Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και
Μηχανικων Η/Υ

Εργασια στο Μεταπτυχιακο Μαθημα
Δικτυα Κινητων και Προσωπικων Επικοινωνιων

Ανίχνευση Επιθέσεων σε Ασύρματα Δίκτυα μέσω Αναγνώρισης Ανωμαλιών στη Δικτυακή Κίνηση

Δημήτριος Πολίτης (ΥΔ)

Επιβλέπων
Καθ. Ευστάθιος Συκάς

11 Απριλίου 2017

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Περίληψη

Η ανίχνευση ανωμαλιών στη δικτυακή κίνηση ασύρματων δικτύων είναι μια σημαντική διαδικασία, η οποία χρησιμοποιείται για την διάγνωση βλαβών, την ανίχνευση επιθέσεων και την παρακολούθηση εφαρμογών. Σε αυτό το πόνημα εξετάζουμε διάφορες προσεγγίσεις ανίχνευσης εισβολών, που βασίζονται σε μεθόδους καταγραφής των ανωμαλιών στη δικτυακή κίνηση και οι οποίες περιλαμβάνουν μεταξύ άλλων στατιστικές, signature based ή μεθόδους που περιλαμβάνουν μηχανική μάθηση (machine learning). Η προσέγγισή μας βασίζεται στην καταγραφή και ταξινόμηση σύγχρονων μεθόδων ανίχνευσης εισβολών σε ασύρματα δίκτυα(wireless intrusion detection system (IDS) με βάση τον τύπο του ασύρματου δικτύου, την τεχνική ανίχνευσης, τη διαδικασία συλλογής δεδομένων και τις μεθόδους ανάλυσης. Περιγράφουμε σε αδρές γραμμές τα υπέρ και τα κατά κάθε τεχνικής ανίχνευσης επιθέσεων, λαμβάνοντας υπόψη και την υπολογιστική τους πολυπλοκότητα.

1 Εισαγωγή

Τα πληροφοριακά συστήματα ενσωματώνονται όλο και περισσότερο στην καθημερινότητά μας. Καθώς αυτή η διαδικασία προχωρά, η ανάγκη για αυξημένα επίπεδα ασφαλείας στα υπόψη δίκτυα, ολοένα και αυξάνεται. Λόγω του χαμηλού κόστους εγκατάστασης και συντήρησης των ασύρματων δικτύων, αυτά χρησιμοποιούνται όλο και περισσότερο για τη σύνδεση αυτών των πληροφοριακών συστημάτων (εφεξής ΠΣ). Η ασφάλιση των συστημάτων αυτών από κάθε επιβολή, καθίσταται απαραίτητη ιδίως σε περιπτώσεις κρίσιμων εφαρμογών.

Κάθε δίκτυο εκτίθεται κατά τη λειτουργία του σε διάφορους κινδύνους, οι οποίοι μπορεί να είναι φυσικοί, τεχνικοί ή να προέρχονται από κακόβουλους χρήστες. Στην τελευταία περίπτωση είναι σύνηθες φαινόμενο η ανίχνευση ανωμαλιών ή ακραίων τιμών στην κίνηση του δικτύου. Θεωρούμε ως ανωμαλία στην δικτυακή κίνηση ένα σύνολο παρατηρήσεων, το οποίο δε δείχνει να συμμορφώνεται με το υπόλοιπο σύνολο των δεδομένων. Αποκλίνουσες συμπεριφορές είναι δυνατό να ταυτοποιηθούν, αναλύοντας συνήθως τις ιδιότητες της κίνησης του δικτύου [14].

Η πρώτη επαφή ενός εισβολέα με οποιοδήποτε δίκτυο είναι τα σημεία εισόδου. Σε αυτά εφαρμόζονται συνήθως μέτρα αποτροπής πρόσβασης (intrusion prevention, IPS). Ένα απλό παράδειγμα είναι ο έλεγχος πρόσβασης με κλειδί, το οποίο εισάγουν οι χρήστες κατά τη διαδικασία αυθεντικοποίησης. Ένα πιο ασφαλές παράδειγμα είναι η εφαρμογή ενός σχήματος αυθεντικοποίησης, που περιλαμβάνει two factor authentication. Οι μέθοδοι αποτροπής πρόσβασης συνήθως αποτυγχάνουν ενάντια σε συγκεκριμένους τύπους απειλών, για παράδειγμα οποιαδήποτε επίθεση προέρχεται από ήδη αυθεντικοποιημένους κόμβους.

Σε αυτές τις περιπτώσεις είναι αποτελεσματικότερη η χρήση μεθόδων ανίχνευσης επιθέσεων (intrusion detection system, IDS). Με τη χρήση μιας τέτοιας μεθόδου είναι δυνατή η ανίχνευση επιτιθέμενων που δεν έγιναν αντιληπτοί από το IPS. Ένας απλός τρόπος για την ανίχνευση εισβολών είναι η εύρεση ασύρματων κόμβων, που εμφανίζουν μη ομαλή συμπεριφορά σε σχέση με τη συνήθως παρατηρούμενη. Η ανίχνευση επιθέσεων είναι ένα πολύ σημαντικό πεδίο έρευνας με πληθώρα εφαρμογών. Τα εργαλεία ανίχνευσης απειλών, σε συνεργασία με τα εργαλεία αποτροπής επιθέσεων και αυτά που παρέχουν την ανταπόκριση και την ανοχή (response and tolerance) δημιουργούν την ασπίδα των ΠΣ ενάντια σε κυβερνοεπιθέσεις, οι οποίες στοχεύουν συστήματα με κρίσιμες λειτουργίες. [9].

Η παρούσα μελέτη εστιάζει στην ανίχνευση απειλών με τη χρήση της μελέτης ανωμαλιών στη δικτυακή κίνηση. Τα κύρια σημεία της μελέτης και η ροή αυτής είναι όπως παρακάτω: Αρχικά, αναλύονται οι διαφορές που παρουσιάζουν τα ασύρματα από τα ενσύρματα δίκτυα και αναλύεται ο σκοπός της παρούσας μελέτης. Στη συνέχεια δίνονται στοιχεία για την έρευνα που έχει γίνει πάνω στο πεδίο της ανίχνευσης επιθέσεων σε ασύρματα δίκτυα, αναφέρονται οι κύριοι κίνδυνοι - απειλές που αντιμετωπίζουν τα ασύρματα δίκτυα και πραγματοποιείται ανάλυση και ταξινόμηση των τεχνικών ανίχνευσης επιθέσεων στη βιβλιογραφία, με βάση τον τύπο τους αλγόριθμους ανίχνευσης. Τέλος, παρουσιάζονται τα συμπεράσματα της παρούσας μελέτης.

2 Κίνητρο και Υπόβαθρο

2.1 Εισαγωγή

Τα ασύρματα δίκτυα παρουσιάζουν αρκετές ιδιαιτερότητες σε σχέση με τα ενσύρματα, οι οποίες θέτουν προβλήματα τόσο στην παρακολούθηση της υγείας του δικτύου, τόσο και στην εφαρμογή μέτρων για την ασφάλισή του. Στα ενσύρματα δίκτυα είναι δυνατή η προστασία του δικτύου με απομόνωση του φυσικού μέσου (physical partitioning) ή περιορισμό της συνδεσιμότητας μεταξύ υπο-δικτύων. Στα ασύρματα δίκτυα αυτό δεν είναι δυνατό καθώς όλοι οι κόμβοι μοιράζονται το ίδιο φυσικό μέσο, ενώ η θέση τους είναι συνεχώς μεταβαλλόμενη.

Στα ασύρματα δίκτυα λόγω της συνεχούς κινητικότητας των κόμβων, δεν είναι δυνατός ο συντονισμός τους, ο οποίος είναι απαραίτητος για την ορθή λειτουργία των συστημάτων IDS. Για τον ίδιο λόγο δεν είναι δυνατή η συλλογή δεδομένων για μεγάλο χρονικό διάστημα σε συγκεκριμένο φυσικό χώρο (περιοχή κάλυψης). Αυτό σημαίνει ότι ένας μοναδικός κόμβος δεν είναι δυνατό να συλλέξει ένα αρκετά μεγάλο δείγμα δεδομένων για να διαγνώσει με ακρίβεια την ορθή λειτουργία των υπόλοιπων κόμβων του δικτύου [13]. Η διαδικασία ανίχνευσης περιπλέκεται περισσότερο, αν σκεφθεί κανείς ότι ένας ασύρματος κόμβος έχει τη δυνατότητα παρακολούθησης και συλλογής δεδομένων μόνο μέσα στο χώρο κάλυψης του.

Τα συμβατικά IDS χρησιμοποιούν τα ενεργά στοιχεία του δικτύου (routers, switches, gateways) για να ελέγξουν τη δικτυακή κίνηση. Αυτός ο εξοπλισμός συνήθως δεν είναι διαθέσιμος στο πεδίο, στους χώρους στους οποίους είναι ανεπτυγμένο ένα ασύρματο δίκτυο. Αυτό σημαίνει ότι είναι δύσκολη η ενοποιημένη συλλογή και επεξεργασία δεδομένων κίνησης για ολόκληρο το δίκτυο σε εύλογο χρονικό διάστημα. Επίσης, θα πρέπει να σημειωθεί ότι τα δεδομένα που συλλέγονται από γειτονικούς κόμβους ενός ασύρματου δικτύου αναμένεται να παρουσιάζουν υψηλή συσχέτιση, καθώς και τα υπό-παρατήρηση αντικείμενα στο φυσικό κόσμο είναι συσχετιζόμενα [4].

Στα ασύρματα δίκτυα κακόβουλοι κόμβοι - πελάτες μπορούν να εισέρχονται και να εξέρχονται από την περιοχή κάλυψης του δικτύου σε τυχαίες χρονικές στιγμές ή μπορεί να συνεργάζονται με άλλους κακόβουλους κόμβους, με σκοπό τη δημιουργία προσκομμάτων στη δικτυακή κίνηση ή την προστασία από εντοπισμό τους. Επίσης, οι κόμβοι μπορεί να λειτουργούν κακόβουλα μόνο για μικρό χρονικό διάστημα και να επανέρχονται σε φυσιολογική λειτουργία αργότερα, στην οποία θα παραμένουν για τυχαίο χρόνο. Θα πρέπει να σημειωθεί, ότι αντίθετα με τα ενσύρματα δίκτυα, ένας επιτιθέμενος δε χρειάζεται να έχει πρόσβαση στο φυσικό μέσο για να εκδηλώσει την επίθεσή του, καθώς του αρκεί να εκπέμψει ένα δυνατό παρεμβάλον σήμα για να απαγορεύσει τη χρήση του φάσματος στους κανονικούς χρήστες του δικτύου [12].

Στα ασύρματα δίκτυα πολλά πακέτα απορρίπτονται ή εμφανίζονται ετεροχρονισμένα λόγω σφαλμάτων εκπομπης ή παρεμβολών κ.τ.λ, και είναι δυνατό να εμφανίζονται ως κακόβουλη συμπεριφορά. Επίσης, τα ασύρματα δίκτυα επηρεάζονται από τη μορφολογία του εδάφους, τις ατμοσφαιρικές συνθήκες (θερμοκρασία και υγρασία), καθώς και από την ανθρώπινη δραστηριότητα (κατασκευές, θορυβώδες αστικό περιβάλλον). Για αυτούς τους λόγους οι παραδοσιακές μέθοδοι ανίχνευσης επιθέσεων δεν βρίσκουν ευθεία εφαρμογή στα ασύρματα δίκτυα [13]. Όλα τα παραπάνω δυσχεραίνουν τον εντοπισμό κακόβουλων κόμβων και την λήψη αντιμέτρων για την αντιμετώπισή τους.

Τέλος, τα ασύρματα δίκτυα φέρουν εκτός του ωφέλιμου φορτίου και μεγάλο φορτίο

metadata, όπως πληροφορίες για την ισχύ του σήματος και το λόγο ισχύος προς θόρυβο. Το γεγονός αυτό έχει δυο επιπτώσεις: κατά πρώτον η λειτουργία παρακολούθησης της δικτυακής κίνησης θα πρέπει να περιλαμβάνει, δυνατότητες προσανατολισμένες στην ιδιαιτερότητα των ασύρματων δικτύων, ενώ θα πρέπει να προβλεφθεί και η τοποθέτηση των σταθερών κόμβων του δικτύου (κόμβοι εξυπηρετητές - base stations) σε κατάλληλη γεωμετρική διάταξη. Κατά δεύτερο η τεχνική ανίχνευσης επιθέσεων θα πρέπει να είναι σε θέση να λειτουργεί με δεδομένα, τα οποία είναι ελλιπή είτε λόγω σφαλμάτων μετάδοσης, είτε λόγω φυσικού διαχωρισμού των κόμβων (εμπόδια κ.α) [12].

Οι σημαντικές διαφοροποιήσεις μεταξύ των δύο παραπάνω τύπων δικτύων, υποδεικνύουν την ανάγκη αντιμετώπισης των ιδιαιτεροτήτων, που παρουσιάζονται στην ανίχνευση και αντιμετώπιση επιθέσεων στα ασύρματα δίκτυα. Σκοπός μας είναι η μελέτη των μεθόδων ανίχνευσης επιθέσεων σε ασύρματα δίκτυα, με ανάλυση της δικτυακής κίνησης για την εύρεση ανωμαλιών, που υποδεικνύουν κακόβουλη συμπεριφορά.

2.2 Υπάρχουσα Έρευνα

Προσφάτως έχει γίνει πολλή έρευνα πάνω στην ανίχνευση επιθέσεων στα ασύρματα δίκτυα, αλλά μπορεί να θεωρηθεί ότι βρίσκεται ακόμα σε πρώιμα στάδια [5]. Η περισσότερη προσπάθεια έχει σημειωθεί σε περιοχές όπως η ασφαλής δρομολόγηση, η διαχείριση κλειδιών και καταπιστευμάτων, η προστασία της διαθεσιμότητας των υπηρεσιών και η ανίχνευση επιθέσεων (Intrusion Detection, IDS). Στις περισσότερες μελέτες η ανίχνευση επιθέσεων εμφανίζεται ως συμπληρωματικός μηχανισμός, όταν όλοι οι μηχανισμοί αποτροπής επιθέσεων (IPS) αποτυγχάνουν να κρατήσουν τους εισβολείς εκτός του δικτύου.

Στο [13] δίνεται ένας τρόπος ασφάλισης της δικτυακής πρόσβασης, με τη χρήση τροποποιημένων κεφαλίδων για τη δημιουργία σχέσεων εμπιστοσύνης μεταξύ των κόμβων (Statistically Unique and Cryptographically Verifiable (SUCV) identifiers). Στο μέρος που αφορά την υλοποίηση των μεθόδων IDS, στηρίζεται στη χρήση τοπικών IDS agents σε κάθε κόμβο.

Στο [5] οι επιθέσεις ανιχνεύονται με την αντιπαραβολή της δικτυακής κίνησης με ένα καθολικά αποδεκτό μοντέλο, το οποίο αντιπροσωπεύει την συνήθη μη-κακόβουλη κίνηση. Η μέθοδος αυτή αποφεύγει την εξάρτηση από την τήρηση και ενημέρωση υπογραφών για κακόβουλη κίνηση (signature-based IDS). Παρόμοια μέθοδος παρουσιάζεται και στο [4] με την αναγνώριση επιθέσεων να χωρίζεται σε δυο φάσεις:

- offline ανάλυση. Περιλαμβάνει τη δημιουργία του μοντέλου δεδομένων για την συνήθη αναμενόμενη κίνηση και για τις υπό αξιολόγηση παραμέτρους.
- real time ανάλυση, κατά την οποία ανιχνεύονται ανωμαλίες στη δικτυακή κίνηση μέσω σύγκρισης της παρούσας κίνησης με το ήδη υπάρχον μοντέλο.

Μια διαφορετική προσέγγιση παρουσιάζεται στο [10], η οποία χρησιμοποιεί επιπλέον και χαρακτηριστικά του σήματος και της διάδοσής του (signal path loss - signal power), ενώ με μεθόδους μηχανικής μάθησης (machine learning) εντοπίζει μη εξουσιοδοτημένη χρήση του ηλεκτρομαγνητικού φάσματος. Παρόμοια προσέγγιση παρουσιάζεται στο [9], όπου χρησιμοποιούνται δέντρα απόφασης για την ανάλυση των δεδομένων και την ανίχνευση εισβολών. Η ανίχνευση της μη εξουσιοδοτημένης χρήσης του φάσματος πραγματοποιείται υπό τις παρακάτω προϋποθέσεις:

- Η ισχύς εκπομπής ενός κόμβου είναι μεγαλύτερη από ένα επιτρεπτό κατώφλι. Το γεγονός αυτό δημιουργεί παρεμβολές στους γειτονικούς κόμβους.

- Ένας κόμβος χρησιμοποιεί ένα τμήμα του φάσματος, το οποίο υποτίθεται ότι θα έπρεπε να είναι σε κατάσταση ηρεμίας. Σε αυτή την περίπτωση ο κόμβος αυτός θεωρείται κακόβουλος.

- Ένας πομπός χρησιμοποιεί ένα τμήμα του φάσματος, το οποίο φυσιολογικά έχει αποδοθεί σε ένα άλλο κόμβο.

Όλα τα παραπάνω ισχύουν με την παραδοχή ότι χρήστες σε γειτονικές ζώνες χρησιμοποιούν διαφορετικές συχνότητες στον ίδιο χρόνο, με τρόπο ώστε να μην υπάρχουν παρεμβολές μεταξύ τομέων αλληλοκάλυψης.

Η μέθοδος των [1] και [11] χρησιμοποιεί έτοιμα audit data, για την ανίχνευση εισβολέων και τον αποτελεσματικό αποκλεισμό τους από τους πόρους του δικτύου. Στη συγκεκριμένη πρόταση δεν υπάρχει κάποιο κεντρικό σύστημα ελέγχου της κίνησης, αλλά η ανάλυση και ταυτοποίηση των εισβολέων γίνεται σε κάθε κόμβο ξεχωριστά και σε συνεργασία με τους γειτονικούς κόμβους. Παρόμοια πρόταση αποτελούν και τα [17] - [2], στα οποία χρησιμοποιούνται και στατιστικές μέθοδοι, οι οποίες λαμβάνουν υπόψη τη συσχέτιση των συλλεγόμενων δεδομένων.

Τέλος, στο [16] παρουσιάζεται μια πρόταση η οποία χρησιμοποιεί Bayesian models για την μοντελοποίηση της ροής των δεδομένων σε αποδεκτές συμπεριφορές. Σε δεύτερο χρόνο πραγματοποιείται ανάλυση σε ένα μειωμένο υποσύνολο των δεδομένων, τα οποία προέρχονται από κόμβους οι οποίοι έχουν χαρακτηριστεί ως δυνητικά κακόβουλοι από την ανάλυση πρώτου σταδίου. Σε αυτό το στάδιο χρησιμοποιείται και ανάλυση με μαρκοβιανές αλυσίδες για την αναγνώριση εποχικότητας ή άλλων τάσεων στη ροή των δεδομένων.

Στο επόμενο τμήμα παρουσιάζονται αναλυτικά οι τύποι των ασύρματων δικτύων και οι κύριες απειλές που συναντώνται στη βιβλιογραφία.

3 Απειλές σε Ασύρματα Δίκτυα

3.1 Τύποι Ασύρματων Δικτύων

Μπορούμε να κατηγοριοποιήσουμε τα ασύρματα δίκτυα που συναντούμε συχνότερα με βάση το σκοπό τον οποίο εξυπηρετούν όπως παρακάτω:

- Wireless local area networks - Τα δίκτυα WLAN χρησιμοποιούν πρωτόκολλα IEEE 802.11 για τη δικτύωση των κόμβων μέχρι 250 μέτρα.
- Wireless personal area networks - Τα δίκτυα WPAN χρησιμοποιούν το ηλεκτρομαγνητικό φάσμα για τη διασύνδεση μικρού αριθμού ιδιωτικών κόμβων, οι οποίοι βρίσκονται σε απόσταση μέχρι 10 μέτρα.
- Wireless sensor networks - Τα δίκτυα WSN είναι ασύρματοι κόμβοι ειδικού σκοπού, οι οποίοι τοποθετούνται στο χώρο με αρχιτεκτονικές διαφορετικού εύρους. Για παράδειγμα, μπορεί να υπάρχουν πολλοί περιφερειακοί κόμβοι και λίγοι σταθμοί βάσης ή σχετικά μικρός αριθμός περιφερειακών κόμβων γύρω από ένα μοναδικό σταθμό βάσης.
- Ad hoc networks - Τα υπόψη δίκτυα υλοποιούν συνδέσεις μεταξύ κόμβων χωρίς να υπάρχει κάποιος κεντρικός σταθμός - συντονιστής του δικτύου. Περιλαμβάνουν τα Metropolitan Ad hoc Networks, MANETs και τα Vehicular Ad hoc Networks, VANETs.
- Mobile telephony - Τα δίκτυα κινητής τηλεφωνίας αποτελούνται από μεγάλο αριθμό φορητών συσκευών και μερικούς σταθμούς βάσης.
- Wireless mesh networks - Τα δίκτυα WMN παρουσιάζουν υψηλό αριθμό συνδεσιμότητας μεταξύ των κόμβων (ειδικού σκοπού) και αυτή τους η ιδιότητα του προσδίδει την δυνατότητα της αυτοΐασης.
- Cyber physical systems - Τα δίκτυα CPS έχουν αυστηρούς περιορισμούς χρονισμού, προβλέψιμη δικτυακή κίνηση και είναι συνήθως κατασκευασμένα από εξαρτήματα παλαιότερης τεχνολογίας [12].

3.2 Ταξινόμηση Απειλών

Οι απειλές που αντιμετωπίζουν δυνητικά τα ασύρματα δίκτυα είναι σημαντικά διαφοροποιημένες σε σχέση με τις αντίστοιχες των ενσύρματων, κυρίως λόγω των διαφορών που εκτέθηκαν παραπάνω. Οι σημαντικότερες κατηγορίες επιθέσεων αναλύονται παρακάτω:

Επιθέσεις εναντίον περιοχής (ενάντια σε ένα ή μικρό αριθμό γειτονικών κόμβων) Υπάρχουν κυρίως τέσσερις τύποι επιθέσεων αυτής της κατηγορίας [6].

- Επιβολή σιωπής - Ένας κόμβος που έχει δεχθεί επίθεση τηρεί σιγή και δεν εξυπηρετεί (silencing).
- Παραποίηση ταυτότητας - Ένας κόμβος υποδύεται ότι είναι ένας άλλος, ο οποίος είναι πραγματικά μέλος του δικτύου (spoofing).

- Πολλαπλή παραποίηση ταυτότητας - Ένας κόμβος εκπέμπει πολλαπλά πακέτα, τα οποία φαίνεται να προέρχονται από πολλές διαφορετικές πηγές (sybil attack).

- Αλλαγή της περιοχής κάλυψης ενός κόμβου - Ένας κόμβος ο οποίος έχει δεχθεί επίθεση, εκπέμπει με μεγαλύτερη ισχύ καλύπτοντας τους γείτονές του ή δημιουργώντας παρεμβολές (jamming).

Επιθέσεις ενάντια σε κόμβο

- Επιθέσεις που έχουν στόχο είτε να καταστρέψουν τον κόμβο είτε να τον κάνουν να λειτουργεί με διαφορετικό τρόπο (tampering).

- Φυσική κατάληψη ενός κόμβου με απώτερο σκοπό την εξαγωγή κλειδιών κρυπτογράφησης, για την παθητική παρακολούθηση της κίνησης ή παράκαμψη συστημάτων αποτροπής πρόσβασης, με εισαγωγή κακόβουλων κόμβων στο δίκτυο (node capture attack).

Επιθέσεις αλλοίωσης της δικτυακής κίνησης Αυτού του τύπου οι επιθέσεις μπορούν να κατηγοριοποιηθούν περαιτέρω στις υπόψη κατηγορίες:

- Αλλοίωση των πινάκων δρομολόγησης με σκοπό την ανακατεύθυνση των πακέτων σε συγκεκριμένους κόμβους (sinkhole attack)

- Δημιουργία δικτυακής κίνησης με μέγεθος τέτοιο ώστε να παρεμποδίζεται ή να καθίσταται αδύνατη η εξυπηρέτηση της δικτυακής κίνησης (Denial of service).

- Απόρριψη όλων ή κάποιων από τα πακέτα που διέρχονται από ένα κόμβο, ο οποίος έχει καταληφθεί από τον επιτιθέμενο (selective forwarding).

- Διοχέτευση ή αναδρομολόγηση δικτυακής κίνησης μέσω της δημιουργίας ενός διαδρόμου μεταξύ δυο κόμβων (wormholes).

- Εκπομπή παραποιημένων πακέτων route reply σε ένα κόμβο πηγή. Ένας κόμβος που έχει καταληφθεί από κάποιο επιτιθέμενο, ακούει στο δίκτυο για πακέτα route request και απαντά με παραποιημένα πακέτα route reply, τα οποία καταδεικνύουν ως τη μικρότερη σε μήκος διαδρομή αυτή που διέρχεται μέσω του κακόβουλου κόμβου. Με αυτό τον τρόπο επιτυγχάνεται τελικώς η δρομολόγηση όλων των πακέτων μέσω του κακόβουλου κόμβου, ο οποίος είναι ρυθμισμένος να τα απορρίπτει. Το παραπάνω έχει ως αποτέλεσμα την παράλυση του δικτύου (blackhole attack).

- Παρόμοια επίθεση με την παραπάνω είναι η πλημμυρίδα του δικτύου με λανθασμένα πακέτα δρομολόγησης, με τα ίδια αποτελέσματα (routing request flooding attack).

- Πιο στοχευμένη επίθεση, η οποία χρησιμοποιεί την ίδια αρχή αλλά αλλοιώνει τα πακέτα route reply μεταξύ συγκεκριμένων κόμβων εκκίνησης και προορισμού (routing request disrupt attack).

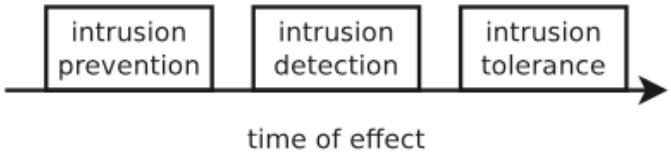
- Παθητική παρακολούθηση και υποκλοπή της δικτυακής κίνησης (eavesdropping).

Στο επόμενο τμήμα περιγράφονται οι αρχές της ανίχνευσης επιθέσεων και αναλύεται η μέθοδος ανίχνευσης με βάση τις ανωμαλίες στη δικτυακή κίνηση.

4 Ανίχνευση Εισβολών με Ανάλυση της Κίνησης

4.1 Εισαγωγή

Είναι γενικά χρήσιμο κατά την ανάλυση της δικτυακής κίνησης, να θεωρούμε τα μέτρα προστασίας ενός δικτύου στο πεδίο του χρόνου. Ένα μέτρο αποτροπής πρόσβασης (IPS) σταματά τον επιτιθέμενο στην είσοδο του δικτύου. Αμέσως μετά ακολουθεί η ανίχνευση των εισβολέων, οι οποίοι τυχόν έχουν περάσει από το πρώτο επίπεδο. Θα πρέπει να σημειωθεί, ότι ένα IPS δεν είναι πάντα αποτελεσματικό ενάντια σε όλα τα είδη επιθέσεων, για παράδειγμα eavesdropping. Σε αυτή την περίπτωση το δίκτυο θα πρέπει να είναι σε θέση να αντέξει τις επιπτώσεις της επίθεσης χωρίς να επηρεαστεί η λειτουργικότητά του (tolerance). Αυτό συνήθως επιτυγχάνεται με διατάξεις load-balancing ή failover. Το σχήμα 4.1 παρουσιάζει την χρονική ακολουθία των μέτρων προστασίας ενός δικτύου.



Σχήμα 4.1: Χρονική ακολουθία των μέτρων προστασίας

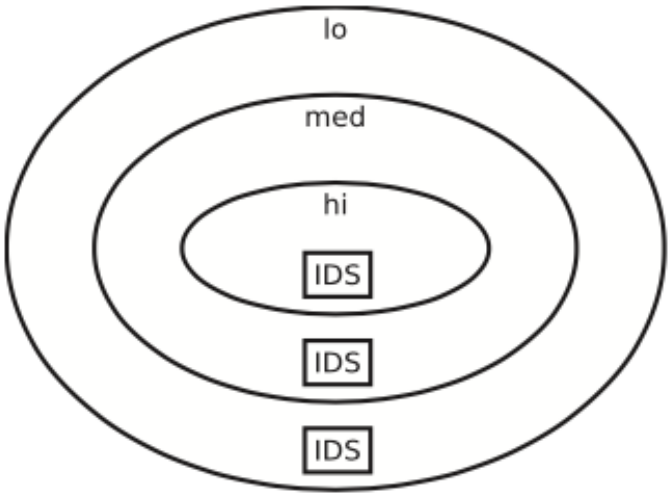
4.2 Οργάνωση Ζωνών Ασφαλείας

Στη βιβλιογραφία συναντούμε συνήθως αναφορές για οργάνωση της άμυνας του δικτύου σε ζώνες και κατά βάθος. Κάθε ζώνη προστατεύεται από δικό της firewall και IDS. Οι ζώνες οργανώνονται με τέτοιο τρόπο, ώστε να αυξάνεται το επίπεδο διαβάθμισης - ασφαλείας καθώς προχωρούμε προς το εσωτερικό. Το σχήμα 4.2 παρουσιάζει αυτό τον τρόπο οργάνωσης.

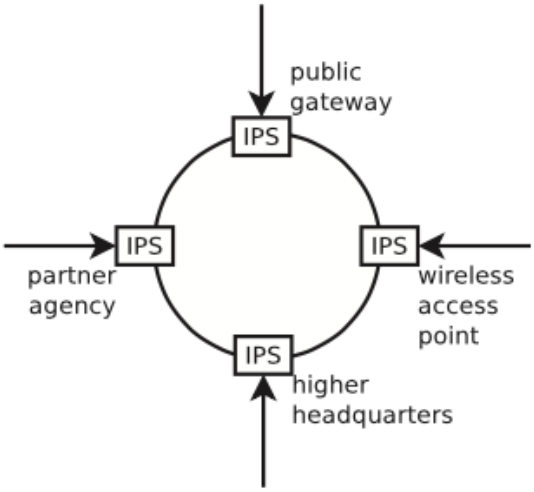
Στα ασύρματα δίκτυα, επειδή δεν υπάρχει σαφώς καθορισμένο σημείο εισόδου, κάθε κόμβος δυνητικά μπορεί να παίξει αυτό το ρόλο. Αυτό συμβαίνει γιατί οι ασύρματοι κόμβοι (base station - infrastructure node) είναι διεσπαρμένοι γεωγραφικά, καλύπτοντας εκτεταμένες περιοχές, ενώ είναι δυνατό να συνδέονται με τις σταθερές υποδομές με διάφορους τρόπους ή να λειτουργούν σε διαφορετικό επίπεδο ασφαλείας από ότι οι υπόλοιποι. Σε αυτή την περίπτωση η κλιμάκωση κατά βάθος θα πρέπει να ενσωματώνει και την περιμετρική άμυνα, με την έννοια ότι συστήματα ασφαλείας πρέπει να τοποθετούνται σε όλα τα περιφερειακά σημεία εισόδου - access points, στα intranet links επικοινωνίας με συνεργάτες κ.τ.λ. Το σχήμα 4.3 περιγράφει την έννοια της περιμετρικής άμυνας.

4.3 Μετρικές Αποτελεσματικότητας Ανίχνευσης Επιθέσεων

Γενικά μπορούμε να διακρίνουμε τις εργασίες που εκτελεί ένα IPS σε δύο κατηγορίες:



Σχήμα 4.2: Οργάνωση ζωνών ασφαλείας σε βάθος



Σχήμα 4.3: Οργάνωση περιμετρικής άμυνας

- Συλλογή δεδομένων δικτυακής κίνησης, που αφορούν σε ύποπτες ενέργειες. Παραδείγματα τέτοιων δεδομένων είναι η καταγραφή συμβάντων συστήματος που αφορούν τον κόμβο, καταγραφή δικτυακής κίνησης αλλά και μηνύματα άλλων κόμβων που ενημερώνουν για ύποπτους χρήστες (reputation scores).

- Ανάλυση δεδομένων που έχουν περισυλλεγεί, με τη χρήση στατιστικών μεθόδων, pattern matching και μεθόδων εξόρυξης δεδομένων.

Οι μελετητές των συστημάτων IPS χρησιμοποιούν τρεις κυρίως μετρικές για να αποφανθούν για την αποτελεσματικότητα ενός συστήμστος: false positive rate (FPR), false negative rate (FNR), και detection rate (DR) [12]. Ένα FPR καταγράφεται όταν ένα IDS καταδεικνύει ένα κόμβο με φυσιολογική κίνηση, ως κακόβουλο. Αντίστοιχα FNR καταγράφεται, όταν ένας κόμβος με κακή συμπεριφορά δεν ανιχνεύεται ως κακόβουλος. Το ποσοστό ανίχνευσης DR είναι συνώνυμο με την ευαισθησία του συστήματος ανίχνευσης επιθέσεων και υπολογίζεται από τη σχέση:

$$DR = 1 - FPR - FNR$$

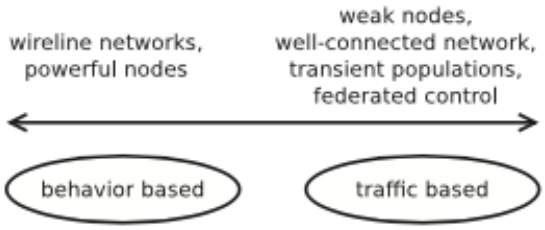
Άλλες μετρικές έχουν κατά καιρούς προταθεί, όπως το detection latency (DL), ενώ για

κινούμενους κόμβους με μικρή επεξεργαστική ισχύ, παίζει ρόλο η κατανάλωση ισχύος, η επιρροή στην ταχύτητα μεταγωγής δεδομένων και ο επεξεργαστικός φόρτος.

4.4 Συλλογή και Ανάλυση Δεδομένων

4.4.1 Συλλογή Δεδομένων

Για να είναι σε θέση ένα IDS να ανιχνεύσει επιθέσεις σε ένα δίκτυο, χρησιμοποιεί διάφορες μεθόδους συλλογής και ανάλυσης των δεδομένων. Κατά την φάση της συλλογής των δεδομένων ένα IDS είναι δυνατό να εξάγει αυτά, είτε από την δικτυακή κίνηση (traffic based collection), είτε από την εξέταση των αρχείων καταγραφής συμβάντων (behavior based collection). Το σχήμα 4.4 δείχνει τα χαρακτηριστικά των μεθόδων συλλογής.



Σχήμα 4.4: Διαδικασία συλλογής δεδομένων

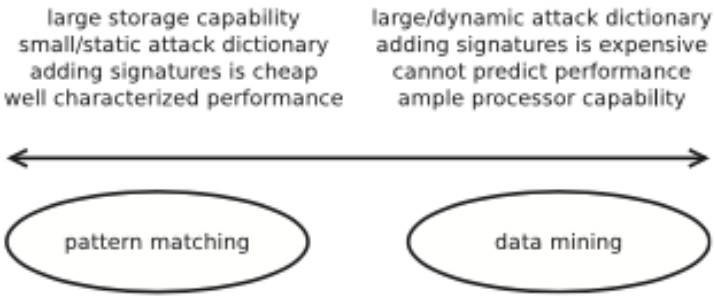
Η συλλογή δεδομένων που βασίζεται στη δικτυακή κίνηση προσφέρεται περισσότερο για εφαρμογή σε ασύρματα δίκτυα, καθώς οι κόμβοι είναι μετακινούμενοι με μικρούς αποθηκευτικούς χώρους, γεγονός το οποίο καθιστά την αποθήκευση αρχείων καταγραφών δύσκολη. Από την άλλη πλευρά είναι δυνατό να χρησιμοποιηθούν μέθοδοι καταγραφής συμβάντων σε δίκτυα κινητής τηλεφωνίας, όπου οι σταθμοί βάσης έχουν ενσύρματες συνδέσεις με ισχυρές υπολογιστικά και αποθηκευτικά υποδομές.

4.4.2 Ανάλυση Δεδομένων

Κατά την φάση της ανάλυσης χρησιμοποιούνται εξειδικευμένες μέθοδοι για την ανάλυση των δεδομένων, τα οποία συλλέχθηκαν στο προηγούμενο στάδιο. Οι συνήθεις μέθοδοι που συναντώνται, είναι δυνατό να διακριθούν σε δυο κύριες κατηγορίες. Μέθοδοι εξόρυξης δεδομένων (data mining) και σύγκρισης μοτίβων (pattern matching). Στην πρώτη περίπτωση συμπεριλαμβάνονται κυρίως τα IDS που χρησιμοποιούν τεχνικές anomaly detection. Στη δεύτερη περίπτωση ελέγχεται η δικτυακή κίνηση ανά κόμβο με τη χρήση υπογραφών (signature based) ή γνωστών attack dictionaries. Άλλα μέτρα σύγκρισης μπορεί να περιλαμβάνουν την παρατήρηση απόκλισης της απόδοσης ενός κόμβου από γνωστές αναμενόμενες τιμές [12].

Μια μέθοδος ανάλυσης είναι δυνατό να περιλαμβάνει τεχνικές και από τις δυο προαναφερθέντες περιοχές, ως συνδυασμό. Σε αυτή την περίπτωση είναι δυνατό να τεθούν σε εφαρμογή τεχνικές μηχανικής μάθησης, γενετικού προγραμματισμού, νευρωνικών δικτύων και Bayesian κατηγοριοποιήσεων. Στο σχήμα 4.5 παρίστανται τα χαρακτηριστικά των μεθόδων ανάλυσης.

Γενικότερα, ασύρματοι κόμβοι με μικρή επεξεργαστική ισχύ και ένα στατικό μοντέλο αναμενόμενων επιθέσεων, τείνουν προς τη χρήση τεχνικών pattern matching, ενώ ισχυροί υπολογιστικά κόμβοι μπορούν να χρησιμοποιήσουν τεχνικές data mining για να αντιμετωπίσουν ένα δυναμικό αντίπαλο [12].



Σχήμα 4.5: Διαδικασία ανάλυσης δεδομένων

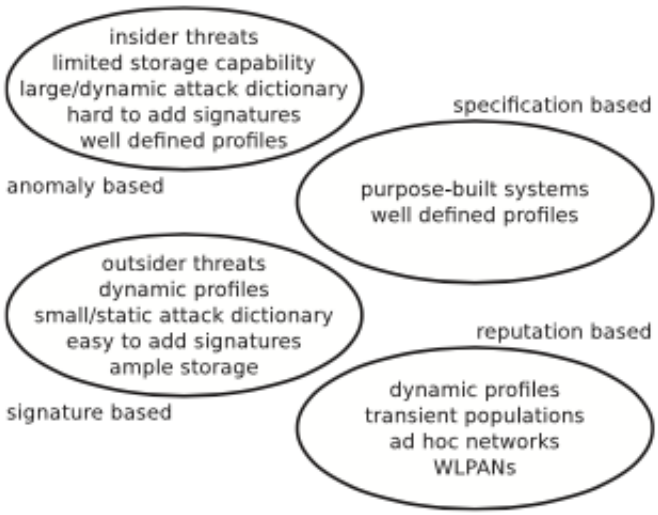
4.5 Ανίχνευση Επιθέσεων

4.5.1 Εισαγωγή

Στη βιβλιογραφία έχουν προταθεί διάφορες μέθοδοι για την ανίχνευση επιθέσεων. Οι κυριότερες που συνήθως συναντώνται είναι όπως παρακάτω:

- Βασισμένες σε ανωμαλίες στη δικτυακή κίνηση (anomaly based) - Εξετάζουν τη δικτυακή κίνηση με συγκεκριμένες μετρικές και με βάση καθορισμένο μοντέλο της φυσιολογικής κίνησης.
- Βασισμένες σε προδιαγραφές συστήματος (specification based) - Αναζητούν μη φυσιολογικές τιμές στην απόδοση του συστήματος.
- Βασισμένες σε αξιολόγηση (reputation based management) - Ανιχνεύουν κόμβους που εμφανίζουν εγωιστική και όχι απαραίτητα κακόβουλη συμπεριφορά.
- Βασισμένες σε υπογραφές επιθέσεων (signature based) - συγκρίνουν τη δικτυακή κίνηση με συγκεκριμένα γνωστά μοτίβα ή συμπεριφορές.

Στο σχήμα 4.6 εμφανίζονται επιγραμματικά οι τεχνικές ανίχνευσης επιθέσεων.



Σχήμα 4.6: Τεχνικές ανίχνευσης επιθέσεων

4.5.2 Anomaly Based Ανίχνευση Επιθέσεων

4.5.2.1 Εισαγωγή

Έχουν κατά καιρούς προταθεί στη βιβλιογραφία διάφορες μέθοδοι για αυτού του τύπου την ανίχνευση. Ένα από τα θέματα που αντιμετωπίζουν συνήθως οι μελετητές του πεδίου αυτού, είναι ο καθορισμός της έννοιας της κανονικότητας στη δικτυακή κίνηση.

Τα κύρια προβλήματα που μπορεί να συναντήσει ένας μελετητής αυτού του τύπου ανίχνευσης επιθέσεων είναι [3]:

- Ο σαφής ορισμός μιας περιοχής ομαλής λειτουργίας, όπως προαναφέρθηκε, είναι μια αρκετά δύσκολη εργασία. Επιπρόσθετα τα όρια φυσιολογικής και μη, δικτυακής συμπεριφοράς είναι συχνά δυσδιάκριτα. Για αυτό το λόγο μια ύποπτη συμπεριφορά, η οποία κινείται κοντά στα όρια, μπορεί στην πραγματικότητα να είναι φυσιολογική και το αντίστροφο.

- Όταν η μη φυσιολογική κίνηση προκαλείται από κακόβουλους χρήστες, συχνά αυτοί προσαρμόζουν τη συμπεριφορά τους, ώστε οι μη φυσιολογικές παρατηρήσεις να εμφανίζονται εντός ορίων.

- Σε πολλές περιπτώσεις η έννοια της κανονικότητας αναπροσαρμόζεται συνεχώς, μαζί με την εξέλιξη και τις δυνατότητες της τεχνολογίας και έτσι παρατηρήσεις που θεωρούνται σήμερα μη φυσιολογικές μπορεί μελλοντικά να είναι αποδεκτές και το αντίστροφο.

- Η διαθεσιμότητα έτοιμων δεδομένων εκπαίδευσης είναι συνήθως δύσκολο πρόβλημα. Επίσης, τα τυχόν υπάρχοντα δεδομένα καθίστανται ταχέως παρωχημένα, καθώς τα όρια της αποδεκτής συμπεριφοράς αναπροσαρμόζονται, όπως αναφέρθηκε παραπάνω.

- Πολύ συχνά τα συλλεγόμενα δεδομένα περιέχουν θόρυβο, ο οποίος παρομοιάζει με μη φυσιολογική κίνηση και έτσι είναι δύσκολος ο διαχωρισμός και η αφαίρεσή του.

Οι μελετητές χρησιμοποιούν διαφορετικές προσεγγίσεις για διακριτά, συνεχή και πολυμεταβλητά σύνολα δεδομένων εκπαίδευσης (training datasets). Παραδείγματα διακριτών συνόλων είναι αριθμοί κλήσης ή καταστάσεις ενός συστήματος. Σε αυτά τα σύνολα μπορούν να εφαρμοστούν τεχνικές αναγνώρισης βασισμένες σε Longest Common Subsequence (LCS) για ένα πεπερασμένο χρονικό διάστημα ή απευθείας εφαρμογή αποστάσεων Hamming [12].

Σχετικά παραδείγματα συνεχών datasets είναι η θέση ενός κόμβου ή η ταχύτητα μεταγωγής πακέτων. Σε αυτή την περίπτωση η ανίχνευση είναι αποτελεσματική μόνο με διαστήματα εμπιστοσύνης και όχι με ακριβείς τιμές.

Datasets με πολυμεταβλητά δεδομένα μπορούν να είναι μια πλειάδα δεδομένων (θέση, χρόνος, ισχύς σήματος). Σε αυτού του είδους τα δεδομένα μπορούν να εφαρμοσθούν τεχνικές ανίχνευσης, οι οποίες στηρίζονται σε προσεγγίσεις μηχανικής μάθησης (γενετικοί αλγόριθμοι, νευρωνικά δίκτυα, κατηγοριοποιητές Bayes).

4.5.2.2 Κύριοι Τύποι Ανωμαλιών Δικτυακής Κίνησης

Μια σημαντική διάσταση των τεχνικών ανίχνευσης anomaly based, είναι η φύση της μη-ομαλότητας. Οι παρατηρούμενες ανωμαλίες μπορούν να διακριθούν στις ακόλουθες κατηγορίες.

- Σημειακές αποκλίσεις (point anomalies) - Αν ένα στιγμιότυπο δεδομένων παρουσιάζει σημαντική διαφοροποίηση από το υπόλοιπο σύνολο των δεδομένων. Είναι ο πιο

κοινός τύπος παρουσιαζόμενης απόκλισης και μελετάται περισσότερο στη βιβλιογραφία.

- Υπό συνθήκη (context anomalies) - Αν ένα στιγμιότυπο δεδομένων θεωρείται εκτός ορίων εξεταζόμενο υπό συγκεκριμένες συνθήκες και όχι σε άλλες περιπτώσεις. Η κρίση εξαρτάται σε αυτή την περίπτωση από τη δομή του συνόλου των δεδομένων και καθορίζεται κατά την διατύπωση του υπό εξέταση προβλήματος. Τέτοιου είδους αποκλίσεις μελετώνται συνήθως σε προβλήματα χρονοσειρών [3].

- Συλλεκτικές (collective anomalies) - Αν ένα υποσύνολο συσχετιζόμενων δεδομένων παρουσιάζεται ως μη φυσιολογικό σε σχέση με το υπόλοιπο σύνολο. Τα στοιχεία του υποσυνόλου μπορεί να μη θεωρούνται ως αποκλίνοντα, εάν εξετασθούν ξεχωριστά αλλά όταν εμφανίζονται μαζί ταυτόχρονα σε ένα στιγμιότυπο δεδομένων.

4.5.2.3 Τρόποι Λειτουργίας Anomaly Based Τεχνικών

Οι τεχνικές ανίχνευσης μπορούν να κατηγοριοποιηθούν με βάση τον τύπο των δεδομένων εκπαίδευσής, σε τρεις μεγάλες κατηγορίες.

Supervised Methods Αυτού του είδους οι τεχνικές θεωρούν την ύπαρξη κατηγοριοποιημένων δεδομένων εκπαίδευσης τόσο για τις φυσιολογικές όσο και για τις αποκλίνουσες περιπτώσεις [3]. Η τυπική προσέγγιση είναι η δημιουργία ενός μοντέλου πρόβλεψης και για τις δύο κατηγορίες και η σύγκριση των στιγμιοτύπων δεδομένων με το μοντέλο, έτσι ώστε να αποφασιστεί σε ποια από τις δυο ανήκει.

Η συγκεκριμένη τεχνική παρουσιάζει δυο μεγάλα προβλήματα. Κατά πρώτον τα αποκλίνοντα στιγμιότυπα δεδομένων είναι αρκετά λιγότερα σε πλήθος από ότι τα φυσιολογικά. Το πρόβλημα αυτό αναλύεται εκτενώς στη βιβλιογραφία της εξόρυξης δεδομένων και της μηχανικής μάθησης [3]. Κατά δεύτερον η συλλογή δεδομένων που αντιπροσωπεύουν ανώμαλη κίνηση είναι συνήθως δύσκολη. Έχουν προταθεί στη βιβλιογραφία μέθοδοι σκόπιμης εισαγωγής δεδομένων που αποκλίνουν, εντός του συνόλου των δεδομένων εκπαίδευσης για να ξεπεράσουν την παραπάνω δυσκολία [3].

Semisupervised Methods Η τεχνική αυτή λειτουργεί με κατηγοριοποιημένα δεδομένα μόνο για μια κατηγορία στιγμιοτύπων δεδομένων (φυσιολογική ή μή). Συνήθως μοντελοποιείται μόνο η φυσιολογική κατηγορία. Αυτές οι τεχνικές βρίσκουν συνήθως εφαρμογή σε περισσότερα πεδία, κυρίως σε αυτά για τα οποία δεν είναι εύκολη η μοντελοποίηση όλων των μη φυσιολογικών περιπτώσεων. Η συνήθης προσέγγιση είναι η δημιουργία ενός μοντέλου για τη φυσιολογική κίνηση και η σύγκριση των στιγμιοτύπων των δεδομένων με αυτό.

Σε μερικές περιπτώσεις της βιβλιογραφίας συναντάται η μοντελοποίηση μόνο της κατηγορίας των μη-φυσιολογικών δεδομένων [3]. Αυτή η τεχνική δε χρησιμοποιείται πολύ λόγω του ότι είναι δύσκολη η μοντελοποίηση όλων των πιθανών καταστάσεων μη-φυσιολογικής κίνησης.

Unsupervised Methods Αυτές οι τεχνικές δεν χρησιμοποιούν ξεχωριστά δεδομένα εκπαίδευσης αλλά χρησιμοποιούν τα στιγμιότυπα δεδομένων της δικτυακής κίνησης με την παραδοχή, ότι τα φυσιολογικά στιγμιότυπα είναι πιο συχνά από τα αποκλίνοντα. Αν αυτή η παραδοχή απέχει από την πραγματικότητα, οι τεχνικές παρουσιάζουν υψηλό FNR.

Οι τεχνικές unsupervised λόγω του ότι δεν έχουν κάποιο έτοιμο μοντέλο δικτυακής κίνησης, έχουν ένα πιο ευρύ φάσμα εφαρμογών. Επειδή όμως η κατηγοριοποίηση της δικτυακής κίνησης εξαρτάται μόνο από τα στιγμιότυπα μη φυσιολογικής κίνησης, που έχει

συναντήσει το σύστημα μέχρι εκείνη τη στιγμή, το παραγόμενο μοντέλο είναι συνεπές μόνο για αυτές τις αποκλίνουσες περιπτώσεις.

4.5.2.4 Κατηγορίες Anomaly Based Τεχνικών

Στο σημείο αυτό κρίνεται σκόπιμο να γίνει αναφορά στις διάφορες κατηγορίες των τεχνικών με βάση τους αλγορίθμους που χρησιμοποιούν.

Classification based anomaly detection Η κατηγοριοποίηση (clasification) χρησιμοποιείται για την εκμάθηση ενός μοντέλου (clasifier), με τη χρήση ονοματισμένων στιγμιοτύπων δεδομένων (training data instances) και στη συνέχεια κατηγοριοποιεί τα στιγμιότυπα των δεδομένων ελέγχου (testing data instances) με βάση το γνωστό μοντέλο.

Οι τεχνικές κατηγοριοποίησης μπορούν να διαχωριστούν σε δυο ευρείς τύπους:

- Multi-class - όταν τα δεδομένα εκμάθησης ανήκουν σε πολλαπλές κατηγορίες φυσιολογικής κίνησης. Σε αυτή την περίπτωση ένα στιγμιότυπο δεδομένων ελέγχου ονοματίζεται ως αποκλίνον εάν δεν ανήκει σε καμία από τις φυσιολογικές κατηγορίες.

- One-class - όταν υπάρχει μόνο μια κατηγορία φυσιολογικών δεδομένων.

Το κύριο πλεονέκτημα των τεχνικών κατηγοριοποίησης είναι κυρίως η ταχύτητά τους, καθώς τα δεδομένα ελέγχου συγκρίνονται με προϋπολογισμένα μοντέλα. Ειδικότερα, αλγόριθμοι που βασίζονται σε δέντρα απόφασης, εμφανίζονται ως οι πιο αποδοτικοί [3]. Το κύριο μειονέκτημα των τεχνικών αυτών είναι η δυσκολία της ακριβούς κατηγοριοποίησης των δεδομένων εκπαίδευσης, ειδικά σε multi-class περιπτώσεις.

Στις επόμενες παραγράφους αναλύονται τεχνικές κατηγοριοποίησης που χρησιμοποιούν διαφορετικούς αλγόριθμους παραγωγής του μοντέλου εκμάθησης (clasifier).

- Neural Networks-Based - Είναι συνήθως multi-class τεχνικές, οι οποίες χρησιμοποιούν δεδομένα εκμάθησης για την εκπαίδευση ενός τεχνητού νευρωνικού δικτύου, στην κλάση των φυσιολογικών τιμών. Στη συνέχεια τα στιγμιότυπα δεδομένων ελέγχου δίδονται ως είσοδος στο νευρωνικό δίκτυο. Εάν τα δεδομένα ελέγχου γίνουν αποδεκτά από το δίκτυο, τότε είναι φυσιολογικά, ενώ εάν απορρίπτεται, δεν είναι.

- Bayesian Networks-Based - Είναι συνήθως multi-class τεχνικές οι οποίες χρησιμοποιούν ένα δίκτυο Bayes για τον υπολογισμό των πιθανοτήτων της φυσιολογικότητας και μη, δεδομένου ενός στιγμιότυπου δεδομένων ελέγχου. Για την εκτίμηση των πιθανοτήτων λαμβάνονται υπόψη και τα στιγμιότυπα των δεδομένων εκπαίδευσης [3].

- Support Vector Machines-Based - Είναι συνήθως one-class τεχνικές και χρησιμοποιούν Support Vector Machines για την εκμάθηση μιας περιοχής, η οποία περιέχει τα αποδεκτά στιγμιότυπα δεδομένων εκπαίδευσης. Στη συνέχεια ο αλγόριθμος αποφαίνεται εάν τα δεδομένα ελέγχου εμπίπτουν στην γνωστή περιοχή (φυσιολογικά στιγμιότυπα) ή όχι.

- Rule-Based - Σε αυτή την τεχνική γίνεται εκμάθηση κανόνων, οι οποίοι περιγράφουν την αναμενόμενη φυσιολογική συμπεριφορά. Ένα στιγμιότυπο δεδομένων, το οποίο δεν καλύπτεται από κανένα από τους παραπάνω κανόνες θεωρείται ως μη φυσιολογική κίνηση. Αυτή η τεχνική μπορεί να εφαρμοστεί τόσο σε multi-class όσο και σε one-class εκδοχές. Η βασική τεχνική χωρίζεται σε δυο φάσεις. Κατά την πρώτη

φάση γίνεται η εκμάθηση των κανόνων μέσω των δεδομένων εκπαίδευσης, με κάποιο σχετικό αλγόριθμο εκμάθησης κανόνων (π.χ. RIPPER, δέντρα απόφασης κ.α. [3]). Κάθε κανόνας χαρακτηρίζεται από ένα επίπεδο εμπιστοσύνης (confidence level). Σε δεύτερη φάση αξιολογούνται τα δεδομένα ελέγχου με βάση τους προαναφερθέντες κανόνες.

Nearest Neighboor Based - Οι τεχνικές αυτές βασίζονται στην παραδοχή ότι οι φυσιολογικές τιμές είναι συνήθως συγκεντρωμένες σε πυκνές γειτονιές, ενώ οι αποκλίνουσες είναι αρκετά μακριά από αυτές. Η τεχνική αυτή χρησιμοποιεί μια μετρική απόστασης μεταξύ των δεδομένων. Αυτή η μετρική μπορεί να καθοριστεί κατά περίπτωση. Για παράδειγμα για συνεχείς τιμές δεδομένων μπορεί να χρησιμοποιηθεί η Ευκλείδεια απόσταση.

Το κύριο πλεονέκτημα της τεχνικής αυτής είναι ότι λόγω της φύσης της (unsupervised), μπορεί να χρησιμοποιηθεί σε ένα ευρύ πεδίο εφαρμογών, απλά καθορίζοντας την κατάλληλη μετρική της απόστασης. Το κύριο μειονέκτημά της είναι, ότι η επιλογή της μετρικής απόστασης μπορεί να μην είναι βέλτιστη ή να βασίζεται σε αυθαίρετη κρίση, αυξάνοντας το FNR. Σε ορισμένες περιπτώσεις εμφανίζει υψηλή υπολογιστική πολυπλοκότητα, αναλόγως με την μετρική που επιλέγεται.

Clustering Based Συσταδοποίηση είναι η κατηγοριοποίηση συναφών δεδομένων σε συστάδες (clusters). Η συσταδοποίηση είναι κατά κύριο λόγο μια τεχνική unsupervised, αν και έχουν προταθεί κατά καιρούς και semisupervised τεχνικές [3]. Η μέθοδος αυτή είναι παρόμοια με την προηγούμενη καθώς και εδώ υπολογίζεται μια μετρική απόστασης από συστάδες φυσιολογικών τιμών. Η βασική διαφορά με τη προηγούμενη μέθοδο βρίσκεται στο γεγονός ότι υπολογίζει την απόσταση του στιγμιότυπου δεδομένων ελέγχου από τη συστάδα, ενώ η προηγούμενη μέθοδος από τον πιο κοντινό γείτονα. Τα πλεονεκτήματα και μειονεκτήματα της τεχνικής είναι παρόμοια με αυτά των nearest neighboor based.

Statistical Based - Οι τεχνικές αυτές λειτουργούν υπό την παραδοχή, ότι φυσιολογικά στιγμιότυπα δεδομένων ελέγχου, εμφανίζονται σε περιοχές υψηλής πιθανότητας ενός στοχαστικού μοντέλου, ενώ αντίστροφα, μη φυσιολογικές τιμές εμφανίζονται σε περιοχές χαμηλότερης πιθανότητας. Οι στατιστικές τεχνικές εφαρμόζουν ένα στατιστικό μοντέλο (συνήθως προερχόμενο από φυσιολογικά στιγμιότυπα δεδομένων) στα δεδομένα ελέγχου. Έπειτα υλοποιούν έναν στατιστικό έλεγχο συμπερασμού για το εάν τα δεδομένα ελέγχου ακολουθούν ή όχι το μοντέλο. Υπάρχουν δυο κύριες κατηγορίες αυτών των τεχνικών, όπως παρακάτω:

- Parametric Based - Θεωρούν ότι τα δεδομένα ακολουθούν γνωστή στατιστική κατανομή και υπολογίζουν τις παραμέτρους της με βάση τα δεδομένα εισόδου.
- Non-Parametric Based - Γενικά δε θεωρούν γνωστή την στατιστική κατανομή.

Τα κύρια πλεονεκτήματα των τεχνικών αυτών είναι ότι εάν το στατιστικό μοντέλο είναι κοντά στην πραγματικότητα, αποδίδει μια γρήγορη και ακριβή εκτίμηση της κατηγορίας των δεδομένων, εντός ενός διαστήματος εμπιστοσύνης. Επίσης, σε αυτή την περίπτωση η τεχνική μπορεί να είναι unsupervised χωρίς να είναι απαραίτητη η ύπαρξη δεδομένων εκπαίδευσης.

Το κύριο μειονέκτημα της μεθόδου είναι ότι εάν το μοντέλο δεν ανταποκρίνεται στην πραγματικότητα, το DR είναι αρκετά χαμηλό. Επίσης μεγάλο ρόλο στην ακρίβεια της μεθόδου παίζει και ο ορθός καθορισμός των διαστημάτων εμπιστοσύνης. Τέλος, στις παραμετρικές μεθόδους, η επιλογή μιας στατιστικής κατανομής, η οποία δεν ανταποκρίνεται στα δεδομένα εισόδου μειώνει κατά πολύ το DR της τεχνικής ανίχνευσης.

Information Theory Based - Οι τεχνικές αυτές αναλύουν το πληροφοριακό φορτίο των δεδομένων ελέγχου χρησιμοποιώντας μετρικές από τη Θεωρία της Πληροφορίας, όπως πολυπλοκότητα Kolmogorov, εντροπία, σχετική εντροπία κ.α. [3]. Η τεχνική αυτή λειτουργεί υπό την παραδοχή ότι ανωμαλίες στα δεδομένα εισόδου δημιουργούν διαταραχές της κανονικότητας στο πληροφοριακό φορτίο του συνόλου των δεδομένων.

Τα κύρια πλεονεκτήματα αυτών των τεχνικών είναι ότι μπορούν να λειτουργήσουν και ως unsupervised, ενώ δεν κάνουν κάποια παραδοχή για τη στατιστική κατανομή των δεδομένων εισόδου. Το κύριο μειονέκτημα της μεθόδου είναι η εκθετική υπολογιστική πολυπλοκότητα, αν και έχουν προταθεί προσεγγιστικές μέθοδοι όπου η πολυπλοκότητα εμφανίζεται γραμμική [3].

4.6 Συζήτηση και Εκτιμήσεις

Η έρευνα σε ότι αφορά την ανίχνευση επιθέσεων έχει μεγάλο ενδιαφέρον, ιδιαίτερα αυτή που αφορά σε δίκτυα κινητής τηλεφωνίας, κυρίως λόγω του ευρέος πεδίου εφαρμογής της και των εμπλεκόμενων οικονομικών μεγεθών. Στη βιβλιογραφία έχουν προταθεί κατά καιρούς διάφορες μέθοδοι πάνω στο θέμα.

Στο [7] προτείνεται το ABID, ένα semi-supervised IDS το οποίο χρησιμοποιεί μηχανική μάθηση (Instance based Learning) και βασίζεται στην ανάλυση της κινητικότητας των ασύρματων κόμβων (mobility profiles). Οι συγγραφείς παρατηρούν ότι ένα IDS του παραπάνω τύπου, είναι εξαιρετικά αποτελεσματικό ενάντια σε επιθέσεις node capture, καθώς ένας κακόβουλος χρήστης έχει συνήθως διαφορετικό προφίλ μετακίνησης από τους υπόλοιπους κόμβους. Το σύστημα ρυθμίζεται με βάση δυο παραμέτρους:

- Επίπεδο ακρίβειας (precision level, PL) - Αφορά στην ακρίβεια προσδιορισμού της θέσης ενός μετακινούμενου κόμβου (γεωγραφικό μήκος και πλάτος).
- Μήκος ακολουθίας (sequence length, SL) - Αφορά στο πλήθος των υπό εξέταση διαδρομών.

Η μέθοδος χαρακτηρίζει παρατηρούμενες τιμές, οι οποίες είναι πολύ κοντά στα δεδομένα εκπαίδευσης, ως κακόβουλη για να αποφύγει επιθέσεις τύπου profile replay. Το μειονέκτημα αυτής της μεθόδου είναι η μεγάλη περίοδος εκπαίδευσης, η οποία διαρκεί έως και 6 μήνες. Οι συγγραφείς εστιάζουν κυρίως σε επιθέσεις τύπου profile replay και node capture.

Στο [8] προτείνεται ένα πολυεπίπεδο IDS το οποίο χρησιμοποιεί νευρωνικά δίκτυα και αποκαλείται Host based Multi-level Behaviour Profiling Mobile IDS (HMBPM). Εξετάζονται χαρακτηριστικά επιπέδου εφαρμογής (layer 7), όπως URL που ζητήθηκαν, επιπέδου δικτύου (πακέτα που εκπέμφθηκαν) και επιπέδου συστήματος (επεξεργαστικός φόρτος). Στην υπόψη μελέτη υλοποιούνται τρία ακτινικά νευρωνικά δίκτυα, ένα για κάθε ένα από τις παρακάτω δραστηριότητες: λεπτομέρειες κλήσεων, χρήση συσκευής και δραστηριότητα bluetooth. Η μέθοδος τροποποιεί περιοδικά τα χαρακτηριστικά(features) του συνόλου δεδομένων των νευρωνικών δικτύων με βάση τις αλλαγές στα μοτίβα συμπεριφοράς. Το μειονέκτημα αυτής της μεθόδου είναι το υψηλό ποσοστό αποτυχίας ανιχνεύσεων, το οποίο μπορεί να φτάσει και το 36.4%. Οι συγγραφείς εστιάζουν κυρίως σε επιθέσεις τύπου spoofing και node capture.

Τέλος, στο [15] οι μελετητές προτείνουν ένα multitrust IDS που ονομάζεται Intrusion Detection Architecture for Mobile Networks (IDAMN), το οποιο ανιχνεύει τις επιθέσεις σε πραγματικό χρόνο (κατά τη διάρκεια της κλήσης) και κατανέμει το υπολογιστικό φορτίο ιεραρχικά. Η προτεινόμενη μέθοδος χρησιμοποιεί τρεις τεχνικές για να ανιχνεύσει τις επιθέσεις:

- Μελέτη της ταχύτητας κίνησης των κόμβων - πελατών για ανίχνευση κλωνοποιημένων κόμβων.
- Ανίχνευση αναντιστοιχιών μεταξύ της δραστηριοτήτων κόμβων - σταθμών βάσης και της ανιχνευόμενης πυκνότητας των κόμβων - πελατών.
- Σύγκριση συμπεριφοράς χρηστών με γνωστά προφίλ.

Τα γνωστά προφίλ χρηστών αποτελούνται από δυο μέρη: κινητικότητα - διαδρομή και λεπτομέρειες κλήσεων. Για το μέρος που αφορά στις κλήσεις, η μέθοδος λαμβάνει υπόψη της περισσότερο τα νεότερα δεδομένα από τα παλαιότερα, ενώ το μέρος της κινητικότητας χρησιμοποιεί περισσότερο τις συχνότερες διαδρομές από τις πιο σπάνιες.

Το πλεονέκτημα αυτής της μεθόδου είναι ότι το FPR της είναι χαμηλό και κυμαίνεται μεταξύ 1% - 7%. Το μειονέκτημά της είναι ότι το DR είναι αρκετά χαμηλό, έως και 60%. Οι συγγραφείς εστιάζουν κυρίως σε επιθέσεις τύπου spoofing και node capture.

4.6.1 Εκτίμηση Αποτελεσματικότητας

Το μεγαλύτερο πλεονέκτημα των μεθόδων anomaly based είναι το ότι δεν είναι απαραίτητο να ψάχνουν για κάτι συγκεκριμένο. Το γεγονός αυτό απαλείφει την ανάγκη να προτυποποιηθούν όλοι οι αναμενόμενοι τύποι επιθέσεων και να ανανεώνονται τα attack dictionaries [12].

Ένα μεγάλο μειονέκτημα αυτών των μεθόδων είναι ότι είναι επιρρεπείς σε υψηλά ποσοστά ψευδών αναγνωρίσεων (false positives). Ένα ακόμα μειονέκτημα των μεθόδων αυτών είναι ότι κατά τη φάση προτυποποίησης - εκπαίδευσης του συστήματος, αυτό είναι ευάλωτο σε πλήθος επιθέσεων τις οποίες δε μπορεί να αναγνωρίσει.

Επίσης μια παραδοχή η οποία γίνεται σε αυτές τις μεθόδους, είναι ότι οι ανωμαλίες στην δικτυακή κίνηση συμβαίνουν σπάνια σε σχέση με τη αποδεκτή φυσιολογική κίνηση. Αν και αυτό τις περισσότερες φορές είναι αποδεκτό, υπάρχουν περιπτώσεις στις οποίες αυτό δεν ισχύει. Τέτοιο παράδειγμα αποτελεί η ανίχνευση μη φυσιολογικής κίνησης προερχόμενης από worm malware. Σε αυτή την περίπτωση, η μη φυσιολογική κακόβουλη κίνηση είναι μεγαλύτερου όγκου από την φυσιολογική [3].

Ένα χαρακτηριστικό (feature) είναι ένα πεδίο σε μια πλειάδα πολυμεταβλητού συνόλου δεδομένων. Το πλήθος των χαρακτηριστικών ενός συνόλου δεδομένων αποτελεί έναν κατά προσέγγιση εκτιμητή της αποδοτικότητας της μεθόδου ανίχνευσης επιθέσεων, καθώς μεγάλο πλήθος χαρακτηριστικών υπονοεί μεγαλύτερες απαιτήσεις σε μνήμη και επεξεργαστική ισχύ. Θα πρέπει να σημειωθεί ότι η επιλογή του πλήθους των χαρακτηριστικών αποτελεί ένα δύσκολο πρόβλημα καθώς η επιλογή πολλών χαρακτηριστικών δεν αποδίδει απαραίτητα καλύτερα ποσοστά ανίχνευσης.

Οι μέθοδοι ανίχνευσης με εύρεση ανωμαλιών είναι πιο αποδοτικές για ασύρματα δίκτυα κινητής τηλεφωνίας, WMN και υπό επίβλεψη CPs. Το κοινό χαρακτηριστικό όλων των παραπάνω τύπων ασύρματων δικτύων είναι ότι είναι κατασκευασμένα με ειδικό τρόπο ώστε να εξυπηρετούν συγκεκριμένο σκοπό και να έχουν ένα καθορισμένο πλαίσιο λειτουργιών.

Επίσης, ασύρματα δίκτυα WLAN, WPAN και Ad-Hoc μπορούν να χρησιμοποιήσουν ευεργετικά μεθόδους ανίχνευσης με εύρεση ανωμαλιών, λόγω των αρκετών και εν πολλοίς μη-έμπιστων πελατών που συμμετέχουν σε αυτά.

Οι μέθοδοι αυτοί βρίσκουν επίσης αποδοτική εφαρμογή σε δίκτυα WSN, λόγω κυρίως των μικρών δυνατοτήτων τους σε αποθηκευτικό χώρο, καθώς δεν είναι απαραίτητη η τήρηση attack dictionaries.

5 Συμπεράσματα

Στο παρόν, εκτέθηκαν συνοπτικά οι κύριοι τύποι ασύρματων δικτύων με τα ιδιαίτερα χαρακτηριστικά τους. Στη συνέχεια αναλύθηκαν οι απειλές και οι επιπτώσεις που αυτές μπορούν να προκαλέσουν στην ορθή λειτουργία των ασύρματων δικτύων.

Επιπλέον αναφέρθηκαν οι έννοιες της ασφάλισης των δικτύων και η ορθή κατά βάθος συγκρότηση των ζωνών άμυνας. Αναλύθηκαν οι λειτουργίες της αποτροπής πρόσβασης (IPS) και ανίχνευσης επιθέσεων (IDS). Στη συνέχεια περιγράφηκαν τα κύρια έργα ενός (IDS), αναλύθηκαν οι τεχνικές συλλογής και ανάλυσης δεδομένων και έγινε αναφορά στις μεθόδους ανίχνευσης επιθέσεων της βιβλιογραφίας.

Η προσοχή εστιάσθηκε κυρίως στις μεθόδους ανίχνευσης επιθέσεων με βάση την εύρεση ανωμαλιών στην κίνηση του δικτύου. Περιγράφηκαν οι πιθανοί τύποι ανωμαλιών που συναντώνται συχνότερα. Στη συνέχεια αναλύθηκαν οι τρόποι λειτουργίας των μεθόδων αυτών (supervised, semi-supervised, unsupervised) και οι τεχνικές προσέγγισης με τα πλεονεκτήματα και μειονεκτήματά τους (στατιστικές, μη-παραμετρικές, νευρωνικά δίκτυα κτλ). Επίσης, εκτέθηκαν οι δυνατότητες και οι αδυναμίες της μεθόδου anomaly based. Τέλος αναφέρθηκαν οι εφαρμογές των μεθόδων της βιβλιογραφίας στα ασύρματα δίκτυα κινητής τηλεφωνίας.

Κατάλογος Σχημάτων

Βιβλιογραφία

[1] Alem, Yibeltal Fantahun και Zhao Cheng Xuan: *Preventing black hole attack in mobile ad-hoc networks using anomaly detection*. 2010 2nd International Conference on Future Computer and Communication, 2010.

[2] Chaki, Nabendu και Rituparna Chaki: *Intrusion detection in wireless ad-hoc networks*. 2014.

[3] Chandola, V., Banerjee A. και Kumar: *Anomaly detection: A survey*. 2009.

[4] Chatzigiannakis, V., S. Papavassiliou, M. Grammatikou, και B. Maglaris: *Hierarchical anomaly detection in distributed large-scale sensor networks*. 11th IEEE Symposium on Computers and Communications (ISCC'06), 2006.

[5] Deng, Hongmei, R. Xu, J. Li, F. Zhang, R. Levy, και Wenke Lee: *Agent-based cooperative anomaly detection for wireless ad hoc networks*. 12th International Conference on Parallel and Distributed Systems - (ICPADS'06), 2006.

[6] Du, Wenliang, Lei Fang, και Peng Ning: *Lad: Localization anomaly detection for-wireless sensor networks*. 19th IEEE International Parallel and Distributed Processing Symposium, 2005.

[7] Hall, J., M. Barbeau, και E. Kranakis: *Anomaly-based intrusion detection using mobility profiles of public transportation users*. WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005., 2005.

[8] Li, Fudong, Nathan Clarke, Maria Papadaki, και Paul Dowland: *Behaviour profiling on mobile devices*. 2010 International Conference on Emerging Security Technologies, 2010.

[9] Limthong, Kriangkrai: *Performance of interval-based features in anomaly detection by using machine learning approach*. International Journal of Machine Learning and Computing, 4(3):292–299, 2014.

[10] Liu, S., Y. Chen, W. Trappe, και L. J. Greenstein: *Aldo: An anomaly detection framework for dynamic spectrum access networks*. IEEE INFOCOM 2009 - The 28th Conference on Computer Communications, 2009.

[11] Mahmood, R.a. Raja και A.i. Khan: *A survey on detecting black hole attack in aodv-based mobile ad hoc networks*. 2007 International Symposium on High Capacity Optical Networks and Enabling Technologies, 2007.

[12] Mitchell, Robert και Ing Ray Chen: *A survey of intrusion detection in wireless network applications*. Computer Communications, 42:1–23, 2014.

[13] Patwardhan, A., J. Parker, A. Joshi, M. Iorga, και T. Karygiannis: *Secure routing and intrusion detection in ad hoc networks*. Third IEEE International Conference on Pervasive Computing and Communications, 2005.

[14] Rajasegarar, S., C. Leckie, και M. Palaniswami: *Anomaly detection in wireless sensor networks*. IEEE Wireless Communications, 15(4):34–40, 2008.

[15] Samfat, D. και R. Molva: *Idamn: an intrusion detection architecture for mobile networks*. IEEE Journal on Selected Areas in Communications, 15(7):1373–1380, 1997.

[16] Turcotte, Melissa: *Anomaly detection in dynamic networks*. 2014.

[17] Zhang, Yongguang και Wenke Lee: *Intrusion detection in wireless ad-hoc networks*. Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00, 2000.