Πανεπιστήμιο Μακεδονίας	University of Macedonia
ΔΠΜΣ Πληροφοριακά Συστήματα	Master Information Systems
Δίκτυα Υπολογιστών	Computer Networks
Καθηγητής: Α.Α. Οικονομίδης	Professor: A.A. Economides

SECURITY, ATTACKS AND COUNTERMEASURES IN WIRELESS CELLULAR NETWORKS – ΑΣΦΑΛΕΙΑ, ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΣΤΑ ΚΥΨΕΛΩΤΑ ΔΙΚΤΥΑ

Δελαπόρτας Αναστάσιος

A.M : 16044

tasosdellaportas@hotmail.gr

Θεσσαλονίκη

Μάιος 2016

ΠΕΡΙΛΗΨΗ

Η σημασία της ασύρματης κυψελωτής επικοινωνίας στην καθημερινή μας ζωή έχει αυξηθεί αρκετά στην τελευταία δεκαετία. Εκτός από τη χρησιμοποίηση των κυψελωτών τηλεφώνων για τη μετάδοση φωνής, τα χρησιμοποιούμε συνήθως για να έχουμε πρόσβαση στο Διαδίκτυο, να διευθύνουμε χρηματικές συναλλαγές, να στέλνουμε μηνύματα κειμένου και να ρωτήσουμε πολύ χρήσιμες πληροφορίες. Η χρήση των κινητών τηλεφώνων στην καθημερινή επικοινωνία μας, ωστόσο, εγείρει πολλά εκκρεμή θέματα ασφαλείας. Σε αυτή την εργασία προσδιορίζονται πιθανές επιθέσεις στην ασύρματη κυψελωτή δικτυακή αρχιτεκτονική και προτείνονται μερικά κατάλληλα μέτρα. Διάφορες επιθέσεις μπορούν να αποτραπούν προκειμένου να διατηρηθεί η ασφάλεια στην ασύρματη κυψελωτή επικοινωνία.

Abstract

Wireless cellular communication has become an important part of our daily life in the last decade. Apart from the usage of cell phones for phone calls , we also use them to access the Internet , carry out financial transactions , send text messages and ask for useful information . The usage of mobile phones , though , raises many security issues . In this project, potential attacks in wireless cellular network infrastructure are defined and some suitable countermeasures are suggested. Therefore, several attacks may be prevented in order to ensure security in wireless cellular communication.

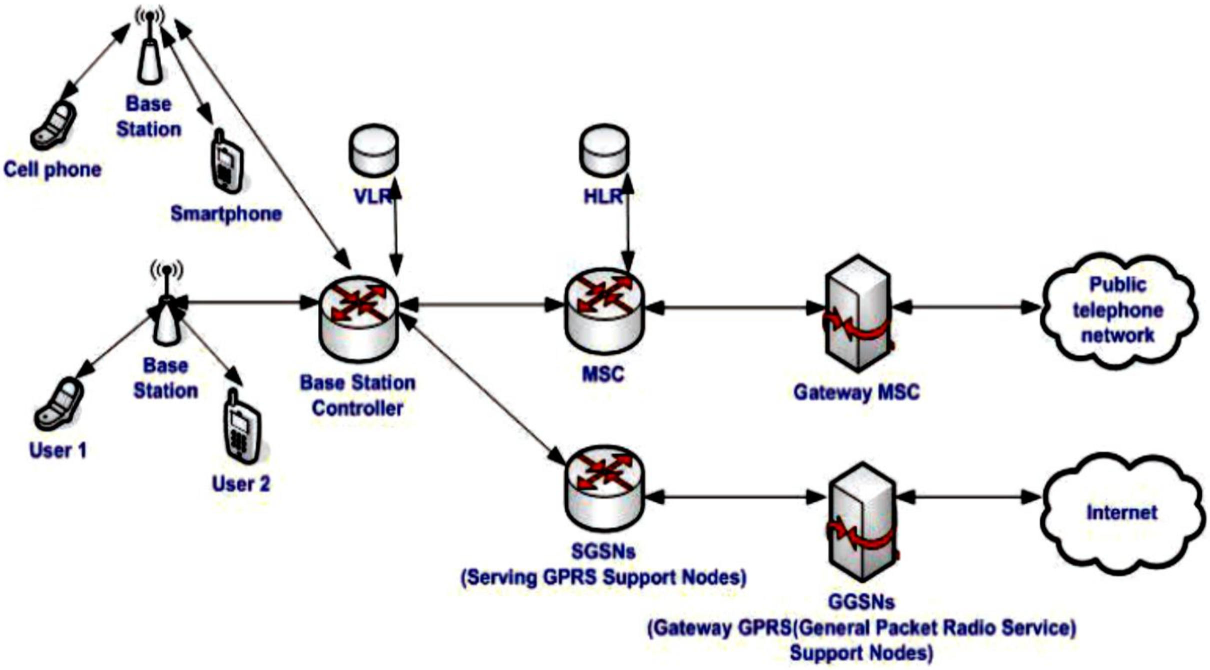
1. ΕΙΣΑΓΩΓΗ

Η πρόβλεψη και η τάση που διαφαίνεται από τις έρευνες που πραγματοποιούνται από τη Microsoft στους πελάτες της δείχνουν ότι το 2014 η χρήση του κινητού Διαδικτύου έχει υπερβεί τη χρήση του Διαδικτύου υπολογιστών γραφείου (Microsoft Tag, 2012). Το ερευνητικό κέντρο Διαδίκτυο Pew και το πρόγραμμα American Life δείχνουν ότι 55% των χρηστών κινητών τηλεφώνων συνδέονται στο διαδίκτυο πιο συχνά από τις κινητές συσκευές τους (Smith, 2012).

Η έρευνα Mobile Commerce Daily δείχνει ότι 51.1% των χρηστών κινητών τηλεφώνων ελέγχουν το ηλεκτρονικό ταχυδρομείο τους χρησιμοποιώντας μόνο μια κινητή συσκευή. Οι χρήστες που πραγματοποιούν αναζητήσεις Διαδικτύου χρησιμοποιώντας μόνο μια κινητή συσκευή είναι περίπου 45.3%. Επίσης 25.4% των καταναλωτών πραγματοποιούν ηλεκτρονικό εμπόριο χρησιμοποιώντας τα τηλέφωνά τους. Όσον αφορά την κοινωνική δικτύωση, η έρευνα δείχνει ότι 42.3% των χρηστών συνδέονται στο Facebook και 14.8% στο Twitter μόνο από τις κινητές συσκευές τους (Tode, 2012). Δεδομένου ότι σημαντικές δραστηριότητες Διαδικτύου πραγματοποιούνται καθημερινά μέσω των smartphones, οι ερωτήσεις που ανακύπτουν φυσικά είναι πόσο ασφαλές αυτό το είδος επικοινωνίας είναι και ποιος είναι ο συμβιβασμός που ο χρήστης πρέπει να εξετάσει. Η παρούσα εργασία έχει στόχο να προσδιοριστούν οι πιθανές επιθέσεις ασφάλειας και να προταθούν μερικά κατάλληλα μέτρα στα ασύρματα κυψελωτά δίκτυα. Το όφελος αναγνώρισης αυτών των πιθανών επιθέσεων είναι να αποτραπούν οι επιτιθέμενοι από την εισβολή στην ασφάλεια των χρηστών και δικτύων.

2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΥΨΕΛΩΤΩΝ ΔΙΚΤΥΩΝ

Η εικόνα 1 παρουσιάζει τη βασική αρχιτεκτονική ενός ασύρματου κυψελοειδούς δικτύου (Venkataram, 2010). Οι σταθμοί βάσης (BS) και οι ελεγκτές σταθμών βάσης (BSC) είναι τα πρώτα συστατικά του ασύρματου κυψελοειδούς δικτύου (WCN).Εκτελούν όλες τις λειτουργίες που είναι απαραίτητες για να διατηρηθούν οι ραδιο-συνδέσεις σε ένα κινητό τηλέφωνο, με την κωδικοποίηση/ αποκωδικοποίηση της φωνής. Κάθε BS περιλαμβάνει όλο το ραδιο- εξοπλισμό, δηλ. κεραίες, επεξεργασία σήματος, ενισχυτές απαραίτητους για τη ραδιο-μετάδοση.



Εικόνα 1: Βασική αρχιτεκτονική κυψελωτού δικτύου

Το BSC λαμβάνει ραδιοσυχνότητες, χειρίζεται την παράδοση από ένα BS σε άλλο μέσα στο BSS. Επίσης είναι αρμόδιο για την εκτέλεση της σελιδοποίησης στα Smartphone.Το κινητό κέντρο μετατροπής (MSC), οι γενικοί κόμβοι υποστήριξης υπηρεσιών ραδιο- πακέτων (SGSN) και οι κόμβοι υποστήριξης πυλών (GPRS) (GGSN) συνδέουν το ασύρματο δίκτυο με το κοινό τηλεφωνικό δίκτυο (PSTN) και το Διαδίκτυο. Το MSC εκτελεί τις υποβολές μεταξύ διαφορετικών BSCs και υποστηρίζει επίσης τη χρέωση, το λογαριασμό, και το roaming των χρηστών μεταξύ των διαφορετικών παρόχων στις διάφορες χώρες (Kurose & Ross, 2009). Τα συστήματα μεταγωγής δικτύων αποτελούνται από έναν κατάλογο εγχώριας θέσης (HLR), τους καταλόγους θέσης επισκεπτών (VLR), και τα κινητά κέντρα μετατροπής

(MSC). Το HLR είναι η σημαντικότερη βάση δεδομένων στο σύστημα, επειδή αποθηκεύει όλες τις πληροφορίες των χρηστών, δηλ. στατικές πληροφορίες, όπως οι προσυπογραμμένες υπηρεσίες, και δυναμικές πληροφορίες, όπως η θέση χρηστών. Το HLR μπορεί να διαχειριστεί τα στοιχεία για αρκετά εκατομμύρια πελατών (Beaubrun, Moulin & Jabeur, 2007). Τα VLR (κατάλογοι θέσης επισκεπτών) είναι δυναμικές βάσεις δεδομένων που αποθηκεύουν τις πολύ σημαντικές πληροφορίες για τους χρήστες κινητών στην περιοχή που ελέγχουν.

Κάθε VLR συνδέεται με ένα MSC που χειρίζεται όλη τη σηματοδότηση που απαιτείται για την οργάνωση της σύνδεσης, την απελευθέρωση της σύνδεσης και την παράδοση σε άλλο MSC. Όλες οι λειτουργίες που απαιτούνται για τις συμπληρωματικές υπηρεσίες, όπως η αποστολή κλήσης, οι κλήσεις με πολλούς συμμετέχοντες, και η αντίστροφη χρέωση εκτελούνται από κάθε MSC.Υπάρχουν δύο τύποι κόμβων στο κεντρικό 3G δίκτυο: κόμβοι υποστήριξης GPRS (SGSN) και κόμβοι υποστήριξης πυλών GPRS (GGSN). Το SGSN είναι αρμόδιο για την παράδοση του διαγράμματος δεδομένων από/ προς τους κινητούς κόμβους στα δίκτυα ραδιο-πρόσβασης με τα οποία το SGSN είναι συνδεμένο. Το SGSN αλληλεπιδρά με το Msc, παρέχει διαπίστευση των χρηστών και handoff και ενεργεί ως πύλη που συνδέει πολλά SGSN. Το Διαδίκτυο είναι απαραίτητο για να έχει στον ιστό και σε διακομιστές βάσεων δεδομένων (Beaubrun, Moulin & Jabeur, 2007).

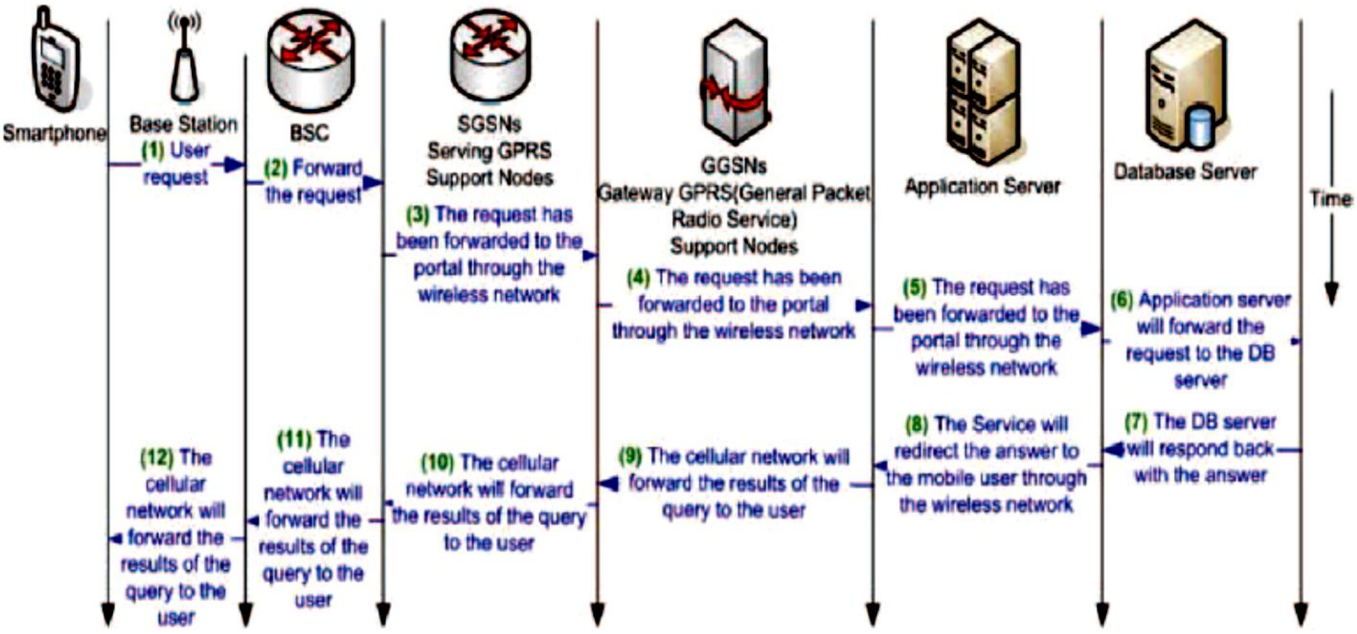
Το κέντρο κινητής μετατροπής είναι το συστατικό που συνδέεται με την οργάνωση, την απελευθέρωση, και τη δρομολόγηση κλήσης στο WCN. Ο κατάλογος θέσης επισκεπτών είναι μια βάση δεδομένων σε μια τρέχουσα διαδικασία ενημέρωσης των αρχείων των συνδρομητών που περιπλανώνται μέσα σε μια περιοχή MSC. Ο κατάλογος αρχικής θέσης είναι η μόνιμη βάση δεδομένων που περιέχει τις πληροφορίες σχετικά με τους συνδρομητές που παίρνουν τα διαπιστευτήρια για να χρησιμοποιήσουν το δίκτυο GSM. Το στοιχείο ταυτότητας συνδρομητών (SIM) χρησιμεύει ως το αρχικό κλειδί για κάθε αρχείο HLR. Οι κόμβοι υποστήριξης GPRS (γενική υπηρεσία ραδιο- πακέτων) καθοδηγούν τα πακέτα σε και από τη γεωγραφική περιοχή SGSN. Το SGSN αποθηκεύει τις πληροφορίες θέσης και τις παραμέτρους χρήστη όλων των χρηστών του GPRS που εγγράφονται με αυτό το SGSN. Οι κόμβοι υποστήριξης πυλών GPRS διασυνδέονται με τα εξωτερικά δίκτυα πακέτων IP (Beaubrun, Moulin & Jabeur, 2007).

3. ΡΟΗ ΜΗΝΥΜΑΤΩΝ ΣΤΑ ΚΥΨΕΛΩΤΑ ΔΙΚΤΥΑ

Στην εικόνα 2 φαίνεται η ροή μηνυμάτων στην περίπτωση που ένας χρήστης κοιτάζει βιαστικά το Διαδίκτυο μέσω του smartphone του και συγκεκριμένα κάνει αναζήτηση ενός στοιχείου στο Amazon.

1. Ένα κινητό τηλέφωνο έχει πρόσβαση στον πιο κοντινό γεωγραφικό σταθμό βάσης που θα διαβιβάσει το αίτημα μέσω του ασύρματου δικτύου στο BSC (ελεγκτής σταθμών βάσης).
2. Το επόμενο βήμα όπου θα διαβιβαστεί το αίτημα του χρήστη είναι το SGSN κι έπειτα το GGSN.
3. Ο διακομιστής της εφαρμογής διαβάζει το αίτημα και το διαβιβάζει στον server.
4. Ο server αναλύει το αίτημα και βλέπει τι είναι το στοιχείο που θα αγοραστεί.
5. Ο server θα ψάξει για το συγκεκριμένο στοιχείο και θα εξάγει τις εγγραφές που ικανοποιούν τα κριτήρια αναζήτησης.

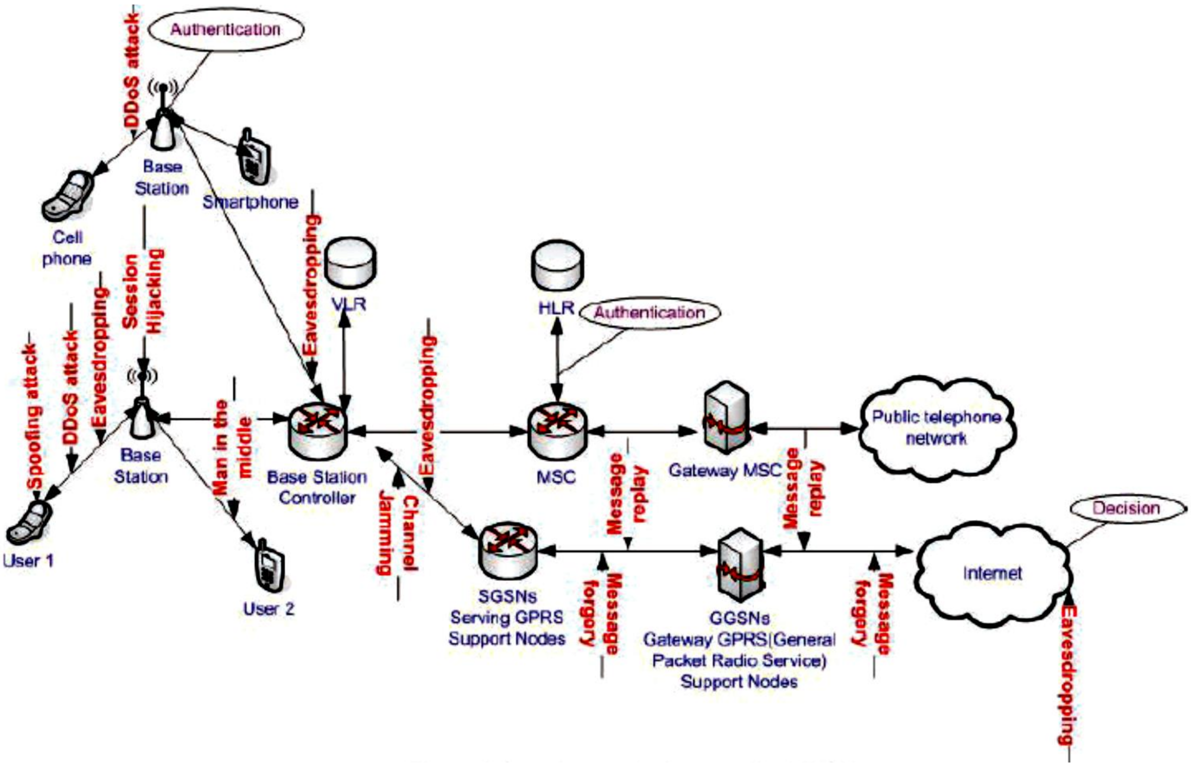
Έχοντας τα αποτελέσματα του αιτήματος, οι πληροφορίες στέλνονται στο χρήστη του smartphone μέσω του Διαδικτύου, της πύλης, και του κυψελωτού δικτύου. Το στοιχείο ζητούμενο θα παρουσιαστεί στο χρήστη και μπορεί να συνεχίσει με την πληρωμή ή κι άλλες αγορές (Beaubrun, Moulin & Jabeur, 2007).



Εικόνα 2: Ροή μηνυμάτων στα κυψελωτά δίκτυα όταν ένα συγκεκριμένο αίτημα στέλνεται από ένα smartphone και το αποτέλεσμα στέλνεται πίσω στο smartphone

4. ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΣΤΑ ΚΥΨΕΛΩΤΆ ΔΙΚΤΥΑ

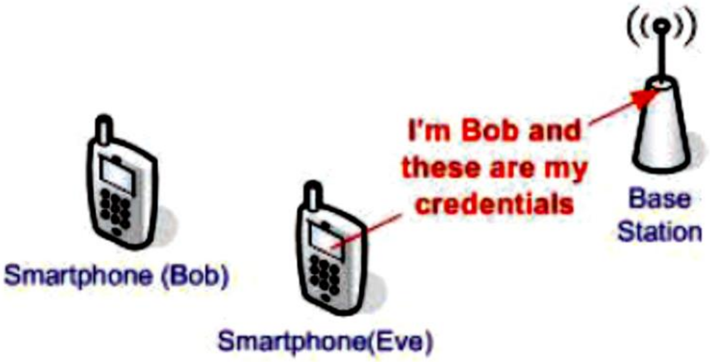
Το ασύρματο κυψελωτό δίκτυο έχει διάφορα τρωτά σημεία και ένας επιτιθέμενος μπορεί να συμβιβάσει ή να «κρυφακούσει» μέσω της δικτυακής αρχιτεκτονικής. Σε αυτό το κεφάλαιο προσδιορίζονται πιθανές επιθέσεις και προτείνονται τα αντίστοιχα μέτρα. Η εικόνα 3 παρουσιάζει τις επιθέσεις που προσδιορίζονται: εξαπάτηση, κατανεμημένη άρνηση υπηρεσίας, συμφόρηση καναλιών, υποκλοπή, πειρατεία της συνεδρίας, παραποίηση μηνυμάτων, απάντηση μηνυμάτων και επίθεση του ατόμου στη μέση.



Εικόνα 3: Επιθέσεις ασφαλείας στα κυψελωτά δίκτυα

4.1 Εξαπάτηση(spoofing attacks)

Η εξαπάτηση όπως περιγράφεται στην εικόνα 4 εμφανίζεται όταν ενεργεί ένας κακόβουλος χρήστης σαν να είναι νόμιμος και εκμεταλλεύεται τις πληροφορίες που ανταλλάσσονται στο δίκτυο (Felten et al., 1997). Ο επιτιθέμενος μπορεί να πλαστογραφήσει τα στοιχεία και τις πράξεις σαν να είναι συνδρομητής του δικτύου στην επικοινωνία με άλλους κόμβους και τους servers. Αυτή η επίθεση είναι εμφανής σε κινητές συσκευές όπως I-Phone, Android, Blackberry και Windows phone.



Εικόνα 4: Επίθεση εξαπάτησης

Μέτρα: Κάθε συσκευή χρησιμοποιεί τρεις παραμέτρους προσδιορισμού όταν πραγματοποιεί ένα αίτημα (ARP) (Plummer, 1982) στο δίκτυο οι οποίες είναι:

1. Η διεύθυνση ελέγχου προσπέλασης MEDIA (MAC) είναι μια μοναδική και μόνιμη φυσική διεύθυνση της συσκευής στο δίκτυο (Okamoto et al., 2002).
2. Το όνομα χρήστη μπορεί να οριστεί από τον χρήστη και μπορεί να τροποποιηθεί οποτεδήποτε. Συνήθως οι χρήστες κάνουν το συνηθισμένο λάθος να το καθορίζουν με το αντίστοιχο όνομα ή το επώνυμο τους. Δεν συστήνεται να χρησιμοποιηθούν αυτά τα στοιχεία για το όνομα χρήστη, καθώς μπορεί να χρησιμοποιηθεί από τους επιτιθεμένους και η συσκευή μπορεί να προσδιοριστεί εύκολα στο δίκτυο.
3. Το πρωτόκολλο Διαδικτύου (IP) χρησιμοποιείται για να διαβιβάσει blocks που λέγονται datagrams από τις πηγές στους δέκτες (Okamoto et al., 2002). Η διεύθυνση IP είναι προσωρινή και εξαρτάται από το δίκτυο όπου ο κινητός κόμβος έχει πρόσβαση αυτή τη στιγμή. Ο κόμβος ίσως συνδεθεί στο Διαδίκτυο μέσω του δικτύου 3G/4G ή του Wi-Fi.

Η παρακολούθηση αυτών των τριών παραμέτρων σε ένα χρονικό πλαίσιο ίσως φανεί χρήσιμο στον καθορισμό εάν εμφανιστεί κάποιος εξαπατητής. Οι χρήστες μπορούν να αλλάζουν πολύ συχνά τη διεύθυνση και το όνομα χρήστη ανάλογα με το δίκτυο που έχει πρόσβαση η συσκευή , επομένως ο χρόνος είναι μια κρίσιμη παράμετρος στο να καθοριστεί εάν τα αλλάζει ο νόμιμος χρήστης ή ένας επιτιθέμενος.

4.2 Κατανεμημένη άρνηση υπηρεσίας (DDoS attacks)

Στην άρνηση υπηρεσίας ο κύριος σκοπός του επιτιθεμένου είναι να αποτρέψει τους νόμιμους χρήστες κινητών να έχουν πρόσβαση στις κυψελοειδείς υπηρεσίες. Η κατανεμημένη άρνηση υπηρεσίας εμφανίζεται όταν επιτίθενται διάφοροι χρήστες στην ασύρματη κυψελοειδή υποδομή ταυτόχρονα (Lau et al., 2000).

Η DDoS είναι μια από τις πιό ισχυρές επιθέσεις που μπορούν να ρίξουν ολόκληρη την υποδομή του δικτύου. Μέσω του DDoS οι διαφορετικοί επιτιθέμενοι μπορούν να στείλουν υπερβολικά στοιχεία στο δίκτυο, περισσότερα από όσα το δίκτυο μπορεί να χειριστεί, με συνέπεια οι άλλοι χρήστες να μην μπορούν να έχουν πρόσβαση στους πόρους του δικτύου (Fenton, 2006). Οι επιθέσεις DDoS στο WCN να εμφανιστούν στις ακόλουθες συνδέσεις της αρχιτεκτονικής:

- κατά τη διάρκεια της επικοινωνίας των χρηστών και του σταθμού βάσης που είναι η πρώτη σύνδεση στην υποδομή.
- κατά τη διάρκεια της επικοινωνίας μεταξύ του GGSN και του κόμβου υποστήριξης GPRS και μεταξύ του SGSN και του Διαδικτύου.
- συγκεκριμένου χρήστης και του υπόλοιπο του κυψελωτού δικτύου.

Μέτρα: Οι αποτελεσματικές ενέργειες για να αποτραπεί η DDoS είναι οι παρακάτω:

1. Αποτρέψτε το να γίνεται δευτεροβάθμιο θύμα: Οι χρήστες κινητών πρέπει να γνωρίζουν το ρόλο τους στη συμμετοχή στην επίθεση DDoS. Είναι σημαντικό να καταλαβαίνουν πώς μπορούν να αποτρέψουν τις συσκευές τους από το να είναι μέρος της επίθεσης. Οι τελικοί χρήστες πρέπει να σιγουρευτούν ότι κανένα πρόγραμμα παρακολούθησης δεν εγκαθίσταται στις συσκευές τους. Σήμερα οι συσκευές παρέχονται συνήθως από τους παρόχους των δικτύων, επομένως επιβάλλουν τις πολιτικές τους από την άποψη των εφαρμογών που επιτρέπονται να μεταφορτωθούν και να εγκατασταθούν (Specht & Lee, 2004).

2. Φιλτράρισμα εξόδου: Ο διακομιστής δικτύου παίζει σημαντικό ρόλο στον προσδιορισμό και την παρεμπόδιση των επιθέσεων ασφάλειας. Με τα διαφορετικά εργαλεία ανάλυσης δικτύων είναι δυνατό να ανιχνευθούν οι επιγραφές πακέτων IP που αφήνουν το δίκτυο. Αναφέραμε πριν ότι κατά τη διάρκεια της επίθεσης εξαπάτησης οι IP της συσκευής θα αλλάξουν και επίσης στην DDoS υπάρχει μεγάλη πιθανότητα να χρησιμοποιηθούν συσκευές εξαπάτησης. Επομένως η τοποθέτηση ενός firewall που θα φιλτράρει όλη την κυκλοφορία που παράγεται από μια συσκευή εξαπάτησης θα βοηθήσει την επίθεση DDoS στο WCN (Distler & Else, 2008).

4.3 Συμφόρηση καναλιού(Jamming attacks)

Η συμφόρηση καναλιού είναι μια τεχνική που χρησιμοποιείται από τους επιτιθεμένους για να προσθέσει θόρυβο ή παρέμβαση μεταξύ των επικοινωνιών των νόμιμων χρηστών στο κυψελωτό δίκτυο (Sampath et al., 2007). Αυτή η επίθεση ίσως πραγματοποιείται στην επικοινωνία μεταξύ:

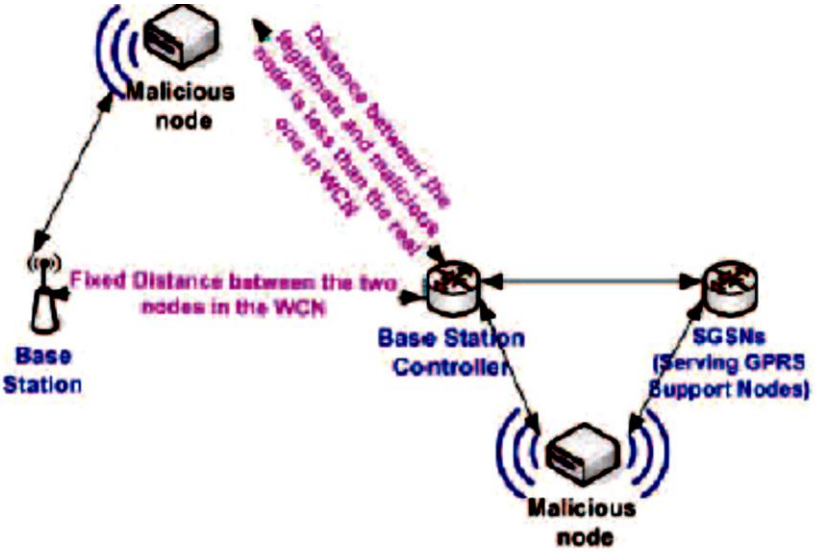
- σταθμού βάσης και ελεγκτή σταθμών βάσης
- ελεγκτή σταθμών βάσης και εν ενεργεία κόμβου υποστήριξης GPRS
- κόμβου υποστήριξης GPRS και GGSN
- GGSN και Διαδικτύου

Μέτρα: Στο WCN ένας jammer είναι μια συσκευή που μπορεί μερικώς ή εξ ολοκλήρου να αναστατώσει έναν σταθμό βάσης ή το σήμα SGSN, με την αύξηση της πυκνότητας φάσματός του (PSD).

Η κακόβουλη συσκευή δεν μπορεί ποτέ να αναπαραγάγει ένα σήμα ούτε μπορεί να προσποιηθεί ότι είναι ένας νόμιμος κόμβο (Mpitziopoulos et al., 2009. Muraleedharan & Osadciw, 2006) όπως περιγράφεται στην εικόνα 5.

Υπάρχουν δύο παράμετροι που πρέπει να εξεταστούν κατά τη διάρκεια αυτής της επίθεσης:

1. Η ισχύς του σήματος μεταξύ δύο κόμβων στο WCN μπορεί να επηρεαστεί από την παρουσία ενός κακόβουλου κόμβου. Κάθε κόμβος στο WCN πρέπει να έχει αρκετές μετρήσεις του επιπέδου θορύβου πριν από το μπλοκάρισμα της επίθεσης έτσι ώστε να είναι εύκολο να ανιχνεύσει έναν κακόβουλο κόμβο. Είναι πολύ δύσκολο για έναν κακόβουλο κόμβο να ενεργήσει ως ένας νόμιμος δεδομένου ότι η ισχύς του θα συγκριθεί με προηγούμενα στατιστικά.
2. Η θέση του κακόβουλου κόμβου είναι μια άλλη παράμετρος που μπορεί να το εκθέσει στο WCN. Δεδομένου ότι ο κακόβουλος κόμβος θα είναι μεταξύ δύο νόμιμων συστατικών του WCN η απόσταση θα είναι πάντα μικρότερη. Εκτός από τους κινητούς κόμβους που είναι τα smartphones, όλο το υπόλοιπο των συστατικών WCN έχει μια σταθερή απόσταση επομένως μεταξύ τους ο προσδιορισμός γίνεται εύκολα και είναι πάντα μεταξύ δύο νόμιμων κόμβων, άρα η απόσταση από τους νόμιμους κόμβους είναι αυτή που θα το εκθέσει στο δίκτυο.



Εικόνα 5: Συμφόρηση καναλιού

4.4 Υποκλοπή(Eavesdropping attacks)

Με βάση τον ορισμό του Wiley, ως υποκλοπή ορίζεται ως μια συμπεριφορά όταν το μήνυμα που προορίζεται για έναν συγκεκριμένο χρήστη στο ασύρματο κυψελωτό δίκτυο παρεμποδίζεται από έναν εισβολέα ή έναν επιτιθέμενο (Peake, 2005). Εάν η επικοινωνία στο WCN δεν κρυπτογραφείται ένας επιτιθέμενος μπορεί να υποκλέψει και να παρεμποδίσει απόρρητη επικοινωνία, όπως εμπιστευτικές κλήσεις, απόρρητα μηνύματα κ.λπ. (Chen & Prasad, 2009). Αυτή η επίθεση μπορεί να πραγματοποιηθεί σε διαφορετικές ασύρματες συνδέσεις μέσω της υποδομής. Στην αρχιτεκτονική μας έχουμε προσδιορίσει αυτές τις επιθέσεις κατά τη διάρκεια της επικοινωνίας μεταξύ:

- των χρηστών και του σταθμού βάσης
- του ελεγκτής σταθμών βάσης και των σταθμών βάσης
- του ελεγκτή σταθμών βάσης και των κόμβων υποστήριξης GPRS
- του Διαδικτύου και των servers

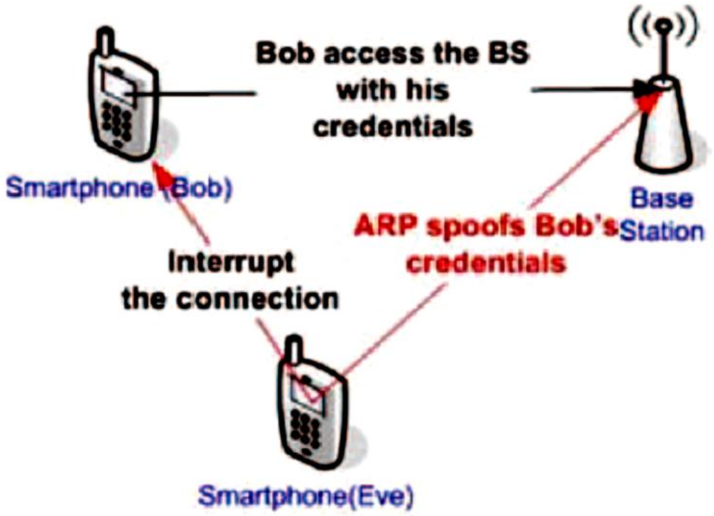
Μέτρα: Υποκλοπή είναι η πράξη του ελέγχου της κυκλοφορίας στο δίκτυο για απλούς κωδικούς πρόσβασης ή πληροφορίες διαμόρφωσης, επομένως η φυσική ασφάλεια του εξοπλισμού είναι σημαντική. Οι ακόλουθες ενέργειες πρέπει να ληφθούν υπόψη για να αποτρέψουν αυτήν την επίθεση:

1. Παροχή φυσικής ασφάλειας για το smartphone με τη δημιουργία κωδικών πρόσβασης για πρόσβαση στη συσκευή. Εάν η συσκευή σας κλαπεί δεν μπορεί να προσεγγιστεί εύκολα εάν ο κλέφτης δεν είναι ειδικευμένος και δεν ξέρει πώς να σπάσει τους κωδικούς στο smartphone.

2. Κατάλληλη τμηματοποίηση του δικτύου (Lin, χ.χ.). Η τμηματοποίηση είναι η διαδικασία διαχωρισμού ορισμένων μερίδων της κίνησης του δικτύου για λόγους απόδοσης και ασφαλείας. Το GGSN είναι αρμόδιο για την αλληλεπίδραση μεταξύ του δικτύου GPRS και των μεταστρεφόμενων δικτύων εξωτερικών πακέτων, όπως το Διαδίκτυο.

4.5 Πειρατεία της συνεδρίας(Hijacking Attacks)

Ένας κακόβουλος κόμβος μπορεί να κάνει πειρατεία σε μια ήδη υπάρχουσα επικοινωνία και μπορεί να ενεργήσει σαν νόμιμος χρήστης του smartphone (Lin, χ.χ.). Ο επιτιθέμενος όπως περιγράφεται στην εικόνα 6 περιμένει έως ότου έχει πρόσβαση ένας νόμιμος χρήστης στο σταθμό βάσης και κλέβει τα πιστοποιητικά του μέσω απατών του ARP. Κατόπιν ο επιτιθέμενος διακόπτει τη σύνδεση του νόμιμου χρήστη και αναλαμβάνει την επικοινωνία με το σταθμό βάσης.



Εικόνα 6: Πειρατεία στη συνεδρία

Μέτρα: Διάφορες ενέργειες μπορούν να ληφθούν υπόψη για να αποτρέψουν την πειρατεία όπως:

1. Η χρήση αλγορίθμου κρυπτογράφησης όπως η RSA, DES, AES_128, SHA και CBA είναι πολύ αποδοτική από την άποψη της κρυπτογράφησης όλων των πληροφοριών που ανταλλάσσονται. Χρησιμοποιώντας ένα δημόσιο κλειδί το απλό κείμενο θα μετατραπεί σε κρυπτογραφημένο και σταλμένο από τον αποστολέα θα

διαβιβαστεί στα κανάλια επικοινωνίας και ο δέκτης θα απαιτήσει ένα ιδιωτικό κλειδί για να το αποκρυπτογραφήσει.

2. Περιορισμός μη απαραίτητων αιτημάτων ARP που μπορούν να εκθέσουν τα πιστοποιητικά των νόμιμων χρηστών. Το πρωτόκολλο ανάλυσης διευθύνσεων μετατρέπει τη διεύθυνση IP στην αντίστοιχη φυσική διεύθυνση δικτύου (MAC). Οι χαρτογραφήσεις των διευθύνσεων IP-MAC προέρχονται από μια προσωρινή μνήμη ARP που διατηρείται σε κάθε συσκευή. Επομένως ένας επιτιθέμενος μπορεί να χρησιμοποιήσει αυτή τη μνήμη για να βρει την IP και τις διευθύνσεις MAC των νόμιμων χρηστών και να κάνει δικά του τα πιστοποιητικά τους.

4.6 Παραποίηση Μηνυμάτων(Message Forgery Attacks)

Η παραποίηση μηνυμάτων πραγματοποιείται όταν μπορεί να αρχίσει ένας επιτιθέμενος να παράγει παραποιημένα μηνύματα που δείχνουν ότι υπάρχει πρόβλημα σε πύλες ή servers του δικτύου. Όταν αυτό το πλαστό πρόβλημα τραβήξει την προσοχή των διακομιστών και προσπαθήσουν να το διορθώσουν, οι επιτιθέμενοι θα προσπαθήσουν να εκθέσουν άλλα μέρη της υποδομής (Hwang et al, 2002). Εάν το κανάλι επικοινωνίας δεν κρυπτογραφείται, ένας επιτιθέμενος μπορεί να παρεμποδίσει τα μηνύματα και στις δυο κατευθύνσεις και να αλλάξει το περιεχόμενο χωρίς να το γνωρίζουν οι χρήστες (Venkataram, 2010). Αυτή η επίθεση μπορεί να γίνει σε όλα τα μέρη του κυψελωτού δικτύου και συγκεκριμένα:

- στην επικοινωνία μεταξύ της συσκευής και του σταθμού βάσης.
- στην επικοινωνία μεταξύ του ελεγκτή σταθμών βάσης και των σταθμών βάσης.
  στην επικοινωνία μεταξύ του ελεγκτή σταθμών βάσης και του SGSN και του κόμβου υποστήριξης πυλών GPRS.
- στην επικοινωνία μεταξύ του GPRS και του Διαδικτύου.

Μέτρα: Οι ακόλουθες ενέργειες πρέπει να ληφθούν προκειμένου να αποτραπεί η επίθεση παραποίησης μηνυμάτων στο WCN:

1. Επικύρωση όλων των συσκευών που έχουν πρόσβαση στο δίκτυο (Meier et al., 2006). Όλες οι συσκευές smartphone πρέπει να επιβεβαιώσουν την ταυτότητά τους με το WCN. Όπως αναφέρεται ανωτέρω στην επίθεση απάτης τρεις παράμετροι χρησιμοποιούνται για την επικύρωση μιας συσκευή smartphone, η διεύθυνση MAC,

το όνομα χρήστη και η διεύθυνση IP. Οι πρώτες δύο παράμετροι είναι μόνιμες επομένως χρησιμοποιώντας τες η επικύρωση πραγματοποιείται στο HLR.

2. Κρυπτογράφηση στοιχείων πριν σταλθούν.

3. Η μείωση του διαλείμματος της συνεδρίας μπορεί να αποτρέψει τους επιτιθεμένους από την αλλαγή των μηνυμάτων (Meier et al., 2006). Λιγότερος χρόνος αφήνεται σε κάθε συσκευή για πρόσβαση στις υπηρεσίες του WCN και αυτό μπορεί να ελαχιστοποιήσει τον κίνδυνο για επίθεση και επιβεβαιώνει ότι η συσκευή είναι νόμιμη. Κάθε φορά που επιτυγχάνεται αυτό το διάλειμμα η συσκευή πρέπει να επικυρωθεί προκειμένου να συνεχιστεί με τις υπηρεσίες στο WCN.

4.7 Επανάληψη Μηνυμάτων(Message Reply Attacks)

Η επανάληψη μηνυμάτων συμβαίνει όταν ένας επιτιθέμενος προσπαθεί να επαναλάβει τα μηνύματα προκειμένου να κλαπεί μια συνεδρία από έναν χρήστη smartphone. Αυτή η επίθεση ίσως εμφανιστεί στην επικοινωνία μεταξύ:

- Smartphone και σταθμού βάσης
- Κόμβου υποστήριξης πύλης GPRS και διαδικτύου

Μέτρα: Στην επίθεση επανάληψης μηνυμάτων ο εισβολέας συλλαμβάνει και αντιγράφει το μήνυμα και το επαναλαμβάνει στο δέκτη παριστάνοντας τον αποστολέα. Οι ακόλουθες ενέργειες πρέπει να γίνουν προκειμένου να αποτραπεί ή να ελαχιστοποιηθεί αυτή η επίθεση:

1. Κρυπτογράφηση SSL στο κανάλι επικοινωνίας (Meier et al., 2006): Οι περισσότεροι από τους χρήστες smartphone εγκαθιστούν τις εφαρμογές στις συσκευές τους για να χρησιμοποιήσουν το συγκεκριμένο λογισμικό. Αντί να μπαίνουν στο Facebook, το Twitter κλπ μέσω του πρωτοκόλλου HTTP που δεν έχει αλγορίθμους κρυπτογράφησης, το HTTPS πρέπει να είναι απαραίτητο.

2. Η εστίαση του επιτιθεμένου είναι το μήνυμα που ανταλλάσσεται επομένως η κατοχή ενός μοναδικού προσδιοριστικού θα το καταστήσει ευκολότερο να προσδιοριστεί εάν το μήνυμα έχει επαναληφθεί ή όχι (Meier et al., 2006).

4.8 Επίθεση «Άνθρωπος στη μέση»(Man in the Middle attacks)

Η επίθεση επιτρέπει σε έναν εισβολέα να παραστήσει έναν έγκυρο σταθμό βάσης σε έναν συνδρομητή ανεξάρτητα από το αν η επικύρωση και η βασική συμφωνία χρησιμοποιούνται (Meyer & Wetzel, 2004). Ένας επιτιθέμενος μπορεί να βρεθεί μεταξύ των μηνυμάτων ενός smartphone και των σταθμών βάσης και να παρεμποδίσει τα μηνύματα μεταξύ τους και να τα αλλάξει.

Μέτρα: Ο προσδιορισμός που βασίζεται στο αποτύπωμα ραδιοσυχνότητας είναι μια αποδοτική τεχνική για να προσδιοριστεί ένας εισβολέας στην επικοινωνία μεταξύ του σταθμού βάσης και του smartphone. Το αποτύπωμα RF αποτελείται από τη λαμβανόμενη ισχύ ενός σήματος στην συγκεκριμένη συχνότητα (Kent & Atkinson, χ.χ.). Επειδή η θέση του σταθμού βάσης είναι γνωστή και στατική και καθένας τους έχει ένα μοναδικό αποτύπωμα RF μπορεί να χρησιμοποιηθεί για να διαφοροποιήσει τους νόμιμους σταθμούς βάσης. Είναι πολύ δύσκολο να κλωνοποιηθεί το αποτύπωμα RF επομένως αυτό είναι μια αποτελεσματική λύση για να αποτραπεί αυτού του είδους η επίθεση στο WCN.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Παρουσιάστηκαν οκτώ είδη επιθέσεων στα κυψελωτά δίκτυα και τα αντίστοιχα μέτρα. Όλα τα συστατικά της αρχιτεκτονικής του WCN κινδυνεύουν να δεχθούν επιθέσεις ασφάλειας, αλλά τα πιο συνηθισμένα είναι οι κινητοί κόμβοι, τα smartphones και σταθμοί βάσης. Τα πιστοποιητικά συσκευών και τα υπερβολικά αιτήματα ARP μπορούν να οδηγήσουν σε διαφορετικές επιθέσεις ασφάλειας όπως υποκλοπές ή πειρατεία. Οι αλγόριθμοι κρυπτογράφησης, τα ασφαλή κανάλια επικοινωνίας, το αποτύπωμα ραδιοσυχνότητας, η επικύρωση, η κατάλληλη τμηματοποίηση του δικτύου, η χρήση μοναδικού προσδιοριστικού μηνυμάτων, το φιλτράρισμα της εξόδου και η ισχύς των σημάτων είναι μερικά από τα μέτρα που θα αποτρέψουν τις επιθέσεις. Μελλοντικά θα μπορούσαν να πραγματοποιηθούν πειράματα σε 4 διαφορετικές πλατφόρμες Smartphone όπως είναι τα Android, Blackberry, I-Phone και Windows phone αναλύοντας τα πακέτα που συλλαμβάνονται.

6. ΑΝΑΦΟΡΕΣ – ΒΙΒΛΙΟΓΡΑΦΙΑ

Attacks. Systems, Man, and Cybernetics, *2000 IEEE International Conference, 3*, pp. 2275 – 2280.

Aristides Mpitziopoulos, Damianos Gavalas,Charalampos Konstantopoulos, and Grammati Pantziou,A Survey on Jamming Attacks and Countermeasures in WSNs, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 4, FOURTH QUARTER 2009.

Beaubrun, R., Moulin, B. & Jabeur, N. (2007). “An Architecture for Delivering”.

Chen, K. C. & Prasad, R. (2009). *Cognitive Radio Networks*. John Wiley & Sons.

Distler, d. & Esler, J. (2008). *Performing Egress Filtering*, SANS Institute InfoSec Reading Room.

Felten, E. W., Balfanz, D., Dean, D. & Wallach, D. S. (1997). Web Spoofing: An Internet Con Game. *Technical Report*, 540–96.

Fenton J., (2006). *Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)*, Cisco Systems Inc..

Hwang M., Lee Ch. & Tang Y., (2002). "A Simple Remote User Authentication Scheme." *Mathematical and Computer Modelling*, 36, pp. 103-107.

Kent and Atkinson, *Security Architecture for the Internet Protocol*.

Kurose, J. F. & Ross, K. W. (2009). *Computer Networking A Top-Down Approach*, Addison Wesley.

Lau F., Rubin S., Smith M. & Trajkovic L., (2000). Distributed Denial of Service

Specht, S. M. & Lee, R. B. (2004). Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems*, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550.

Lin, M. *An Overview of Session Hijacking at the Network and Application Levels*, SANS Institute InfoSec Reading Room.

Location-Based Services,” *IJCSNS International Journal of Computer Science and Network Security, 7* (7).

Meier, J.D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. and Murukan, A. (2006). *Improving Web Application Security: Threats and Countermeasures*, Microsoft Corporation.

Meyer U., Wetzel S., (2004). "A man-in-the-middle attack on UMTS". *Proceeding WiSe '04 Proceedings of the 3rd ACM workshop on Wireless security*, ACM New York.

Microsoft Tag, (2012). *Mobile statistics and facts*.

Muraleedharan, R. & Osadciw, L. A. (2006). *Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System*, SPIE.

Peake, T. M. (2005). *Eavesdropping in communication networks*. Cambridge University Press, University of Copenhagen.

Phelps, T. (2012). To Root or Not to Root.

Plummer, D. C. (1982). An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses, *RFC 826*.

Smith, A. (2012). *A Look at Internet Use on Mobile Phones,* PewResearchCenter Publications.

Okamoto, O., Maruyama, M. & Sajima, T. (2002). Forwarding Media Access Control (MAC) Frames over Multiple Access Protocol over Synchronous Optical Network/Synchronous Digital Hierarchy (MAPOS), *NTT Laboratories and Sun Microsystems*.

Sampath, A., Hui Dai, Haitao Zheng, Zhao, B.Y. (2007). “Multichannel Jamming Attacks using Cognitive Radios. Computer Communications and Networks”. *Proceedings of 16th International Conference on Digital Object Identifier*. pp. 352 – 357.

Tode, C. (2012). *25pc of mobile users shop online only via a smartphone or tablet: study*, Mobile Commerce Daily.

Venkataram, (2010). Wireless & Mobile N/W Security. Tata McGraw-Hill Education.