότρυπες

Σε μια επίθεση σκουληκότρυπας (wormhole) ένας επιτιθέμενος λαμβάνει μηνύματα από ένα σημείο του δικτύου, τα διοχετεύει σε άλλο σημείο του δικτύου και στη συνέχεια τα επαναλαμβάνει στο δίκτυο από αυτό το σημείο. Οι σκουληκότρυπες μπορούν να χρησιμοποιηθούν για να πείσουν δύο απομακρυσμένους κόμβους ότι είναι γείτονες αναμεταδίδοντας πακέτα μεταξύ τους Αν ο επιτιθέμενος εκτελεί αυτήν τη διαδικασία άδολα και αξιόπιστα δεν

δημιουργείται κακό. Στην πραγματικότητα, ο επιτιθέμενος παρέχει χρήσιμη υπηρεσία συνδέοντας το δίκτυο πιο αποτελεσματικά. Ωστόσο, η σκουληκότρυπα θέτει τον επιτιθέμενο σε πιο ισχυρή θέση από τους άλλους κόμβους του δικτύου και ο επιτιθέμενος μπορεί να το εκμεταλλευτεί με πολλούς τρόπους. Οι σκουληκότρυπες μπορούν να χρησιμοποιηθούν σε συνδυασμό με την επιλεκτική προώθηση, το κρυφάκουσμα, την επίθεση καταβόθρας και τη σιβυλλική επίθεση [32][50].

7.4.2.9 Επιλεκτική προώθηση

Τα δίκτυα πολλαπλών αλμάτων συνήθως στηρίζονται στην υπόθεση ότι οι συμμετέχοντες κόμβοι θα προωθήσουν με συνέπεια τα λαμβανόμενα μηνύματα. Σε μια επίθεση επιλεκτικής προώθησης, κακόβουλοι κόμβοι μπορεί να αρνηθούν να προωθήσουν ορισμένα μηνύματα και απλά να τα αφήσουν, εξασφαλίζοντας ότι δεν θα διαδοθούν παραπέρα. Μια απλή μορφή της επίθεσης είναι όταν ένας κακόβουλος κόμβος συμπεριφέρεται σαν μαύρη τρύπα (black hole) και αρνείται να προωθήσει κάθε πακέτο που δέχεται. Όμως, ένας τέτοιος επιτιθέμενος, κινδυνεύει να αποκλειστεί από τους γειτονικούς κόμβους και να επιλεγεί κάποια εναλλακτική διαδρομή. Μια πιο επιδέξια μορφή επίθεσης είναι όταν ο επιτιθέμενος προωθεί επιλεκτικά πακέτα [32][49].

8 Νομικά θέματα ασφάλειας

8.1 Εισαγωγή στα νομικά θέματα ασφάλειας

Η νομοθεσία που αφορά στα θέματα ασφάλειας δημιουργεί αξία για τους πολίτες η οποία απορρέει από την εφαρμογή της. Ειδικότερα, ως προς την εφαρμοσιμότητα οι νέες τεχνολογίες πληροφορικής βάζουν σε δοκιμασία μεγάλα τμήματα της παραδοσιακής νομοθεσίας. Η σχετική νομοθεσία στα προηγμένα κράτη διευρύνεται έτσι ώστε να συμπεριλαμβάνει νέου τύπου αδικήματα, όμως για την αποτελεσματική εφαρμογή της, είναι αναγκαία η κατάλληλη εκπαίδευση δικαστικών, αστυνομικών, χρηστών καθώς και η θέσπιση ελεγκτικών φορέων και εποπτικών αρχών, που στόχο θα έχουν την αποτελεσματική επίβλεψη της νομοθετικής εφαρμογής. Είναι σημαντικό να αναφερθεί πως καταλυτικά θα συνδράμουν στην εφαρμογή των παραπάνω η εισαγωγή τεχνικών και οργανωτικών μέτρων ασφάλειας και μέτρα για την επιτάχυνση της διεθνούς συνεργασίας [53].

Οποιαδήποτε γενική νομοθεσία πρέπει να συνοδεύεται από νομοθετήματα τομεακού χαρακτήρα. Η ραγδαία εξάπλωση των νέων τεχνολογιών σε όλους τους τομείς της κοινωνικής και οικονομικής ζωής, δημιουργεί ειδικές χωριστές ανάγκες για την προστασία των προσωπικών δεδομένων ανάλογα με τις ιδιαιτερότητες του κάθε τομέα. Από το 1947 μέχρι σήμερα το συμβούλιο της Ευρώπης έχει υιοθετήσει μια σειρά από συστάσεις που καλύπτον τις ιατρικές βάσεις δεδομένων, την κοινωνική ασφάλιση, το μάρκετινγκ, τα δεδομένα για τους εργαζόμενους, την εμπορευματοποίηση των δεδομένων του δημόσιου τομέα τα δεδομένα της αστυνομίας, τα δεδομένα της ερευνάς και τις στατιστικής, της τηλεπικοινωνίες. Πρόταση τομεακής οδηγίας για τα ψηφιακά τηλεπικοινωνιακά δίκτυα έχει ήδη υποβληθεί από την ευρωπαϊκή επιτροπή [53].

Παράλληλα, γενικού χαρακτήρα είναι η πρόταση οδηγίας της ευρωπαϊκής ένωσης προς τα κράτη μελή να ενθαρρύνουν τις επαγγελματικές οργανώσεις, ώστε να υιοθετήσουν τομεακούς κώδικες δεοντολογίας, ενώ αφήνει ανοιχτό το ενδεχόμενο νέων τομεακών νομοθετικών προτάσεων [53]. Τα νομοθετήματα και οι κώδικες δεοντολογίας τομεακού χαρακτήρα, έχουν ένα κοινό χαρακτηριστικό, ότι στο βαθμό που εκπονούνται σε στενή συνεργασία με (ή από τους ίδιους τους) ενδιαφερομένους φορείς, συμβάλλουν αποφασιστικά στην ευαισθητοποίηση των χρηστών των προσωπικών δεδομένων κάθε τομέα [53]. Υπάρχει όμως και μία βασική διάφορα, ότι τα πρώτα έχουν νομική ισχύ δημόσιου δικαίου, κάτι το οποίο αποκτά ιδιαίτερη σημασία εφόσον προβλέπονται αυστηρές κυρώσεις, ενώ οι δεύτεροι αφήνονται ανάλογα στην "νομιμοφροσύνη" των μελών των επαγγελματικών οργανώσεων, δεν είναι βέβαιο ότι δεσμεύουν και τα μη μελή του συγκεκριμένου τομέα και στην αποφασιστικότητα εθελοντικών διαχειριστικών οργάνων όσον αφόρα την επιβολή κυρώσεων. Σε ορισμένα κράτη μελή της Ευρωπαϊκής Ένωσης όπως η Βρετάνια, η Ιρλανδία, και η Ολλανδία, υπάρχει μακρά και σχετικά επιτυχής παράδοση τέτοιων μορφών αυτοδιαχείρισης σε αντίθεση με την ισχύουσα κατάσταση στις χώρες της νότιας Ευρώπης και ειδικά στην Ελλάδα, όπου η αποτελεσματικότητα τους είναι εξαιρετικά αμφίβολη. Χρειάζεται νομοθετική παρέμβαση με τη μεγαλύτερη συμμέτοχη των ενδιαφερόμενων φορέων, τόσο για την πληρότητα του νομοθετήματος όσο και για την ενημέρωση των χρηστών των προσωπικών δεδομένων [53]. Μεγάλης σημασίας είναι ο ρόλος της υπηρεσίας έλεγχου που προβλέπεται από όλες τις ευρωπαϊκές νομοθεσίες και από την πρόταση Οδηγίας της Ευρωπαϊκής Ένωσης. Η υπηρεσία αυτή ελέγχει κατά κανόνα τόσο το ιδιωτικό όσο και το δημόσιο τομέα, επομένως πρέπει να είναι ουσιαστικά ανεξάρτητη από την Κυβέρνηση. Σε περίπτωση αμφισβητήσεων, τον τελευταίο ρολό έχει η Δικαστική εξουσία και όχι ο υπουργός δικαιοσύνης ή το υπουργικό συμβούλιου. Η υπηρεσία έλεγχου πρέπει να έχει εξουσίες τόσο κατασταλτικές (άσκηση έλεγχου, απαγόρευση

παράνομης επεξεργασίας δεδομένων, προσφυγή στην δικαιοσύνη), όσο και προληπτικές (έκδοση ερμηνευτικών εγκυκλίων, οργάνωση εκπαιδευτικών σεμιναρίων, θεσμοθετημένο διάλογο με τις ομάδες των χρηστών, συμβολή στην σύνταξη κωδικών δεοντολογίας). Φυσικά απαραίτητη προϋπόθεση για την επιτυχή εξάσκηση των καθηκόντων της αποτελεί η ύπαρξη επαρκών μέσων και πόρων, ανθρώπινων και υλικών [53].

Πρέπει τέλος στις αρμοδιότητες (αλλά και στις δυνατότητες) της υπηρεσίας έλεγχου να περιλαμβάνεται και η συνεργασία με τις αντίστοιχες υπηρεσίες άλλων κρατών. Αυτό γίνεται ολοένα περισσότερο αναγκαίο όσο τα τηλεπικοινωνιακά δίκτυα και η πρόοδος της τεχνολογίας διευκολύνουν τη μεταφορά και την επεξεργασία προσωπικών δεδομένων σε οποιαδήποτε χωρά της υδρόγειου [53]. Οι υπηρεσίες έλεγχου στις οποίες και αποδίδονται σημαντικές εξουσίες αποτελούν “προπύργιο” του τελικού κριτής της σωστής εφαρμογής του νομού και αρμόδιος για την επιβολή κυρώσεων είναι ο δικαστής. Βεβαία οι υπηρεσίες έλεγχου διαθέτουν στο στελεχιακό τους δυναμικό τόσο νομομαθείς όσο και ειδικούς της πληροφορικής, που εξειδικεύονται στην εφαρμογή του νομού με την πείρα που αποκτούν, οι δικαστές σπάνια διαθέτουν ειδικές γνώσεις είτε του δικαίου της πληροφορικής είτε των εφαρμογών της πληροφορικής σε όλες της πτυχές της κοινωνικής και οικονομικής ζωής. Για τη διαπίστωση νομιμότητας της συγκεκριμένης επεξεργασίας δεδομένων ο νόμος δεν περιέχει πάντοτε ρητές προϋποθέσεις, αλλά παραπέμπει στην συγκριτική εκτίμηση των συμφερόντων τόσο των προσώπων που αφόρα η επεξεργασία, όσο και των χρηστών που προβαίνουν στην επεξεργασία. Είναι βέβαιο ότι από την γενική φύση τους και τουλάχιστον μέχρι να υπάρχουν πολυάριθμα τομεακά νομοθετήματα για την προστασία των προσωπικών δεδομένων θα αφήσουν μεγάλο πεδίο ερμηνείας και εξειδίκευσης στην νομολογία. Αυτό δεν αφόρα βεβαίως μονό στην προστασία των προσωπικών δεδομένων, αλλά στο σύνολο του δικαίου που επηρεάζεται ή δημιουργείται από την πληροφορική. Η συνεχής

επιμόρφωση των δικαστών θα ήταν επομένως εξαιρετικά χρήσιμη [53]. Με την εξάπλωση της χρήσης των νέων τεχνολογιών της πληροφορίας σε παγκόσμιο επίπεδο και των δυνατοτήτων κατάχρησης προσωπικών δεδομένων, ιδιαίτερα σε χώρες οπού η νομοθεσία είναι από ανεπαρκής έως ανύπαρκτη ή ο νομός παραβιάζεται από ισχυρά συμφέροντα(είτε του δημόσιου είτε του ιδιωτικού τομέα), το πλέον αποτελεσματικό όπλο για την προστασία των προσωπικών δεδομένων είναι η συμμέτοχη της κοινωνίας. Ο πολίτης πρέπει να μάθει με σαφήνεια και χωρίς υπερβολές, ποια είναι τα οφέλη καθώς και ποιά είναι τα σχετικά δικαιώματα του και ποιοι οι κίνδυνοι από την επεξεργασία των πρωσικών του δεδομένων [53]. Παράλληλα οι χρηστές, πρέπει να ενημερωθούν για της υποχρεώσεις που επιβάλλει η νομοθεσία. το ζητούμενο είναι να βρεθούμε στην πορεία που σήμερα ακόλουθοι, τουλάχιστον στις ανεπτυγμένες χώρες, η προστασία του περιβάλλοντος που περιλαμβάνεται ήδη στο σχεδιασμό της παράγωγης και στην εκστρατεία μάρκετινγκ πολλών προϊόντων. Να φτάσουμε δηλαδή στο σημείο οπού σε συνθήκες ελευθέρου ανταγωνισμού ο πολίτης θα προτίμα εκείνες της υπηρεσίες (τηλεπικοινωνιών, πιστωτικών καρτών, πωλήσεων από απόσταση, ιατρικής περίθαλψης κ.λπ.)που θα σέβονται και θα προστατεύουν τα προσωπικά δεδομένα. Από της ευρωπαϊκές χώρες ο υψηλότερος βαθμός ενδιαφέροντος των πολιτών, παρατηρείται στην Γερμάνια και αυτό συμβάλει στην θέσπιση αυστηρής, γενικής και τομεακής, νομοθεσίας και σε νομολογία όπως η περίφημη απόφαση του Συνταγματικού Δικαστηρίου της Καρλσρούης που αναγνωρίζει στον πολίτη δικαίωμα "πληροφοριακής αυτοδιάθεσης" Είναι ενδιαφέρουσα η διαφορά ανάμεσα στο πνεύμα της γερμανικής νομοθεσίας που στηρίζει τη νομιμότητα της επεξεργασίας των προσωπικών δεδομένων κυρίως στη συναίνεση του πολίτη και της γαλλικής νομοθεσίας, οπού η νομιμότητα στηρίζεται στην έγκριση της υπηρεσίας έλεγχου. Για να είναι σε θέση να εκτιμήσει τις περιστάσεις και να συναινέσει, ο πολίτης θα πρέπει να είναι ενημερωμένος. Και αυτό είναι φυσικά υποχρέωση του κράτους [53]. Η εξέλιξη των τεχνολογιών πληροφορίας και τηλεπικοινωνιών, καθιστά ολοένα και δυσκολότερο τον έλεγχο της επεξεργασίας

των προσωπικών δεδομένων με "παραδοσιακούς τρόπους" καθώς η ποσότητα των δεδομένων που γίνονται αντικείμενο επεξεργασίας, ο συνολικός αριθμός των χρηστών τέτοιων δεδομένων και η ταχύτητα μεταφοράς των δεδομένων μέσω τηλεπικοινωνιών δικτύων αυξάνονται με ραγδαίους ρυθμούς. Η λύση του προβλήματος αυτού βρίσκεται σε μεγάλο βαθμό στην ίδια την τεχνολογία. Είναι τεχνικά δυνατό στο σχεδιασμό του λογισμικού που χρησιμοποιείτε για την επεξεργασία των προσωπικών δεδομένων, πχ για σκοπούς εργασιακούς, ιατρικής περίθαλψης, κοινωνικών ασφαλίσεων, εμπορικών συναλλαγών, στατιστικής, έρευνας αγοράς, κλπ, να περιλαμβάνονται κανόνες για την αποτελεσματική προστασία των προσωπικών δεδομένων, που θα επιτρέπουν δηλαδή επεξεργασία προσωπικών δεδομένων στο βαθμό που είναι απόλυτος αναγκαίος για τους συγκεκριμένους σκοπούς, που θα σβήσουν η παγώνουν τα δεδομένα όταν δεν απαιτούνται πλέον για τους σκοπούς αυτούς, που θα επιτρέπουν την πρόσβαση μονό σε εξουσιοδοτημένα άτομα, που θα διευκολύνουν την παρακολούθηση της πορείας των δεδομένων προς τους διαφόρους αποδεκτές-χρηστές [53]. Είναι δυνατό να κατασκευαστεί ειδικό λογισμικό για τις ανάγκες των υπηρεσιών έλεγχου, έτσι ώστε να διευκολύνεται και να επιτυγχάνεται ο έλεγχος των δηλώσεων επεξεργασίας που υποβάλλουν οι χρηστές και τις όποιες επιβάλλουν οι περισσότερες ευρωπαϊκές νομοθεσίες και η πρόταση οδηγίας της Ευρωπαϊκής Ένωσης. Είναι προφανές ότι η βιομηχανία λογισμικού θα προχωρήσει προς αυτή την κατεύθυνση όταν υπάρξει σχετική ζήτηση από την αγορά. Και η ζήτηση θα υπάρξει όταν, όπως αναφερθήκαμε η προστασία των προσωπικών δεδομένων θα είναι εμπρός του κοινωνικού προβληματισμού και μέρος τις εμπορικής πολίτικης των επιχειρήσεων. Σε ένα άλλο κλάδο του Δικαίου, εκείνο της προστασίας της πνευματικής ιδιοκτησίας, οπού τα οικονομικά συμφέροντα για την προστασία των ηλεκτρονικών πνευματικών έργων (βάσεων δεδομένων, υπηρεσιών ψυχαγωγίας,MULTIMEDIA) είναι ήδη ισχυρά, έχουν γίνει σημαντικά βήματα από την ίδια την τεχνολογία. Χάρη στο υποπρόγραμμα CIED που συγχρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση στα πλαίσια του

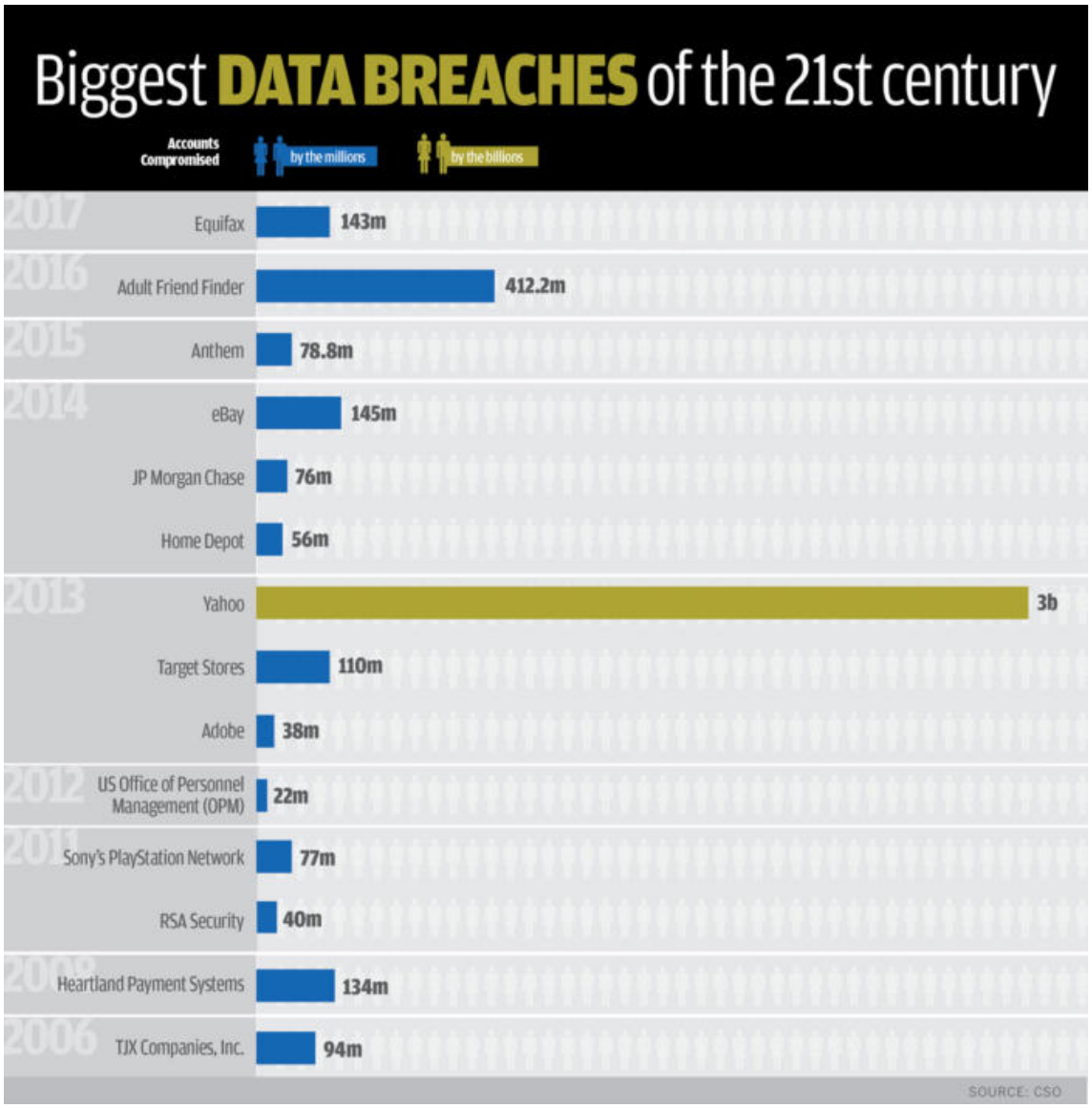
προγράμματος ESPRIT, οι παραγωγοί τέτοιων έργων έχουν σήμερα την τεχνολογική δυνατότητα να ελέγχουν πλήρως τη χρήση των έργων τους από κάθε κατηγορία χρηστών και να εισπράττουν αυτομάτως το αντίτιμο των δικαιωμάτων τους, ανάλογα με την συγκεκριμένη χρήση και κατηγορία χρήστη [53]. Για την προστασία των προσωπικών δεδομένων κάποιες μελέτες τεχνολογικού χαρακτήρα έχουν προγραμματίσει στα πλαίσια του προγράμματος της Ε.Ε για την ασφάλεια των πληροφοριών, που έχει ως στόχο την επίτευξη του τρίπτυχου" εμπιστευτικότητα, πληρότητα, διαθεσιμότητα" για τις ηλεκτρονικές πληροφορίες. Μέτρα για την ασφάλεια των προσωπικών δεδομένων απαιτούνται βεβαία από κάθε ευρωπαϊκή νομοθεσία και από την πρόταση οδηγίας της Ε.Ε. Αλλά τα μέτρα αυτά είναι ένα μικρό μέρος της πιθανής συμβολής της τεχνολογίας στην αποτελεσματική προστασία των προσωπικών δεδομένων [53]. Αν οι νέες τεχνολογίες πληροφοριών αφορούν ένα διαρκώς αυξανόμενο αριθμό ανθρώπινων δραστηριοτήτων και αν η προστασία των προσωπικών δεδομένων είναι ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, τότε οι ανθρωπινές δραστηριότητες που περιλαμβάνουν επεξεργασία δεδομένων η τουλάχιστον ορισμένες από αυτές που θα θεωρηθούν εν δύναμη περισσότερο επιβλαβείς θα πρέπει να συνοδεύονται από έκθεση επιπτώσεων της συγκεκριμένης επεξεργασίας για τα προσωπικά δεδομένα. Αυτό ήδη συμβαίνει σε αντίστοιχες περιπτώσεις για την την προστασία του περιβάλλοντος. Συμφώνα με το άρθρο 130 ρ παράγραφος 2 της Ενιαίας πράξης, όπως έχει ενσωματωθεί στην Συνθήκη για την Ευρωπαϊκή Ένωση, οι ανάγκες στο τομέα της προστασίας του περιβάλλοντος πρέπει να λαμβάνονται υπόψη στον καθορισμό και την εφαρμογή των άλλων πολιτικών της Κοινότητας 53. Κάτι ανάλογο θα χρειαστεί και για τα προσωπικά δεδομένα και θα συμβάλει θετικά στο έργο των υπηρεσιών έλεγχου, στην άσκηση των δικαιωμάτων τους από τους ιδίους πολίτες και στη συνειδητοποίηση των χρηστών [53]. Όλα όσα αναφέρθηκαν στις προηγούμενες παραγράφους, δηλαδή η θέσπιση τομεακών νομοθετημάτων, η κατάλληλη υποστήριξη των υπηρεσιών έλεγχου, η επιμόρφωση των δικαστικών, η συνειδητοποίηση των

πολιτών, η παράγωγη κατάλληλου λογισμικού, η έκθεση για τις επιπτώσεις της επεξεργασίας προσωπικών δεδομένων, θα έχουν μικρή αποτελεσματικότητα εάν δεν περιοριστεί η ανεξέλεγκτη επεξεργασία προσωπικών δεδομένων σε κάποιες τρίτες χώρες. Τεχνικά αυτό είναι εξεταστικά εύκολο, ενώ ο πλήρης προληπτικός έλεγχος της εξαγωγής δεδομένων είναι αδύνατος. Δειγματοληπτικός έλεγχος ή κυρώσεις για παράνομη εξαγωγή που αποκαλύπτεται εκ των υστέρων έχουν βεβαία και κάποια προληπτική επίδραση, αλλά πιθανότητα αφορούν μονό την κορυφή του παγόβουνου [53]. Η Ευρώπη κυρίως η διευρυμένη Ευρωπαϊκή Ένωση με εξαίρεση την Ελλάδα και την Ιταλία προηγείται σημαντικά, σε ότι αφόρα την νομοθεσία προστασίας των προσωπικών δεδομένων, όλων ανεξαιρέτως των τρίτων κρατών, συμπεριλαμβανομένων των κύριων ανταγωνιστών της στο τομέα των νέων τεχνολογιών πληροφόρησης, των ΗΠΑ, της Ιαπωνίας και των ταχέως αναπτυσσόμενων κρατών της Άπω Ανατολής. Αν η κατάσταση αυτή παραμείνει και μεχρί να σημειωθούν οι εξελίξεις που πιθανολογούνται στην παράγραφο 4,τοτε θα κινδυνεύσουν μόνο όχι η ιδιωτική ζωή και τα δικαιώματα των Ευρωπαίων πολιτών αλλά και η ανταγωνιστικότητα των Ευρωπαϊκών εταιριών που επεξεργάζονται προσωπικά δεδομένα και που αφενός υποχρεούνται να λάβουν μέτρα προστασίας που έχουν οικονομικό κόστος και αφετέρου δεν έχουν το δικαίωμα να κάνουν χρήση προσωπικών δεδομένων με την ευχέρεια των ανταγωνιστών τους στις τρίτες χώρες. Θα πρέπει λοιπόν οι διατάξεις των άρθρων 26 και 27 της πρότασης Οδηγίας της Ε.Ε να τηρηθούν με αυστηρότητα, έτσι ώστε να θαμπισθεί επαρκής σχετική νομοθεσία και στης χώρες αυτές. Ήδη παρατηρούνται θετικές εξελίξεις σε ορισμένες Τρεις χώρες, που είναι αποτέλεσμα και της πρότασης οδηγίας [53]. Ο πολίτης θα πρέπει να έχει ,όταν αυτό είναι δυνατό, δικαίωμα επιλογής ανάμεσα σε λύσεις που περιλαμβάνουν και σε λύσεις που δε περιλαμβάνουν επεξεργασία προσωπικών δεδομένων (π.χ. ανάμεσα σε πληρωμή με πιστωτική κάρτα και τις μετρητοίς). Από την σκοπιά των χρηστών θα πρέπει να αποφεύγεται η επεξεργασία προσωπικών δεδομένων χωρίς σοβαρό λόγο (και φυσικά να ακολουθούνται οι

επιταγές του νομού, εφόσον γίνεται τέτοια επεξεργασία).Οι δυνατότητες των τεχνολογιών δεν αποτελούν επαρκή λόγο για την επεξεργασία προσωπικών δεδομένων, αλλά εργαλείο που θα πρέπει να χρησιμοποιείτε όταν τέτοια επεξεργασία είναι απαραίτητη. Στις περισσότερες χώρες του κόσμου και δυστυχώς στην χωρά μας, η προστασία των προσωπικών δεδομένων δεν έχει βρεθεί, στο επίκεντρο της επικαιρότητας και του δημόσιου ενδιαφέροντος παρά μόνο τελευταία με το περιβόητο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) που θα δούμε αναλυτικότερα παρακάτω.

8.2 Παραδείγματα περιπτώσεων διαρροής προσωπικών δεδομένων

Υπάρχουν πολλές περιπτώσεις όπου προσωπικά δεδομένα χρηστών διέρρευσαν λόγω κακόβουλων ενεργειών που εκμεταλλευτήκαν συστεμικές αδυναμίες ή τον λεγόμενο αδύναμο κρίκο στα πληροφοριακά συστήματα που δεν είναι άλλος από τον ανθρώπινο παράγοντα. Ο λόγος που παραθέτουμε μερικές από τις μεγαλύτερες των τελευταίων ετών δεν είναι άλλος από το γεγονός ότι τα πληροφοριακά συστήματα, οι βάσεις δεδομένων και τα πρότυπα επικοινωνίας είναι ίδια, παραπλήσια ή παρόμοια και αυτά των ΑΔΑ. Καθώς λοιπόν δεν είναι εξάλλου λίγες οι περιπτώσεις σκανδάλων που σχετίζονται με προσωπικά δεδομένα (ως προσωπικά δεδομένα λογίζεται κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο) όπως της εμπορευματοποίησης προσωπικών δεδομένων 87 εκατομμυρίων χρηστών της δημοφιλούς πλατφόρμας κοινωνικής δικτύωσης Facebook, κρίνεται σκόπιμο για λόγους στατιστικής και ανάδειξης του κινδύνου που σχετίζεται με την διαρροή προσωπικών δεδομένων η παράθεσή μερικών από των μεγαλύτερων περιπτώσεων διαρροής τους.



ΣΧΗΜΑ 15 – Οι μεγαλύτερες περιπτώσεις κυβερνο-επιθέσεων μέχρι το 2017

Ακολουθεί μια ανάλυση των δέκα μεγαλύτερων διαρροών δεδομένων σύμφωνα με τον παραπάνω πίνακα.

1. Yahoo

Ημερομηνία: 2013 - 14

Επίπτωση: 3 δις λογαριασμοί χρηστών

Λεπτομέρειες: Τον Σεπτέμβριο του 2016, η άλλοτε κυρίαρχη μηχανή αναζήτησης, ενώ διαπραγματευόταν με την Verizon την πώληση του πλειοψηφικού πακέτου μετοχών της, ανακοίνωσε πως είχε πέσει θύμα μιας από τις μεγαλύτερες κυβερνοεπιθέσεις της ιστορίας το 2014, πιθανότατα από τον φορέα προσκείμενο σε κρατικά συμφέροντα όπως φημολογείται έντονα. Πραγματικά ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, ημερομηνίες γέννησης και αριθμοί τηλεφώνων από 500 εκατομμυρίων χρήστες εκλάπησαν. Η εταιρεία δήλωσε ότι η "συντριπτική πλειοψηφία" κωδικών, εκτέθηκαν στην κυβερνοεπίθεση μέσω χρήσης του ισχυρού αλγόριθμο bcrypt. Πρόκειται για μια κατάσταση της οποίας η Yahoo ήταν ενήμερη από το 2013 όταν και εκτυλίχτηκε αρχικά η κυβερνοεπίθεση, αλλά επέλεξε να την υποβιβάσει. Έτσι, τον Οκτώβριο του 2017, η Yahoo αναθεώρησε το μέγεθος της κυβερνοεπίθεσης και δημοσίευσε στοιχεία τα οποία παρουσιάζουν 3 δις λογαριασμούς χρηστών ως θύματα κακόβουλων ενεργειών hacher. Μάλιστα αυτή περιπέτεια κόστισε στην εταιρία 350 εκατομμύρια δολλάρια, ρίχνοντας την τιμή πώλησης στη Verizon στα 4.48 δις δολλάρια.

2. Adult Friend Finder (AFF)

Ημερομηνία: Οκτώβριος 2016

Επίπτωση: Περισσότεροι από 412.2 εκατομμύρια λογαριασμοί χρηστών

Λεπτομέρειες: Το δίκτυο επιχειρήσεων «The FriendFinder Network» το οποίο περιέχει ιστοσελίδες γνωριμιών επέσε θύμα κακόβουλων ενεργειών hacker οι

οποίοι συνέλεξαν πληροφοριες από 6 βάσεις δεομένων που είχαν στοιχεία σε βάθος 20ετίας, όπως ονομάτα, e-mail, προσωπικές πληροφορίες και κωδικοί. Η πλειονότητα των κωδικών προστατεύονταν από τον SHA1-1 hasing αλγόριθμο, ο οποίος και μπορεί να παραβιαστεί σχετικά εύκολα. Αργότερα η Diana Ballou αντιπρόεδρος του AFF ανέφερε πως η εταιρία αντιλήφθηκε μια αδυναμία που είχε σχέση με την εισαγωγή κώδικα σε σημεία επικοινωνίας με το δίκτυο μέσω φορμών. Ο όμιλος AFF δέχτηκε ένα ισχυρό πλήγμα στην αξιοπιστία του που μεταφράστηκε σε μεγάλη οικονομική ζημιά.

3. eBay

Ημερομηνία: Μάιος 2014
Επίπτωση: 145εκατομμύρια λογαριασμοί χρηστών
Λεπτομέρειες: Η εταιρία πλειστηριασμών και αγορών internet ανακοίνωσε μια κυβερνοεπίθεση το Μάιο του 2014 στην οποία οι hacker έλαβαν γνώση των ονομάτων, διευθύνσεων, ημερομηνιών γέννησης και κωδικών όλων των μελών της ιστοσελίδας οι οποίοι επί των ημερών υπολογίζονταν περί τις 145 εκατομμύρια χρήστες. Οι hacker μπόρεσαν να μπουν στο δίκτυο της εταιρίας μέσω των κωδικών ασφαλείας 3 εταιρικών υπαλλήλων και είχαν ελεύθερη πρόσβαση για 229 ημέρες έως ότου εντοπίστηκαν. Ο CEO του eBay, John Donahue επιβεβαίωσε πως το γεγονός μείωσε την επισκεψιμότητα στην ιστοσελίδα παρότι σύμφωνα με το eBay οι hacker δεν έλαβαν γνώση των προσωπικών τραπεζικών στοιχείων των χρηστών.

4. Equifax

Ημερομηνία: Ιούλιος 2017
Επίπτωση: Προσωπικά στοιχεία όπως αριθμοί ΙΚΑ, ημερομηνίες γέννησης, διευθύνσεις ακόμα και αριθμοί διπλωμάτων από 143 εκατομμύρια καταναλωτές έπεσαν στα χέρια hacker.

Λεπτομέρειες: Το Equifax, μια από τις μεγαλύτερες εταιρίες πιστοληπτικής ικανότητας καταναλωτών στην Αμερική, επιβεβαίωσε πως το Σεπτέμβρη του 2017 μια αστοχία στο λογισμικό της ιστοσελίδας του αποτέλεσε το δούρειο ίππο για κλαπούν τα προσωπικά στοιχεία 147.9 εκατομμυρίων καταναλωτών.

5. Heartland Payment Systems

Ημερομηνία: Μάρτιος 2008
Επίπτωση: 134 εκατομμύρια πιστωτικές κάρτες χρηστών παρακολουθούνταν μέσω spyware που παρείσφρησε στα συστήματα της εταιρίας από SQL injection ενέργειες.
Λεπτομέρειες: Τη περίοδο της κυβερνοεπιθέσεις, η Heartland επεξεργαζόταν περισσότερες από 100 εκατομμύρια κινήσεις καρτών. Το γεγονός ότι είχε πέσει θύμα hacker έγινε αντιληπτό μόλις τον Ιανουάριο του 2009 όταν η Visa και η MasterCard ενημέρωσαν τη Heartland περί ύποπτων συναλλαγών που πραγματοποιούνταν μέσω του δικτύου λογαριασμών της.

Εξαιτίας αυτού η Heartland κρίθηκε εκτός συμμόρφωσης με το Data Security Standard (PCI DSS) του κλάδου Πληρωμών Καρτών και της απαγορεύτηκε να επεξεργάζεται πληρωμές των μεγαλύτερων προμηθευτών καρτών μέχρι και το Μάιο του 2009. Επιπρόσθετα η εταιρία κλήθηκε να πληρώσει περισσότερα από 145 εκατομμύρια δολάρια σε αποζημιώσεις. Στο τέλος της χρονιάς οι διωκτικές αρχές των ΗΠΑ κατάφεραν να εντοπίσουν 3 άτομα που ευθύνονταν για την υπόθεση τα οποία και χρησιμοποίησαν τη μέθοδο του SQL injection για να παρεισφρήσουν στο δίκτυο της εταιρίας.

6. Target Stores

Ημερομηνία: Δεκέμβριος 2013
Επίπτωση: Εκλάπησαν στοιχεία χρεωστικών/πιστωτικων καρτών καθώς και προσωπικά στοιχεία των κατόχων από περισσότερα από 110 εκατομμύρια χρήστες.

Λεπτομέρειες: η κυβερνοεπίθεση έγινε προγενέστερα των Αμερικανικών Ευχαριστιών αλλά έγινε αντιληπτή μετά από αρκετές εβδομάδες. Η αρχική εκτίμηση της εταιρίας ήταν πως περί τα 40 εκατομμύρια στοιχεία καρτών εκλάπησαν μέσω λογισμικού που χρησιμοποίησαν οι hacker. Τον Ιανουάριο του 2014, η εταιρία εξέδωσε νέα ανακοίνωσε στην οποία πλέον μιλούσε για 36 εκατομμύρια χρήστες των οποίων τα στοιχεία εκλάπησαν, ενώ η τελική ανάλυση που διεξήγαγε η εταιρία για να καθορίσει το εύρος της ζημιάς έδειξε περί τα 110 εκατομμύρια χρήστες. Τέλος τα γεγονότα αυτά οδήγησαν τους τότε CIO και CEO να παραιτηθούν, ενώ παράλληλα το κόστος της κυβερνοεπίθεσης ανήλθε σε 162 εκατομμύρια δολάρια.

7. **TJX Companies**, **Inc**.

Ημερομηνία: Δεκέμβριος 2006

Επίπτωση: Τα στοιχεία από 94 εκατομμύρια πιστωτικές κάρτες χρηστών εκλάπησαν.

Λεπτομέρειες: Υπάρχουν δυο διαφορετικές εκδοχές για το πώς επετεύχθη αυτή η κυβερνοεπίθεση. Η μια εκδοχή αναφέρει πως μια ομάδα hacker εκμεταλλεύτηκε το αδύναμο encryption system και μπόρεσε να πάρει στοιχεία πιστωτικών καρτών κατά τη διάρκεια μιας wireless συναλλαγής μεταξύ 2 Marshall's καταστημάτων στο Μαϊάμι των ΗΠΑ. Η άλλη αναφέρει πως η κυβερνοεπίθεση έγινε μέσω του δικτύου της TJX κατά τη διάρκεια μια ενέργειας σε καταστήματα της TJX όπου δινόταν η δυνατότητα να κάνει κάποιος ηλεκτρονική αίτηση εργασίας στην εταιρία. Αργότερα συνελήφθη ο Albert Gonzalez, ένας από τους πλέον αναγνωρίσιμους hacker παγκοσμίως, ο οποίος καταδικάσθηκε σε εικοσαετή κάθειρξη. Μάλιστα όπως διέρρευσε αργότερα ο ίδιος είχε εργαστεί ως πληροφοριοδότης των ΗΠΑ με 36.000 δολάρια μισθό. Σύμφωνα με την κρατική ενημέρωση η κυβερνοεπίθεση προκάλεσε ζημίες 200 εκατομμυρίων δολαρίων.

8. **Uber**

Ημερομηνία: Τέλη του 2016

Επίπτωση: Εκλάπησαν τα προσωπικά δεδομένα 57 εκατομμυρίων χρηστών του Uber καθώς και 600.000 οδηγών.

Λεπτομέρειες: Το μέγεθος της κυβερνοεπίθεσης του Uber από μόνο του είναι αρκετό για να μπει στη λίστα μας με τις μεγαλύτερες περίπτωσης κλοπής δεδομένων των τελευταίων ετών. Παραταύτα, αναφορά αξίζει και ο τρόπος που χειρίστηκε η Uber την κυβερνοεπίθεση αυτή καθώς αποτελεί παράδειγμα προς αποφυγή. Συγκεκριμένα η εταιρία έμαθε στα τέλη του 2016 πως δυο hacker έλαβαν γνώση των προσωπικών δεδομένων 57 εκατομμυρίων χρηστών, πλην των στοιχείων τραπέζης τους, καθώς και 600.000 οδηγών σπάζοντας το κωδικό του χρήστη που διατηρούσε η Uber στο GitHub. Η Uber αποφάσισε να διαχειριστεί το θέμα με τον πλέον λάθος τρόπο καθώς δεν ενημέρωσε το κοινό για το συμβάν, συμφώνησε με τους hacker την καταστροφή των δεδομένων έναντι 100.000 δολαρίων – γεγονός αμφίβολο και ενημέρωσαν το κοινό πως η εταιρία έπεσε θύμα “bug bounty” (μέθοδος που ο hacker σου μπλοκάρει τα δεδομένα με σκοπό να σου ζητήσει λύτρα για την απελευθέρωση τους) ενώ στην πραγματικότητα τα δεδομένα είχαν κλαπεί. Η κατάσταση αυτή μεταφράστηκε τόσο σε αρνητική δημοσιότητα της εταιρίας όσο και σε μείωση κατά 20 δις δολάρια της αξιολόγησης της εταιρίας, καθώς τελικά ένα κομμάτι της που πουλήθηκε έναντι 48 δις δολαρίων στη Softbank έναντι των αρχικών 34.

9. **JP Morgan Chase**

Ημερομηνία: Ιούλιος 2014

Επίπτωση: Τα προσωπικά 42 εκατομμυρίων οικογενειών και 7 εκατομμυρίων μικρών επιχειρήσεων εκλάπησαν ως αποτέλεσμα κυβερνοεπίθεσης.

Λεπτομέρειες: Η μεγαλύτερη τράπεζα των ΗΠΑ, έπεσε θύμα hacker κατά τη διάρκεια του καλοκαιριού του 2014. Τα δεδομένα που εκλάπησαν περιείχαν μεταξύ άλλων ονόματα, διευθύνσεις, τηλεφωνικούς αριθμούς, e-mail, εσωτερικές πληροφορίες των πελατών κ.α. Η τράπεζα ανέφερε πως δεν είχαν ζημιωθεί οι προσωπικοί λογαριασμοί των χρηστών καθώς οι hacker δεν είχα συλλέξει τέτοιου

είδους δεδομένα. Παρ' όλα αυτά τα άτομα πίσω από τις κακόβουλες αυτές ενέργειες κατάφεραν και απέκτησαν δικαιώματα διαχειριστή σε περισσότερους από 90 server της τράπεζας καταφέρνοντας να πιστώσουν τους λογαριασμούς τους με περισσότερα από 100 εκατομμύρια δολάρια. Το Νοέμβριο του 2015, οι αρχές των ΗΠΑ εντόπισαν τα άτομα που ευθύνονταν για την εν λόγω κυβερνοεπίθεση και τους έφεραν ενώπιων της δικαιοσύνης.

10. **US Office of Personnel Management** (**OPM**)

Ημερομηνία: 2012-14
Επίπτωση: Προσωπικά δεδομένα 22 εκατομμυρίων δημοσίων υπαλλήλων των ΗΠΑ εκλάπησαν.
Λεπτομέρειες: Hacker, όπως φημολογείται από την Κίνα, μπήκαν στο σύστημα OPM το 2012, όπου και συνέχισαν τις ενέργειες τους, μέχρι να γίνουν αντιληπτοί το Μάρτιο του 2014. Μάλιστα, μια δεύτερη ομάδα hacker πραγματοποίησε κακόβουλες ενέργειες με τη σειρά της στο σύστημα OPM οι οποίες έγιναν αντιληπτές ένα χρόνο αργότερα. Οι hacker πήραν προσωπικά δεδομένα όλων των ειδών μέχρι και αποτυπώματα, ηλεκτρονικές υπογραφές ή ακόμα και πλήρεις φακέλους υπαλλήλων του FBI όπου και εμφανίζοντας όλες οι πληροφορίες για την προσωπική τους ζωή.

8.3 Γενικός Κανονισμός Προστασίας Δεδομένων

Αρχικά, είναι σκόπιμο να επεξηγηθεί συνοπτικά τι είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο οποίος είναι γνωστός και ως GDPR (General Data Protection Regulation General Data Protection Regulation). Ο GDPR στηρίζεται στο κανονισμό της (ΕΕ) 2016/339 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (εφεξής "Κανονισμός"), αφορά στην

διαμόρφωση ενός ενιαίου νομοθετικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης και αντικαθιστά την προηγούμενη Νομοθεσία “Οδηγία 95/46/ΕΚ”. Η (προηγούμενη) Οδηγία είχε ενσωματωθεί στην Ελληνική Νομοθεσία με το Ν. 2438. Δεν πρόκειται δηλαδή, για κάτι εντελώς νέο.

Το δικαίωμα που θεμελιώνει ο GDPR αφορά στη προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα τους Συγκεκριμένα, στο άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») και το άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) ορίζουν ότι κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Ο «κανονισμός» είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος (δηλαδή δεν απαιτείται ειδική προσαρμογή της Εθνικής Νομοθεσίας). (άρθρο 83 του «Κανονισμού»). Στην περίπτωση της χώρας μας, αυτό το ρόλο τον καλύπτει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ας δούμε όμως κάποιους βασικούς ορισμούς οι οποίοι και ορίζουν το GDPR. Ως δεδομένα προσωπικού χαρακτήρα λογίζεται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν

λόγω φυσικού προσώπου. Πιο συγκεκριμένα παραδείγματα δεδομένων προσωπικού χαρακτήρα τα οποία προσδιορίζουν ένα άτομο αποτελούν τα εξής:

1. Στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κ.λπ.)
2. Φυσικά χαρακτηριστικά
3. Εκπαίδευση
4. Εργασιακές σχέσεις
5. Οικονομική κατάσταση
6. Ηλεκτρονικά ίχνη
7. Ενδιαφέροντα, δραστηριότητες, συνήθειες

Επίσης υπάρχει μια υποκατηγορία προσωπικών δεδομένων, τα οποία και αναφέρονται στον πυρήνα της ιδιωτικής μας ζωής, χαρακτηρίζονται από το Νόμο ως ευαίσθητα και απολαύουν μεγαλύτερης προστασίας. Τα ευαίσθητα δεδομένα αναφέρονται αποκλειστικά σε:

1. Φυλετική ή εθνοτική προέλευση
2. Πολιτικά φρονήματα
3. Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
4. συμμετοχή σε συνδικαλιστική οργάνωση
5. υγεία και κοινωνική πρόνοια
6. ερωτική ζωή
7. ποινικές διώξεις και καταδίκες

8. συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων

Ως επεξεργασία δεδομένων νοείται κάθε εργασία ή σειρά εργασιών που πραγματοποιείται με ή όχι τη χρήση αυτοματοποιημένων μέσων σε δεδομένα προσωπικού χαρακτήρα, όπως: συλλογή, καταχώριση, οργάνωση, αποθήκευση, τροποποίηση, εξαγωγή, χρήση, διαβίβαση, διάδοση, συσχέτιση, διασύνδεση, δέσμευση, διαγραφή, καταστροφή. Η επεξεργασία προσωπικών δεδομένων είναι αναγκαία για την παροχή υπηρεσιών από τις δημόσιες υπηρεσίες, τις τράπεζες, τα νοσοκομεία, τα σχολεία, τα καταστήματα, τους τηλεπικοινωνιακούς φορείς κ.λπ., καθώς και για τη άσκηση πολλών άλλων δραστηριοτήτων που διευκολύνουν την καθημερινή μας ζωή.

Φυσικά όλα αυτά τα παραπάνω δεν θα ήταν μείζονος σημασίας εάν δεν κατανοήσει κανείς την σημασία της προστασίας των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα σε μια εποχή, όπου η ανάπτυξη της τεχνολογίας έχει αυξήσει τους κινδύνους για την ιδιωτική μας ζωή. Μέσα σε λίγα δευτερόλεπτα είναι δυνατό να αντληθούν διάφορα στοιχεία για την προσωπική, οικονομική ή και κοινωνική κατάσταση κάποιου προσώπου και το σημαντικότερο να συνδυασθούν με άλλες πηγές πληροφοριών, έτσι ώστε να οδηγήσουν σε μία συνολική καταγραφή της προσωπικότητάς του, στη σύνθεση δηλαδή του ατομικού του «προφίλ». Κάτω από τις συνθήκες αυτές δημιουργήθηκε η ανάγκη προστασίας του ατόμου από την ανεξέλεγκτη επεξεργασία πληροφοριών που το αφορούν.

Εξάλλου τα στοιχεία τα οποία είναι προς επεξεργασία νομίμως έπειτα από συγκατάθεσή μας, από τον εκάστοτε υπεύθυνο επεξεργασίας ο οποίος πρέπει να συμμορφώνεται με συγκεκριμένες αρχές που εξασφαλίζουν ότι τα προσωπικά δεδομένα:

1. Τυγχάνουν επεξεργασίας με τρόπο θεμιτό και νόμιμο
2. Τηρούνται για σαφώς καθορισμένους σκοπούς
3. Περιορίζονται στα απολύτως απαραίτητα για την επίτευξη των σκοπών αυτών
4. Είναι ακριβή και επίκαιρα
5. Τηρούνται για ορισμένο χρονικό διάστημα (ανάλογα με τους σκοπούς)
6. Προστατεύονται από επαρκή μέτρα ασφαλείας
7. Δεν διαβιβάζονται σε χώρες που δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας.

Φυσικά, η επεξεργασία των προσωπικών δεδομένων από τον υπεύθυνο επεξεργασίας πρέπει να συμμορφώνεται με συγκεκριμένες αρχές που εξασφαλίζουν ότι τα προσωπικά δεδομένα:

1. Τυγχάνουν επεξεργασίας με τρόπο θεμιτό και νόμιμο
2. Τηρούνται για σαφώς καθορισμένους σκοπούς
3. Περιορίζονται στα απολύτως απαραίτητα για την επίτευξη των σκοπών αυτών
4. Είναι ακριβή και επίκαιρα
5. Τηρούνται για ορισμένο χρονικό διάστημα (ανάλογα με τους σκοπούς)
6. Προστατεύονται από επαρκή μέτρα ασφαλείας

7. Δεν διαβιβάζονται σε χώρες που δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας.

Πως εξασφαλίζονται, από το νόμο, τα προσωπικά μας δεδομένα όμως; Ο Νόμος 2438/1997 ενσωματώνει στην Ελληνική έννομη τάξη την ευρωπαϊκή οδηγία 95/46/ΕΚ που ορίζει ένα πλαίσιο κανόνων για την επεξεργασία των προσωπικών μας δεδομένων, κοινό σε όλες τις χώρες της Ευρωπαϊκής Ένωσης. Ειδικότερα, ο νόμος θεσπίζει συγκεκριμένα χαρακτηριστικά που πρέπει να πληροί μια επεξεργασία για να είναι νόμιμη, ενώ καθιερώνει δικαιώματα για τα άτομα, ώστε να είναι σε θέση να ελέγχουν τα προσωπικά δεδομένα που τα αφορούν. Για το κρίσιμο θέμα της προστασίας των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες υπάρχει ο ειδικότερος νόμος 3437/2006 που ενσωματώνει στην ελληνική έννομη τάξη την ευρωπαϊκή οδηγία 2002/58/ ΕΚ. Η εποπτεία της εφαρμογής των παραπάνω νόμων, καθώς και άλλων ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων έχει ανατεθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Όμως τι υποχρεούνται να κάνουν οι επιχειρήσεις και εταιρίες επί της ουσίας σύμφωνα με το κανονισμό; Οι εταιρείες πλέον καλούνται να ασχοληθούν και επίσημα με την προστασία των πληροφοριακών τους συστημάτων και την προάσπιση των δεδομένων τους, κάνοντας τακτικά ελέγχους ασφάλειας δικτύων και υποδομών, υλοποιώντας πολιτικές ασφάλειας και διαδικασίες, αλλά και εκπαιδεύοντας τους χρήστες πληροφοριακών συστημάτων για την ορθή χρήση των πληροφοριακών συστημάτων τους. Ο Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στους υπευθύνους επεξεργασίας (το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας

δεδομένων προσωπικού χαρακτήρα), οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων. Κάθε υπεύθυνος επεξεργασίας (άρθρο 30) και, κατά περίπτωση, ο εκπρόσωπός του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος. Το εν λόγω αρχείο περιλαμβάνει όλες τις ακόλουθες πληροφορίες:

1. Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων,

2. Τους σκοπούς της επεξεργασίας,

3. Περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα

4. Τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,

5. Οπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, της τεκμηρίωσης των κατάλληλων εγγυήσεων,

6. Όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων

7. Όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος

Λαμβάνοντας υπόψη (άρθρο 24) τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό

Λαμβάνοντας υπόψη (άρθρο 25) τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

1. Της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα

2. Της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση

3. Της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος

4. Διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα (άρθρο 33) , ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 38 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 38 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Ποιές αρμοδιότητες έχει η Αρχή; Συγκεκριμένα, οι αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού διακρίνονται σε δύο βασικές κατηγορίες ως εξής:

1. Ελεγκτικές: εξέταση προσφυγών/καταγγελιών, διενέργεια ελέγχων στα αρχεία των υπεύθυνων επεξεργασίας (τραπεζών, ασφαλιστικών οργανισμών, νοσοκομείων, παρόχων ηλεκτρονικών επικοινωνιών, κ.λπ.), έκδοση αδειών τήρησης αρχείων με ευαίσθητα δεδομένα, τήρηση μητρώου γνωστοποιήσεων αρχείων με προσωπικά δεδομένα, εποπτεία του Συστήματος Πληροφοριών Σένγκεν (ΣΠΣ) και του Εθνικού Καταλόγου Ανεπιθύμητων Αλλοδαπών (ΕΚΑΝΑ).

2. Ρυθμιστικές: έκδοση οδηγιών και κανονιστικών πράξεων, κάθε άλλη πράξη ή ενέργεια που αποσκοπεί σε γενική και ομοιόμορφη εφαρμογή κανόνων επεξεργασίας, όπως η έκδοση γνωμοδοτήσεων για σχέδια νόμων και κανονιστικών πράξεων, η υποβοήθηση των επαγγελματικών σωματείων κατά την κατάρτιση κωδίκων δεοντολογίας, συστάσεις, υποδείξεις και απαντήσεις σε ερωτήματα υπεύθυνων επεξεργασίας.

Τέλος, αν και η Αρχή μπορεί να βεβαιώσει μόνο Διοικητικές ποινές, μπορει να παραπέμψει την υπόθεση στον αρμόδιο Εισαγγελέα όταν υπάρχουν ενδείξεις ποινικής ευθύνης. Έτσι βλέπουμε πως προβλέπονται ιδιαίτερα αυστηρές ποινές όπως φαίνεται στο παρακάτω διάγραμμα.

Πίνακας 6 - Πιθανά πρόστιμα από την μη εφαρμογή του GDPR

ΥΨΟΣ ΠΡΟΣΤΙΜΟΥ	ΕΙΔΟΣ ΠΑΡΑΒΑΣΗΣ
έως 10 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο	1. οι υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία σύμφωνα με τα άρθρα 8, 11, 25 έως 39 και 42 και 43, 2. οι υποχρεώσεις του φορέα πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 3. οι υποχρεώσεις του φορέα παρακολούθησης σύμφωνα με το άρθρο 41 παράγραφος 4
έως 20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο	1. οι βασικές αρχές για την επεξεργασία, περιλαμβανομένων των όρων που ισχύουν για την έγκριση, σύμφωνα με τα άρθρα 5, 6, 7 και 9 2. τα δικαιώματα των υποκειμένων των δεδομένων σύμφωνα με τα άρθρα 12 έως 22 3. η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό σύμφωνα με τα άρθρα 44 έως 49 4. οποιεσδήποτε υποχρεώσεις σύμφωνα με το δίκαιο του κράτους μέλους οι οποίες θεσπίζονται δυνάμει του κεφαλαίου IX που περιλαμβάνει διατάξεις που αφορούν ειδικές περιπτώσεις επεξεργασίας όπως για δημοσιογραφικούς σκοπούς και για σκοπούς πανεπιστημιακής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, για σκοπούς επεξεργασίας στο πλαίσιο της απασχόλησης εργαζομένων, για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς καθώς και για σκοπούς επεξεργασίας δεδομένων εκκλησιών και θρησκευτικών ενώσεων. 5. μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή δυνάμει του άρθρου 58 παράγραφος 2 ή μη παροχή πρόσβασης κατά παράβαση του άρθρου 58 παράγραφος 1 6. Η μη συμμόρφωση προς εντολή της εποπτικής αρχής όπως αναφέρεται στο άρθρο 58 παράγραφος 2

8.4 Νέες υπηρεσίες και απόρρητο της επικοινωνίας

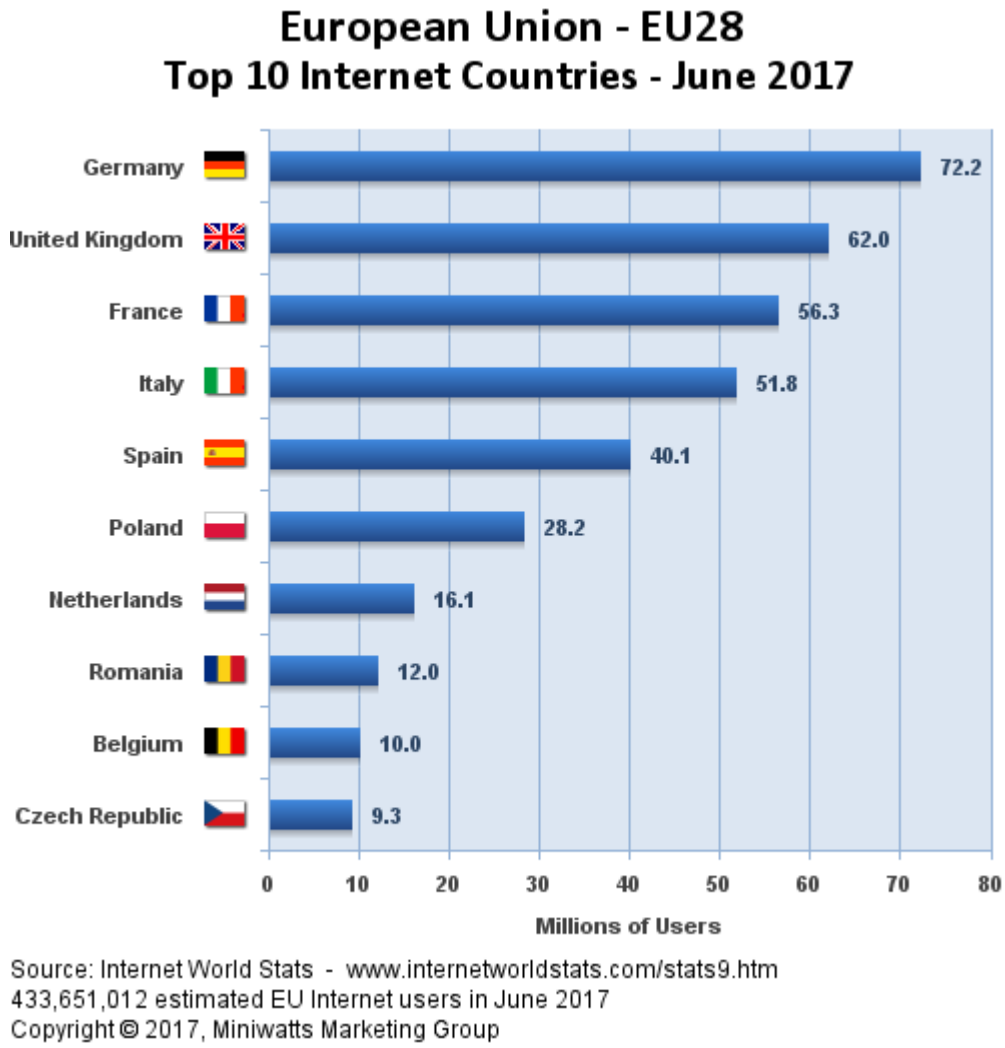
Όπως είδαμε προηγουμένως, η ραγδαία εξέλιξη της τεχνολογίας δίνει έναυσμα στην ανάπτυξη νέων φορμών ηλεκτρονικής εγκληματικότητας και προσβολών του απορρήτου της επικοινωνίας και της ιδιωτικής ζωής. Παραδείγματος χάρη, η εισαγωγή της ψηφιακής τεχνολογίας στις τηλεπικοινωνίες επιτρέπει, αφενός, την παροχή στους συνδρομητές επιπλέον διευκολύνσεων, όπως πχ καταστάσεις αναλυτικής χρεώσεις, οπού αναγράφονται οι κληθέντες αριθμοί από την συσκευή του συνδρομητή, ή η διάρκεια κάθε συνομιλίας και η σχετική τιμολόγηση. Η νέα αυτή υπηρεσία είναι καταρχήν επιθυμητή στο μετρό που επιτρέπει σε μια επιχείρηση την καλύτερη διαχείριση του τηλεπικοινωνιακού κόσμου, όπως πχ με την δυνατότητα έλεγχου και διαχωρισμού των επαγγελματικών και προσκοπικών κλήσεων των υπάλληλων της, ενώ παράλληλα επιτρέπει την άρση πιθανών αμφισβητήσεων από τον πελάτη σχετικά με το ύψος των τελών τα όποια χρεώνονται από τον τηλεπικοινωνιακό οργανισμό [53]. Ταυτόχρονα όμως η αναλυτική αποτύπωση πολλών, ή έστω των τεσσάρων πρώτων ψηφίων των αριθμών που καλούνται από μια συγκεκριμένη συσκευή, καθώς και η διατήρηση των σχετικών στοιχείων στα ηλεκτρονικά αρχεία τιμολόγησης συνδρομητών των τηλεπικοινωνιακών οργανισμών εμπεριέχει το ενδεχόμενο έλεγχου και προσβολής της ιδιωτικής ζωής καλούντων και καλουμένων, με όλες τις συναφείς κοινωνικό-πολιτικές προεκτάσεις της επεξεργασίας προσωπικών δεδομένων, όπως αυτά προσδιορίστηκαν παραπάνω [53]. Παράλληλα, εκτός από τον κίνδυνο προσβολής της ιδιωτικής σφαίρας του ατόμου η συλλογή δεδομένων προσωπικού χαρακτήρα τα οποία αφορούν τους συνδρομητές είναι δυνατόν να χρησιμοποιηθεί από τους τηλεπικοινωνιακούς οργανισμούς για καθαρά εμπορικούς σκοπούς ακόμα δε για την επίτευξη αθέμιτου ανταγωνιστικού πλεονεκτήματος σε σχέση με άλλους παρόχους υπηρεσιών. Λογού χάριν, η

συλλογή των προτιμήσεων του καταναλωτικού κοινού στα πλαίσια μια υπηρεσίας τηλεαγορών ή τηλέ-ηχοπληροφόρισης είναι δυνατόν να μεταπωληθεί σε εταιρεία direct mail με στόχο την εξατομικευμένη προβολή και προώθηση καταναλωτικών προϊόντων [53]. Εξεταζόμενο σε μια ευρύτερη προοπτική, το πρόβλημα γίνεται ακόμα πιο σύνθετο στον εργασιακό χώρο οπού ειδικές συσκευές επιτρέπουν τον έλεγχο των επαγγελματικών και των προσωπικών χρήσεων με στόχο με την θεμιτή μείωση των τηλεπικοινωνιακών δαπανών της επιχείρησης, αλλά με κίνδυνο της αθέμιτης της προσωπικής συνδικαλιστικής ελευθερίας, ιδιαίτερα σε περίπτωση μη εξουσιοδοτημένης πρόσβασης και εκμετάλλευσης των ανώτερο αναλυτικών στοιχείων κλήσεων του προσωπικού από τον εργοδότη, το λογιστήριο της επιχείρησης, αλλά και από τυχόν τρίτους. [53]. Σχετικά με το ζήτημα αυτό, το οποίο αντιμετωπίστηκε στα πλαίσια άλλων έννομων τάξεων, όπως πχ στην Γάλλια, οι ανεξάρτητοι κανονιστική αρχή προστασίας των δεδομένων έχει καθορίσει, με μια σειρά μέτρων, τις τεχνικές και κανονιστικές προδιαγραφές που πρέπει να τηρούνται από την France Telecom αλλά και από τους ανταγωνιστές της για παρόμοιες επεξεργασίες, η παράβαση των οποίων απαιτεί αυστηρές κυρώσεις για την παραβάτισσα τηλεπικοινωνιακή επιχείρηση [35].

8.5 Ασφάλεια δεδομένων και ηλεκτρονική εγκληματικότητα

Πέρα από την συνταγματική διάσταση του, η οποία σχετίζεται με την διασφάλιση του απορρήτου της επικοινωνίας και των ανταποκρίσεων το θέμα της ασφάλειας δεδομένων παρουσιάζει αναμφίβολα μια σημαντικότατη οικονομική διάσταση πλέον όχι μόνο σε συγκεκριμένους κλάδους όπως αυτοί των τηλεπικοινωνιών αλλά στους περισσότερους οργανισμούς που διατηρούν δεδομένα στο δίκτυο. [53]. Καθώς ολοένα και περισσότεροι οργανισμοί χρησιμοποιούν ψηφιακά δεδομένα τα οποία και αποθηκεύουν σε βάσεις δεδομένων που βρίσκονται σε δίκτυα προσβάσιμα από την εκάστοτε επιχείρηση ή οργανισμό δημιουργούνται οι κατάλληλες συνθήκες για να

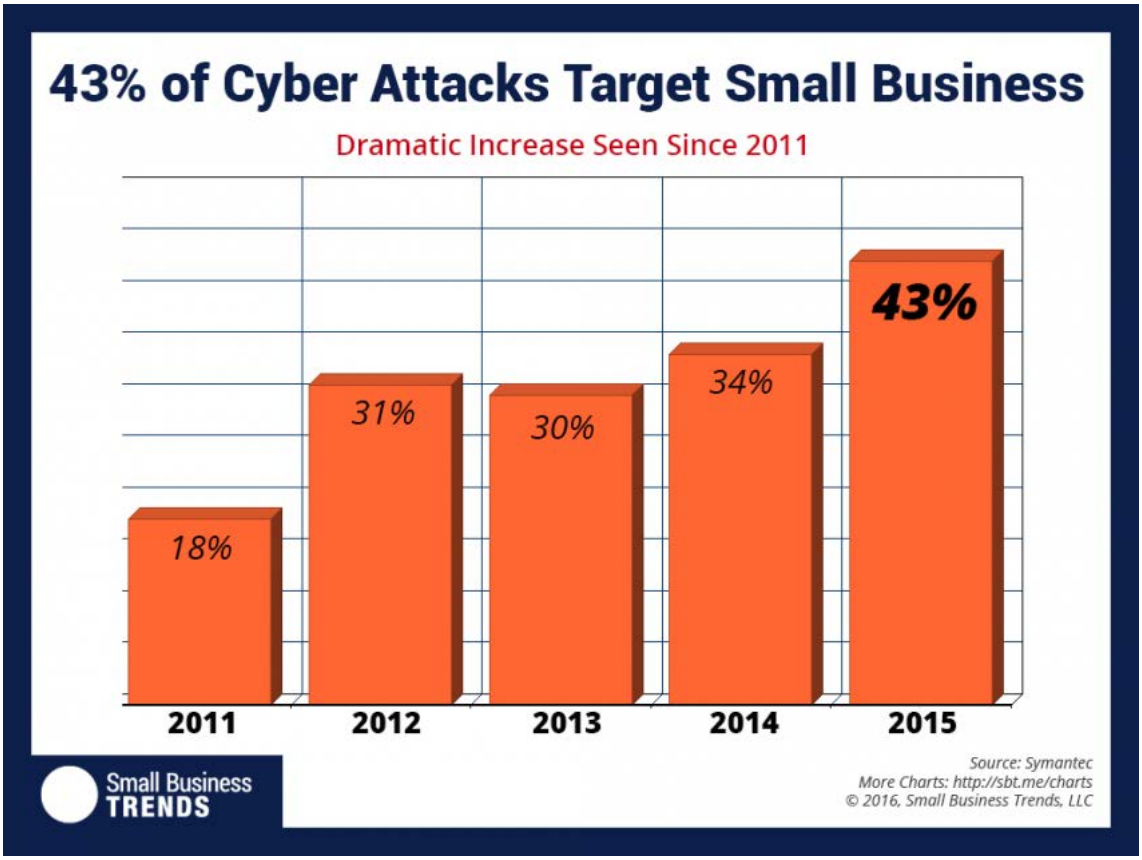
ευδοκιμήσει η ηλεκτρονική εγκληματικότητα. Το προαναφερθέν επιχείρημα αποκτά βαρύνουσα σημασία, εάν αναλογιστεί κανείς την διείσδυση του Internet στα νοικοκυριά της Ευρώπης. Ιδιαίτερα παραστατικό είναι ή παρακάτω εικόνα.



Σχήμα 16 – Χώρες της Ευρώπης με το μεγαλύτερο αριθμό χρηστών Internet

Επίσης, ενώ παλαιότερα θύματα επιθέσεων ηλεκτρονικού εγκλήματος έπεφταν κυρίως οι μεγάλες επιχειρήσεις και οργανισμοί οι οποίοι και διατηρούσαν τα δεδομένα τους ηλεκτρονικά, καθώς το internet και οι υπηρεσίες δικτύου έχουν διεισδύσει στα περισσότερα νοικοκυριά της Ευρώπης και συνδράμουν στην μείωση του κόστους λειτουργίας των επιχειρήσεων – ακόμα και των μικρών,

βλέπουμε αύξηση της ηλεκτρονικής εγκληματικότητας ακόμα και στους κλάδους των μικρομεσαίων που τόσα χρόνια αποτελούσαν ένα ασφαλές προπύργιο.



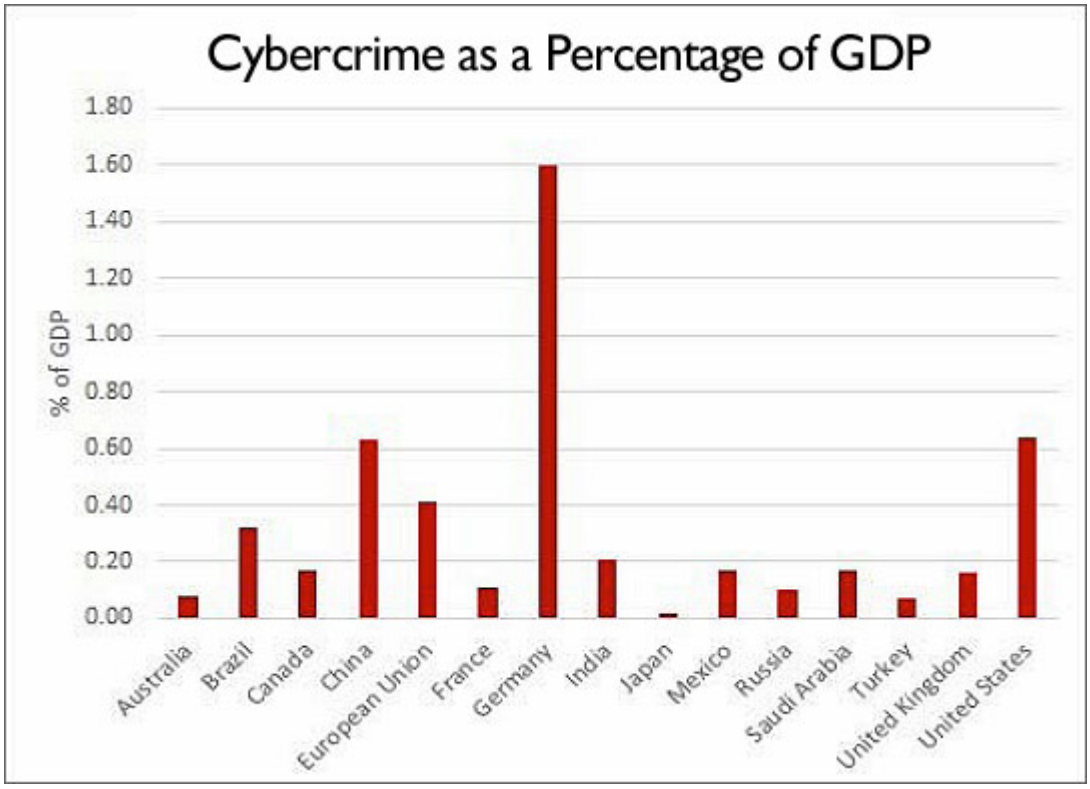
Σχήμα 17 – Ποσοστά κυβερνοεπιθέσεων σε μικρές επιχειρήσεις

8.6 Το κόστος της αθέμιτης πρόσβασης

Συμφώνα με στοιχεία του Αμερικανικού περιοδικού "Fortune" οι εκατό μεγαλύτερες εταιρίες των ΗΠΑ έχουν καταγγείλει τέτοια φαινόμενα τηλεπικοινωνιακής εγκληματικότητας των οποίων το κόστος μέχρι των εντοπισμό της προσβολής μέσω ειδικού λογισμικού έλεγχου ξεπέρασε κατά μέσο όρο τις 25 χιλιάδες δολάρια ανά εταιρία, ποσό το οποίο αντιπροσωπεύει ένα συνολικό ετήσιο κόστος ανώτερο των 100 εκατομμυρίων δολαρίων. Εκτός

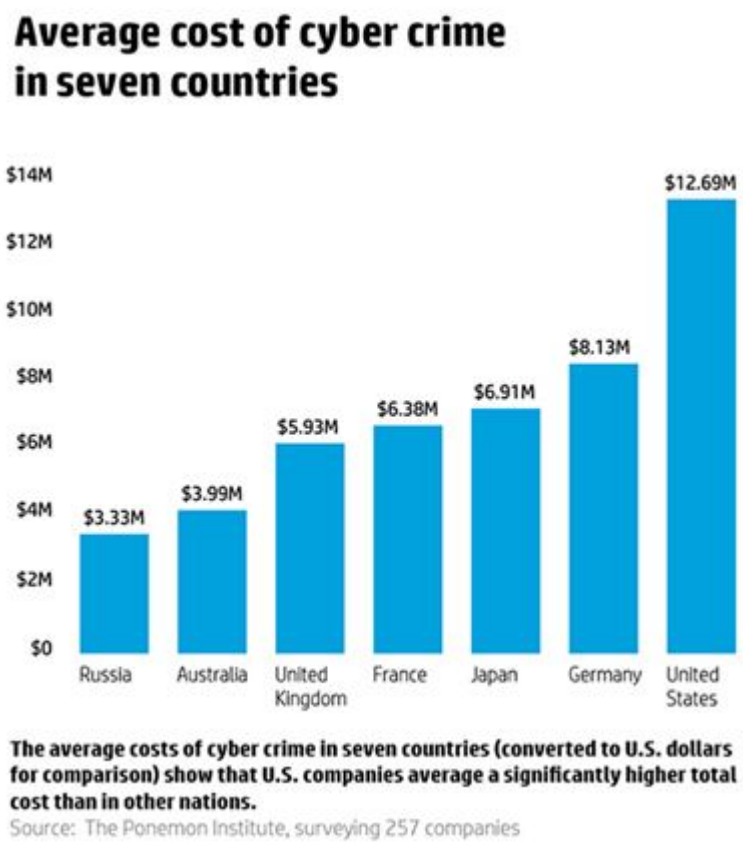
όμως της άμεσα υπολογίσιμης ζημιάς, οι περιπτώσεις αυτές δίνουν συχνά λαβή και σε περεταίρω δικαστικές διενέξεις μεταξύ των οργανισμών και των πελατών τους των οποίων τα συμφέροντα θίγονται με αποτέλεσμα το μετρήσιμο κόστος να ξεπερνά κατά πολύ την αρχική εκτίμηση της ζημιάς [53].

Για να γίνει καλύτερα αντιληπτό, παραθέτουμε μερικά στατιστικά στοιχεία, και ποιο συγκεκριμένα σύμφωνα με μελέτη της GuildInvestment, μίας από τις μεγαλύτερες επιχειρήσεις διαχείρισης χαρτοφυλακίων που χρονικά τοποθετείται στο 2014, το ηλεκτρονικό έγκλημα μπορεί να φθάσει έως και το 1.6% του ετήσιου ΑΕΠ μιας χώρας, ποσό ιδιαίτερα υψηλό αν αναλογιστεί πως στη Γερμανία λόγου χάριν το ΑΕΠ το 2014 ήταν περίπου 3,5 τρις Ευρώ. Φυσικά όλα αυτά χωρίς να υπολογιστεί η ζημιά σε φήμη που υπόκεινται οι εταιρίες καθώς και η εμπιστοσύνη των καταναλωτών που μακροπρόθεσμα θίγουν τα οικονομικά συμφέροντα των εταιριών που υπόκεινται σε κυβερνο-επιθέσεις.



Σχήμα 16 – Κόστος κυβερνο-επιθέσεων ανά χώρα με βάση το ΑΕΠ

Μάλιστα είναι φανερό πως το μέσο κόστος των κυβερνο-επιθέσεων σχετίζεται με το ποσοστό συνδρομητών Internet καθώς και του ηλεκτρονικού κύκλου εργασιών των επιχειρήσεων.



Σχήμα 17 – Μέσο Κόστος Κυβερνο-επιθέσεων ανά χώρα

9 Συμπεράσματα

Τα ασύρματα δίκτυα αισθητήρων αποτελούν μια τεχνολογία η οποία εξελίσσεται και δίνει λύσεις σε ανάγκες εμπορικές προσωπικές και επιστημονικές ανάγκες λόγω του ολοένα και χαμηλότερου κόστους, της χαμηλής ισχύς που χρειάζονται και της ιδιάζουσας ιδιότητας τους ως προς την τοποθέτηση με σκοπό την δημιουργία ενός ασύρματου δικτύου. Ενώ θα μπορούσε κανείς συνοπτικά κατηγοριοποιώντας τις ενέργειές να τις κατατάξει σε εργασίες μέτρησης μεγεθών, αντίληψης γεγονότων (monitoring) αλλά και ανίχνευσης. Φυσικά το μεγάλο τους πλεονέκτημα είναι η δυνατότητα ανάπτυξης τους ως δίκτυο σε δυσπρόσιτα περιβάλλοντα με μεθόδους που δεν απαιτούν φυσική παρουσία Φυσικά τα προαναφερθέντα πλεονεκτήματα έρχονται να αντισταθμιστούν με παράγοντες όπως η υπολογιστική ισχύς, η μνήμη, η ενέργεια, το εύρος ζώνης που αποτελούν περιοριστικούς παράγοντες εκ φύσεων και κατασκευής των ΑΔΑ. Βεβαίως καθώς τα ΑΔΑ χρησιμοποιούν ήδη αναπτυγμένα πρωτόκολλα επικοινωνίας ελαχιστοποιούν τη μετάδοση δεδομένων καθώς και τη ταχύτητα μετάδοσης με σκοπό να αντιμετωπίσουν τους περιοριστικούς παράγοντες στους οποίους και υπόκεινται.

Η τοπολογία που επιλέγεται ανά περίπτωση για την εφαρμογή μιας λύσης ΑΔΑ ποικίλει ανά την περίπτωση και με βάση τις ανάγκες της. Έτσι βλέπουμε peeri-to-peer, star, tree ή mesh τοπολογίες των οποίων η επιλογή σχετίζεται με διαφορετικές ιδιότητες. Το μοντέλο επικοινωνίας ανά τα επίπεδα (OSI layer) έρχεται να προσομοιάσει τα ευρέως γνωστά μοντέλα επικοινωνίας και μάλιστα χωρίς ιδιαίτερες παρεκκλίσεις από τα διάφορα πρωτόκολλα επικοινωνίας όπως η οικογένεια των WI - FI 802.11, τα πρωτόκολλα σε λογική CSMA και τα πρωτόκολλα routing. Φυσικά λόγω των συγκεκριμένων ενεργειών που επιτελούν τα ΑΔΑ και των αντίστοιχα περιορισμένων υπολογιστικών τους δυνατοτήτων σε επεξεργαστική ισχύ και μνήμη χρησιμοποιούν συγκεκριμένα λειτουργικά συστήματα όπως Mantis, Nano, ListOS κ.α.

Ιδιαίτερη μνεία πρέπει να γίνει στις εφαρμογές που έρχονται να παρουσιάσουν τα ΑΔΑ. Βλέπουμε την δυνατότητα εφαρμογής τους σε περιβαλλοντικές, αγροτικές, οικιακές, βιομηχανικές, στρατιωτικές, οικιακές και άλλες κατηγορίες κλάδων. Κοινός παράγοντας σε όλες τις εφαρμογές τους ανά το κλάδο είναι το ιδιαίτερο της τοποθέτησής των ΑΔΑ σε περιβάλλοντα εξαιρετικά δυσπρόσιτα, της δυνατότητας λειτουργίας με την ελάχιστη συμβολή του ανθρώπινου παράγοντα και φυσικά λόγω του ελάχιστα μικρού τους φυσικού μεγέθους. Μάλιστα καθώς μιλάμε για δίκτυα, είναι δυνατή η δημιουργία οικονομιών κλίμακας, μεγεθύνοντας την αξία της υπηρεσίας που παραδίδουν τα ΑΔΑ απλώς προσθέτοντας περισσότερους πομποδέκτες. Η έννοια δηλαδή του οριακού οφέλους βλέπουμε πως δεν έχει ιδιαίτερη εφαρμογή στα ΑΔΑ, καθώς κατά γενική ομολογία περισσότεροι και ισχυρότεροι πομποδέκτες δημιουργούν βελτίωση της υπηρεσίας.

Φυσικά, όπως είναι λογικό οι μηχανισμοί ασφάλειας στα ασύρματα δίκτυα αισθητήρων, αν και πρέπει να υπόκεινται σε αυστηρές προδιαγραφές κατανάλωσης ενέργεια και επεξεργαστικής ισχύς, είναι ένα πολύ σημαντικό κομμάτι της λειτουργίας τους. Σε ένα δίκτυο οι λειτουργίες της δημιουργίας, λήψης και μετάδοσης μηνυμάτων πρέπει να υποστηρίζονται από τους κατάλληλους μηχανισμούς ασφάλειας, ώστε το δίκτυο να λειτουργεί απρόσκοπτα. Ο ορισμός της ασφάλειας πρέπει να περιλαμβάνει τις διεργασίες που γίνονται σε κάθε κομμάτι του δικτύου ώστε τα μηνύματα να φτάνουν ασφαλή στον προορισμό τους. Η ασφάλεια στα δίκτυα αισθητήρων είναι δύσκολο να επιτευχθεί λόγω των ιδιαιτεροτήτων που τα καθορίζουν. Για να εξασφαλίσουμε ότι ένα δίκτυο είναι ασφαλές, πρέπει να διασφαλίσουμε ότι το κάθε κομμάτι που αποτελεί το δίκτυο είναι ασφαλές.

Τα χαρακτηριστικά και οι απαιτήσεις των ασύρματων δικτύων αισθητήρων, μας οδηγούν σε αριθμό τροποποιημένων αλλά και συμβατικών μηχανισμών

ασφαλείας σε σχέση με τα παραδοσιακά δίκτυα υπολογιστών καθώς μοιράζονται τις ίδιες ευπάθειες στις απειλές με τα δίκτυα υπολογιστών όπως τα γνωρίζουμε όπως είναι λογικό από τη στιγμή που χρησιμοποιούν ίδια πρωτόκολλα επικοινωνίας και παρεμφερή αρχιτεκτονική με τα ασύρματα δίκτυα ηλεκτρονικών υπολογιστών. Παράλληλα όμως με βάση την ιδιαιτερότητα τους ως προς την υλοποίηση τους, τα ΑΔΑ εκτίθενται και σε άλλους ειδικότερους κινδύνους όπως ενεργειακούς, καθώς τα ασύρματα δίκτυα αισθητήρων λειτουργούν με μπαταρία ή με κάποιο άλλο αυτόνομο μέσο, πρέπει οι μηχανισμοί ασφαλείας να μην είναι ενεργοβόροι, όμως οι επιθέσεις στον κόμβο μπορούν να εστιάσουν στην κατανάλωση ενέργειας του, ώστε να βγει εκτός λειτουργίας. Επίσης πέραν των ενεργειακών κινδύνων που αντιμετωπίζουν τα ΑΔΑ, αντιμετωπίζουν κινδύνους που έχουν να κάνουν με επιθέσεις από ισχυρούς πομπούς που σκοπό έχουν να πλήξουν τη μετάδοση δεδομένων από τους ασθενής πομπούς που εφαρμόζουν τα ΑΔΑ.

Πρέπει κανείς λοιπόν να συνυπολογίσει την πληθώρα των εφαρμογών των ΑΔΑ, τα αντίστοιχα οικονομικά και κοινωνικά οφέλη που μπορούν να δημιουργήσουν υπό το πρίσμα των ζητημάτων ασφάλειας που εφάπτονται της υλοποίησης και λειτουργίας τους. Η συγκεκριμένη “άσκηση” – ανάλυση αποκτά ιδιαίτερη σημασία εάν γίνει υπό το πρίσμα της νομοθεσίας που έρχεται να προστατεύσει τα προσωπικά δεδομένα τα οποία δημιουργούν και επεξεργάζονται τα ΑΔΑ. Όπως είδαμε και στο κεφάλαιο οκτώ περί Νομικών θεμάτων ασφάλειας και ειδικότερα με το την εφαρμογή από το Μάιο του 2018 του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) υπάρχει μια δυναμική και μια πολιτικό-οικονομική βούληση προς την προστασίας των δεδομένων, ένα χώρο που μέχρι πρότινος αποτελούσε περιοχή αμφισβήτησης ό οποίος συνδεόταν μόνο ποσοτικά με τις ζημιές που εν δυνάμει δημιουργούσε σε μια επιχείρηση ή οργανισμό υπό το πρίσμα της κυβερνοεπίθεσης.

Συνοψίζοντας, τα ΑΔΑ ιδρύουν μια νέα αγορά ενώ παράλληλα δημιουργούν διαφορετική δυναμική σε ήδη υπάρχουσες. Η τεχνολογική εξέλιξη σε θέματα

αυτονομίας, ισχύος επεξεργασίας, πρωτοκόλλων επικοινωνίας κλπ αποτελεί εφαλτήριο για περεταίρω ανάπτυξη των ΑΔΑ και των λύσεων που μπορούν να δώσουν σε καταστάσεις όπου η γεωγραφία, η τοποθεσία και ο χώρος αποτελούσαν μέχρι πρότινος αποτρεπτικούς παράγοντες.

10 Βιβλιογραφικές Αναφορές

1. I. F. Akyilditz, W. Su, Y. Sankarasubramamian, E. Cayirci, “Wireless Sensor Networks: A survey”, Computer Networks, 2002.

2. I. F. Akyilditz, X. Wang, W. Wang, “Wireless mesh networks: A survey”, Computer Networks, 2005

3. J. Yick, B. Mukherjee, D. Ghosal, “Wireless sensor network survey”, Computer Networks, 2008

4. F. Zhao, L.Guibas, “Wireless Sensor Networks”, Elsevier, 2004

5. K. Römer, H. Karl, F. Mattern, “Wireless sensor networks”, 3rd European workshop.(EWSN 06), Zurich, 2006

6. M. Ilyas, I. Mahgoub, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, 2004

7. K. Sohraby, D. Minoli, T. Znati, Wireless sensor networks: Technology, Protocols, and Applications, Wiley, 2007

8. Y W Zhu, XX Zhong and J F Shi. The Design of Wireless Sensor Network System Based on, J. Phys.: Conf. Ser, 48, 2006

9. Stockwell, AgricultureDr. Walter. Wireless Sensor Networks for Precision Agriculture, Intechopen, 2011

10. Κοκκινάκης, Γεώργιος. ΕισαγωγήσταΤηλεπικοινωνιακάΣυστήματα. Πάτρα: s.n., 2004

11.Erik Aguirre,Peio Lopez-Iturri, Leire Azpilicueta, José Javier Astrain, Jesús Villadangos,andFrancisco Falcone, Analysis of Wireless Sensor Network Topology and Estimation of Optimal Network Deployment by Deterministic Radio Channel Characterization, MDPI 2015

12. Mark A. Perillo and Wendi B. Heinzelman, Wireless Sensor Network Protocols, IEEE, 2011

13. Vlado Handziski, Joseph Polastre, Jan-Hinrich Hauer, Cory Sharp, Adam Wolisz, David Culler, David Gay, Hardware Abstraction Architecture, TEP 2, 2007

14. Philip Levis and Cory Sharp, Schedulers and Tasks, TEP 106, 2012.

15. Philip Levis, David Gay, TinyOs Programming, Cambridge University Press, 2009

16. Levis, Philip, TinyOS Programming, Standford CS 2006

17. I. F. Akyildiz, M. C. Vuran, Wireless Sensor Networks, Willey, 2010

18. W. Dargie, Ch. Poellabauer, Fundamentals of Wireless Sensor Networks Theory and Practice, Wiley, 2010

19. K. Martinez, J.K. Hart, R. Ong, “Environmental Sensor Networks”, IEEE Computer, Manuscript id, 2004

20. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, J. Anderson, “Wireless sensor networks for habitat monitoring”, Proc. 1st ACM international Workshop on Wireless Sensor Networks and Applications (WSNA '02), ACM Press, New York, September 2002

21. G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees, M. Welsh, “Monitoring Volcanic Eruptions with a Wireless Sensor Network,” Proc. 2nd European Workshop Wireless Sensor Networks (EWSN 05), IEEE Press, 2005

22. 13. D. Culler, D. Estrin, M. Srivastava, “Overview of Sensor Networks”, IEEE Computer, Vol. 37, No. 8, August 2004

23. P. Zhang, C. Sadler, S. Lyon, M. Martonosi, “Hardware design experiences in ZebraNet”, Proc. ACM SenSys’04, Baltimore, USA, November 2004

24. J. Burrell, T. Brooke, and R. Beckwith, “Vineyard Computing: sensor networks in agricultural production”, IEEE Pervasive Computing,2012

25. M. Hefeeda, S. Fraser ,“Forest Fire Modeling and Early Detection using Wireless Sensor Networks”, University Canada,2012

26. R. G. Lee, K. C. Chen, S. S. Chiang, C. C. Lai, H. S. Liu, M. S. Wei, “A Backup Routing with Wireless Sensor Network for Bridge Monitoring System”, Proc. 4th Annual Communication Networks and Services Research Conference (CNSR’06), Computer Networks, 2006

27. L. Krishnamurthy, R. Adler, P. Buonadonna, J. Chhabra, M. Flanigan, N. Kushalnagar, L. Nachman, M. Yarvis, “Design and Deployment of Industrial

Sensor Networks: Experiences from a Semiconductor Plant and the North Sea", Proc. 3rd International Conference on Embedded Networked Sensor Systems (SenSys '05), November 2005

28. E. Shih, V. Bychkovsky, D. Curtis, J. Guttag, "Demo Abstract: Continuous Medical Monitoring Using Wireless Microsensors", Proc. 2nd International Conference on Embedded Networked Sensor Systems, 2004

29. T. V. Ngoc, "Medical Applications of Wireless Networks: A survey paper written under guidance of Prof. Raj Jain", 2008

30. Γ. Πάγκαλος, Ι. Μαυρίδης*, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων*, Ανικούλας, Θεσσαλονίκη, 2002

31. Αρβανίτης Διονύσιος, "Υλοποίηση πρωτοκόλλων κρυπτογράφησης χαμηλής κατανάλωσης ενέργειας για ασύρματα δίκτυα αισθητήρων", Διπλωματική Εργασία, Πανεπιστήμιο Θεσσαλίας, ΤΜΗΥΤΔ, 2008

32. Δημήτριος Κουτσουβέλας, Ηλίας Κωστούδης, "Ασφάλεια σε δίκτυα ad hoc και δίκτυα αισθητήρων", Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, 2008

33. D. Djenouri, L. Khelladi, "A Survey of security issues in mobile ad hoc and sensor networks", IEEE Communication Surveys, 2005

34. W. Stallings, "Cryptography and Network Security Principles and Practices", 3rd edition, Pearson Education Inc, 2003

35. A. Perrig, R. Szewczyk, V. Wen, D. culler, J. Tygar, "SPINS: security protocols for sensor networks" Proc. 7th Annual ACM International Conference on Mobile Computing and Networks (Mobicom 2001), Rome, Italy,2001

36. F. Hu, N. K. Sharma, "Security considerations in ad hoc sensor networks", Computer Science (Elsevier),September 2003

37. S. Zhu, S. Setia, S. Jajodia, "LEAP: Efficient Security Mechanisms for Large- Scale Distributed Sensor Networks", Proc. 10th ACM conference on computer communications security, Washington, DC, USA 2003

38. Z. Yan, "Security in ad hoc networks", Networking Laboratory,Helsinki University of Technology

39. W. Seah, Y. K. Tan, “Sustainable Wireless Sensor Networks”, InTech, 2010

40. S.Glisic, B.Vucetic, “Spread Spectrum CDMA Systems for Wireless Communications”, Artech House Mobile Communications Series, 1997

41. A. Wood, J. Stancovic, “Denial of Service in Wireless Sensor Networks”, IEEE Computer, 2002

42. G. Schafer, “Sensor Network Security”, The industrial Communications Technology Handbook, CRC Press, 2004

43. C.L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, D. Zamboni, “Analysis of a Denial of Service Attack on TCP”, Proc. IEEE Symp. Security and Privacy, IEEE Press, 1997

44. J. Newsome, E. Shi, D. Shong, A. Perrig, “The Sybil attack in sensor networks: analysis & defenses”, Proc. 3rd international symposium on Information processing in sensor networks, ACM Press, 2004

45. S. Madden, M. J. Franklin, J. M. Hellerstein, W. Hong. TAG, “A tiny aggregation service for ad hoc sensor networks”, In Symposium on Operating Systems Design and Implementation, 2002

46. M. Gruteser, G. Schelle, A. Jain, R. Han, D. Grunwald, “Privacy-aware location sensor networks”, Proc. 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), 2003

47. H. Chan, A. Perrig, “Security and privacy in sensor networks”, IEEE Computer Magazine, 2003

48. X. Wang, W. Gu, K. Schosek, S. Chellappan, D. Xuan, “Sensor network configuration under physical attacks”, Department of Computer Science and Engineering, The Ohio State University, 2004

49. C. Karlof , D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, Proc 1st IEEE International Workshop on Sensor Networks Protocols and Applications, May 2003

50. Y. C. Hu, A. Perrig, D. B. Johnson, “Wormhole attacks in wireless networks”, IEEE Journal on selected areas in communication vol. 24, no 2, February 2006

51. D. W. Carman, P. S. Krus, B. J. Matt, “Constraints and approaches for distributed sensor network security”, tech. report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA , 2000

52. J. Deng, R. Han, S. Mishra, “Countermeasures against traffic analysis in wireless sensor networks”, tech. report, University of Colorado at Boulder, 2004

53. Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα 1995, Εκδόσεις Νέων Τεχνολογιών.

11 Ηλεκτρονικό Υλικό

I. Wikipedia, OSI model: http://en.wikipedia.org/wiki/OSl_model

II. Wikipedia, http://en.wikipedia.org/wiki/Carrier_sense_multiple_access

III. Wikipedia, http://en.wikipedia.org/wiki/Time_division_multiple_access

IV. Wikipedia, http://en.wikipedia.org/wiki/IEEE_462 .15.4-2006

V. Wikipedia,http://en.wikipedia.org/wiki/Sensor_node

VI.Wikipedia,http://el.wikipedia.org/wiki/%CE%91%CE%B9%CF%83%CE%

B8%CE% B7%CF%84%CE%AE%CF%47 %CE%B1 %CF%48

VII. Wikipedia,http://en.wikipedia .org/wiki/Wireless_sensor_network

VIII. Wikipedia, http://en.wikipedia.org/wiki/NesC

IX. CSO, https://www.csoonline.com/article/2130843/data-breach/the-biggest-data-breaches-of-the-21st-century.html

X. European Union Law Library, http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0339

XI. Αρχή Δεδομένων Προστασίας Προσωπικού Χαρακτήρα, http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL