ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΩΝ ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Θέμα: **Ασφάλεια στα δίκτυα 5G**

Κατέβας Χρήστος - p18068
7ο εξάμηνο
Κινητές και ασύρματες επικοινωνίες
Επιβλέπων Καθηγητής Δημήτριος Βέργαδος

ΕΙΣΑΓΩΓΗ

Τα προηγμένα χαρακτηριστικά των 5G (5ης γενιάς) συστημάτων ασύρματου δικτύου παρέχουν νέες απαιτήσεις ασφάλειας και προκλήσεις. Αυτή η εργασία παρουσιάζει μία μελέτη για την ασφάλεια των συστημάτων ασύρματου δικτύου 5G σε σύγκριση με τα παραδοσιακά (κυψελοειδή) δίκτυα. Η εργασία ξεκινά με μια κριτική για ασύρματα δίκτυα, 5G ιδιαιτερότητες καθώς και σχετικά με τις νέες απαιτήσεις και τα κίνητρα της ασύρματης ασφάλειας 5G. Το δυναμικό, οι επιθέσεις και οι υπηρεσίες ασφαλείας συνοψίζονται με την εξέταση των νέων απαιτήσεων της υπηρεσίας και της “νέας” χρήσης στα ασύρματα δίκτυα 5G. Η πρόσφατη ανάπτυξη και τα υπάρχοντα σχήματα για την ασύρματη ασφάλεια 5G παρουσιάζονται με βάση τις αντίστοιχες υπηρεσίες ασφαλείας, όπως έλεγχο ταυτότητας, διαθεσιμότητα, εμπιστευτικότητα δεδομένων, διαχείριση κλειδιών και απόρρητο. Αυτό το κείμενο ασχολείται περαιτέρω με τα νέα χαρακτηριστικά ασφαλείας που αφορούν διαφορετικές τεχνολογίες που εφαρμόζονται σε 5G, όπως ετερογενή δίκτυα, επικοινωνίες από συσκευή σε συσκευή, τεράστια δίκτυα πολλαπλών εισόδων πολλαπλών εξόδων, καθορισμένα από λογισμικό και Internet of Things. Με κίνητρο από αυτές τις δραστηριότητες έρευνας και ανάπτυξης ασφάλειας, προτείνουμε μια νέα αρχιτεκτονική ασύρματης ασφάλειας 5G, με βάση την οποία παρέχεται η ανάλυση διαχείρισης ταυτότητας και ευέλικτου ελέγχου ταυτότητας. Ως μελέτη περίπτωσης, διερευνούμε μια διαδικασία παράδοσης καθώς και ένα σχήμα φόρτωσης σηματοδότησης για να δείξουμε τα πλεονεκτήματα της προτεινόμενης αρχιτεκτονική ασφάλειας.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Συστήματα ασύρματου δικτύου 5G, ασφάλεια, έλεγχος ταυτότητας, διαθεσιμότητα, εμπιστευτικότητα, κλειδί διαχείριση, προστασία της ιδιωτικής ζωής, ετερογενή δίκτυα, επικοινωνίες μεταξύ συσκευών, τεράστια πολλαπλή είσοδος δίκτυα πολλαπλών εξόδων, καθορισμένα από λογισμικό, Internet of Things, αρχιτεκτονική ασύρματης ασφάλειας 5G

ΕΙΣΑΓΩΓΗ

Τα ασύρματα συστήματα 5ης γενιάς, ή 5G, είναι οι κινητές ασύρματες τηλεπικοινωνίες επόμενης γενιάς πέρα από τα τρέχοντα 4G / International Mobile Telecommunications (IMT) - Advanced Systems . Το ασύρματο σύστημα 5G δεν είναι μόνο μια εξέλιξη των παλαιών κυψελοειδών δικτύων 4G, αλλά και του συστήματος με πολλές νέες δυνατότητες υπηρεσίας . Η έρευνα και ανάπτυξη 5G στοχεύουν σε διάφορα προηγμένα χαρακτηριστικά, όπως υψηλότερη χωρητικότητα από τα τρέχοντα 4G, υψηλότερη πυκνότητα κινητών ευρυζωνικών χρηστών και υποστήριξη επικοινωνιών μεταξύ συσκευών (D2D) και μαζικών επικοινωνιών τύπου μηχανής . Ο προγραμματισμός 5G στοχεύει επίσης σε χαμηλότερο λανθάνοντα χρόνο και χαμηλότερη κατανάλωση ενέργειας, για καλύτερη εφαρμογή του Internet of Things (IoT) . Πιο συγκεκριμένα, υπάρχουν οκτώ προηγμένες δυνατότητες ασύρματων συστημάτων 5G, συνδέσεις 1-10 Gbps με τελικά σημεία στο πεδίο, καθυστέρηση 1 χιλιοστών του δευτερολέπτου, εύρος ζώνης 1000x ανά μονάδα, αριθμός συνδεδεμένων συσκευών 10-100x, διαθεσιμότητα 99,999%, κάλυψη 100% , 90% μείωση της χρήσης ενέργειας δικτύου και διάρκεια ζωής μπαταρίας έως και δέκα ετών για συσκευές χαμηλής ισχύος. Για την επίτευξη αυτών των απαιτήσεων απόδοσης, εφαρμόζονται διάφορες τεχνολογίες σε συστήματα 5G, όπως ετερογενή δίκτυα (HetNet), τεράστια πολλαπλή έξοδος πολλαπλών εξόδων (MIMO), χιλιοστόμετρο (mmWave), επικοινωνίες D2D
, δίκτυο καθορισμένου λογισμικού (SDN), οπτικοποίηση λειτουργιών δικτύου (NFV) και τεμαχισμός δικτύου. Η διαδικασία τυποποίησης για ασύρματα συστήματα 5G είναι ακριβώς στην αρχή. Τα ασύρματα συστήματα 5G μπορούν να παρέχουν όχι μόνο παραδοσιακές επικοινωνίες φωνής και δεδομένων, αλλά και πολλές νέες περιπτώσεις χρήσης, νέες εφαρμογές στον κλάδο, καθώς και πολλές συσκευές και εφαρμογές για τη σύνδεση της κοινωνίας γενικότερα . Προσδιορίζονται διαφορετικές περιπτώσεις χρήσης 5G, όπως επικοινωνία μεταξύ οχημάτων και οχημάτων προς υποδομή, βιομηχανικός αυτοματισμός, υπηρεσίες υγείας, έξυπνες πόλεις, έξυπνα σπίτια και ούτω καθεξής . Πιστεύεται ότι τα ασύρματα συστήματα 5G μπορούν να βελτιώσουν τις ευρυζωνικές κινητές συσκευές με κρίσιμες υπηρεσίες και τεράστιο IoT . Η νέα αρχιτεκτονική, οι νέες τεχνολογίες και οι νέες περιπτώσεις χρήσης σε ασύρματα συστήματα 5G θα φέρουν νέες προκλήσεις στην ασφάλεια και την προστασία της ιδιωτικής ζωής .

Λόγω της φύσης της μετάδοσης και του περιορισμένου εύρους ζώνης των ασύρματων επικοινωνιών, είναι πιθανό αλλά δύσκολο να παρέχονται δυνατότητες ασφαλείας όπως έλεγχος ταυτότητας, ακεραιότητα και εμπιστευτικότητα. Υπάρχουν διάφορα ζητήματα ασφάλειας στα τρέχοντα κυτταρικά δίκτυα στο επίπεδο ελέγχου πρόσβασης πολυμέσων (MAC) και στο φυσικό επίπεδο (PHY) όσον αφορά τις πιθανές επιθέσεις, τις βουλκανιές και τις ανησυχίες περί απορρήτου. Τα προστατευτικά ασφαλείας της φωνής και των δεδομένων παρέχονται βασισμένα σε παραδοσιακές αρχιτεκτονικές ασφαλείας με χαρακτηριστικά ασφαλείας όπως διαχείριση ταυτότητας χρήστη, αμοιβαίοι έλεγχοι ταυτότητας μεταξύ του δικτύου και του εξοπλισμού χρήστη (UE), ασφαλές κανάλι επικοινωνίας και ούτω καθεξής. Στα παλαιά κυψελοειδή δίκτυα - Long Term Evolution (LTE), παρέχεται υψηλό επίπεδο ασφάλειας και αξιοπιστίας για τους χρήστες και τους φορείς εκμετάλλευσης δικτύων . Εκτός από την κρυπτογράφηση της κίνησης χρηστών, επιτυγχάνεται αμοιβαίος έλεγχος ταυτότητας μεταξύ ενός UE και ενός σταθμού βάσης. Επιπλέον, η ασφάλεια της πρόσβασης και της διαχείρισης της κινητικότητας του LTE διασφαλίζεται από μια βασική ιεραρχία και έναν μηχανισμό διαχείρισης κλειδιών . Υπάρχουν επίσης ερευνητικές εργασίες σχετικά με την ασφάλεια που σχετίζονται με τις τεχνολογίες που εφαρμόζονται στο LTE . Ωστόσο, απαιτούνται νέες απαιτήσεις ασφαλείας για την υποστήριξη ποικίλων νέων περιπτώσεων χρήσης και των νέων παραδειγμάτων δικτύωσης . Οι μηχανισμοί ασφαλείας είναι απαραίτητοι για να συμμορφωθούν με τα συνολικά προηγμένα χαρακτηριστικά 5G, όπως χαμηλό επίπεδο και υψηλή ενεργειακή απόδοση (EE) . Επιπλέον, σε αντίθεση με τα παλαιά κυψελοειδή δίκτυα, τα ασύρματα δίκτυα 5G θα είναι προσανατολισμένα στις υπηρεσίες, τα οποία έχουν ιδιαίτερη έμφαση στις απαιτήσεις ασφάλειας και απορρήτου από την άποψη των υπηρεσιών.

Οι νέες περιπτώσεις χρήσης μπορούν να έχουν μια ποικιλία συγκεκριμένων απαιτήσεων, όπως εξαιρετικά χαμηλός λανθάνων χρόνος στις επικοινωνίες χρηστών. Οι νέες τεχνολογίες όχι μόνο αποδίδουν προηγμένες δυνατότητες εξυπηρέτησης αλλά και ανοιχτές πόρτες για ευπάθειες και επιβάλλουν νέες απαιτήσεις ασφαλείας στο 5G . Στο HetNet, διαφορετικές τεχνολογίες πρόσβασης ενδέχεται να έχουν διαφορετικές απαιτήσεις ασφάλειας και περιβάλλον πολλαπλών δικτύων η εφαρμογή ενδέχεται να απαιτεί συχνές επαληθεύσεις ταυτότητας με περιορισμούς αυστηρής καθυστέρησης . Το MIMO θεωρείται μια σημαντική τεχνική 5G για την επίτευξη υψηλότερης φασματικής αποδοτικότητας και ενεργειακής απόδοσης. Θεωρείται επίσης ως πολύτιμη τεχνική κατά της παθητικής υποκλοπής. Επιπλέον, τα SDN και NFV σε 5G θα υποστηρίξουν νέα μοντέλα παροχής υπηρεσιών και συνεπώς απαιτούν νέα χαρακτηριστικά ασφαλείας . Με την έλευση των παραδειγμάτων δικτύωσης 5G, απαιτείται μια νέα αρχιτεκτονική ασφάλειας . Για την αντιμετώπιση αυτών των ζητημάτων, η ασφάλεια πρέπει να θεωρηθεί ως αναπόσπαστο μέρος της συνολικής αρχιτεκτονικής και θα πρέπει να ενσωματωθεί στην σχεδίαση του συστήματος από την αρχή. Για την υποστήριξη διάφορων περιπτώσεων χρήσης και νέων μοντέλων εμπιστοσύνης με τον βέλτιστο τρόπο, χρειάζονται ευέλικτοι μηχανισμοί ασφαλείας. Τα μοντέλα αξιοπιστίας των παλαιών κυψελοειδών δικτύων και των ασύρματων δικτύων 5G. Απαιτούνται έλεγχοι ταυτότητας όχι μόνο μεταξύ των συνδρομητών και των δύο φορέων εκμετάλλευσης (τα οικιακά δίκτυα και τα δίκτυα εξυπηρέτησης), αλλά και μεταξύ των συμβαλλομένων υπηρεσιών σε δίκτυα χωρίς καλώδια 5G. Επιπλέον, για την περίπτωση χρήσης κάθετων βιομηχανιών, οι απαιτήσεις ασφαλείας μπορεί να διαφέρουν σημαντικά μεταξύ διαφορετικών εφαρμογών. Για παράδειγμα, οι κινητές συσκευές απαιτούν μηχανισμούς ασφαλείας ελαφρού βάρους ως περιορισμό των πόρων ισχύος, ενώ οι υπηρεσίες υψηλής ταχύτητας απαιτούν αποτελεσματικές υπηρεσίες ασφαλείας με χαμηλό λανθάνοντα χρόνο. Επομένως, η γενική ευελιξία για τους μηχανισμούς ασφαλείας 5G είναι μια άλλη βασική απαίτηση . Η διαχείριση ελέγχου ταυτότητας στο 5G είναι πιο περίπλοκη λόγω διαφορετικών τύπων και ενός τεράστιου αριθμού συσκευών που συνδέονται. Για διαφορετικές εφαρμογές, μπορούν να εφαρμοστούν διαφορετικά μοντέλα ελέγχου ταυτότητας. ο έλεγχος ταυτότητας χρήστη μπορεί να αφαιρεθεί από τον πάροχο δικτύου, ή από τον πάροχο υπηρεσιών ή από τον άλλο. Εκτός από την απαίτηση ευελιξίας της ασφάλειας 5G, ο αυτοματισμός ασφάλειας είναι επίσης βασικό στοιχείο. Συνδυάζει την αυτοματοποιημένη διαχείριση ασφάλειας με αυτοματοποιημένους και έξυπνους ελέγχους ασφάλειας . Δεδομένου ότι περισσότερες προσωπικές πληροφορίες χρησιμοποιούνται σε διάφορες εφαρμογές, όπως η παρακολούθηση που εφαρμόζεται σε ασύρματα δίκτυα άνω των 5G, οι ανησυχίες σχετικά με το απόρρητο κλιμακώνονται. Επιπλέον, διάφορες υπηρεσίες στο 5G μπορούν να συνδεθούν πιο κοντά από πριν. Ως παράδειγμα, η σταθερή τηλεφωνική γραμμή, η πρόσβαση στο Διαδίκτυο και η τηλεοπτική υπηρεσία μπορούν να τερματιστούν ταυτόχρονα λόγω της διακοπής λειτουργίας ενός μεγάλου δικτύου . Επομένως, απαιτείται αυτοματοποίηση ασφαλείας για να καταστεί το σύστημα 5G ισχυρό έναντι διαφόρων επιθέσεων ασφαλείας.

Οι επιθέσεις ασφαλείας μπορούν να ταξινομηθούν σε 2 τύπους, δηλαδή στις παθητικές επιθέσεις και στις ενεργές επιθέσεις . Σε μία παθητική επίθεση, οι εισβολείς προσπαθούν να μάθουν ή να χρησιμοποιήσουν τις πληροφορίες από τους νόμιμους χρήστες, αλλά δεν σκοπεύουν να επιτεθούν στην ίδια την επικοινωνία. Οι δημοφιλείς παθητικές επιθέσεις σε ένα κυψελοειδές δίκτυο είναι δύο είδη, δηλαδή η υποκλοπή και η ανάλυση της κυκλοφορίας. Οι παθητικές επιθέσεις στοχεύουν στην παραβίαση της εμπιστευτικότητας των δεδομένων και του απορρήτου των χρηστών. Σε αντίθεση με τις παθητικές επιθέσεις, στις ενεργές επιθέσεις, οι επιτιθέμνοι μπορεί να τροποποιήσουν τα δεδομένα ή να στοχεύσουν στη διακοπή των επικοινωνιών. Οι τυπικές ενεργές επιθέσεις περιλαμβάνουν επίθεση man-in-the-middle (MITM), επίθεση επανάληψης, επίθεση άρνησης εξυπηρέτησης (DoS) και επίθεση άρνησης υπηρεσίας (DDoS).

Οι μηχανισμοί που χρησιμοποιούνται για την αντιμετώπιση επιθέσεων ασφαλείας μπορούν ουσιαστικά να χωριστούν σε δύο κατηγορίες: κρυπτογραφικές προσεγγίσεις με νέα πρωτόκολλα δικτύωσης και

προσεγγίσεις φυσικού επιπέδου ασφάλειας (PLS). Οι κρυπτογραφικές τεχνικές είναι οι πιο συχνά χρησιμοποιούμενοι μηχανισμοί ασφαλείας, οι οποίοι αναπτύσσονται κανονικά στα ανώτερα επίπεδα των ασύρματων δικτύων 5G με νέα πρωτόκολλα δικτύωσης. Η σύγχρονη κρυπτογραφία αποτελείται από κρυπτογραφία συμμετρικού κλειδιού και κρυπτογραφία δημόσιου κλειδιού. Η κρυπτογραφία συμμετρικού κλειδιού αναφέρεται στις μεθόδους κρυπτογράφησης στις οποίες μοιράζεται ένα μυστικό κλειδί μεταξύ ενός αποστολέα και ενός παραλήπτη. Η κρυπτογραφία δημόσιου κλειδιού ή η ασύμμετρη κρυπτογραφία χρησιμοποιεί δύο διαφορετικά κλειδιά, το ένα χρησιμοποιείται ως δημόσιο κλειδί για κρυπτογράφηση και το άλλο χρησιμοποιείται ως μυστικό κλειδί για την αποκρυπτογράφηση. Η απόδοση μιας υπηρεσίας ασφαλείας εξαρτάται από το μήκος κλειδιού και την υπολογιστική πολυπλοκότητα των αλγορίθμων. Η διαχείριση και η διανομή των ασύμμετρων κλειδιών προστατεύονται καλά στα παραδοσιακά κυτταρικά δίκτυα. Λόγω πιο περίπλοκων πρωτοκόλλων και ετερογενών αρχιτεκτονικών δικτύων στο 5G, η διαχείριση και η διανομή συμμετρικών κλειδιών ενδέχεται να αντιμετωπίσουν νέες προκλήσεις .

Λόγω της περιορισμένης προόδου όσον αφορά τους πρακτικούς κωδικούς ασύρματης σύνδεσης και σε αυστηρά θετική ικανότητα απορρήτου στις δεκαετίες του 1970 και του 1980, η εφαρμογή του PLS παρεμποδίστηκε. Εκείνη την εποχή, τα περισσότερα σύγχρονα συστήματα ασφαλείας υιοθέτησαν την κραυγή-δημογραφία δημόσιου κλειδιού . Το ενδιαφέρον για τη χρήση του PLS γρήγορα τοποθετήθηκε μετά απέδειξε ότι εξακολουθεί να είναι δυνατό για έναν νόμιμο χρήστη με ένα χειρότερο κανάλι από το υποκλοπές να δημιουργεί ένα κρυφό κλειδί σε ένα μη ασφαλές δημόσιο κανάλι. Έχουν γίνει εκτενείς έρευνες PLS πρόσφατα σε ασύρματα συστήματα 5G. Σε αντίθεση με τις συμβατικές προσεγγίσεις που παρέχουν ασφάλεια κυρίως μέσω κρυπτογραφικών τεχνικών, το PLS αναγνωρίζεται ως μια πολλά υποσχόμενη στρατηγική ασφάλειας για την παροχή ασφαλών ασύρματων μεταφορών αξιοποιώντας τα μοναδικά χαρακτηριστικά ασύρματων φυσικών παικτών . Σε σύγκριση με την κρυπτογραφία, το PLS δείχνει πλεονεκτήματα σε δύο πτυχές, δηλαδή, τη χαμηλή υπολογιστική πολυπλοκότητα και την υψηλή επεκτασιμότητα, που καθιστούν την υποψήφια τεχνική PLS υποψήφια τεχνική για κρυπτογραφική κατανομή κλειδιών σε ασύρματα δίκτυα 5G.

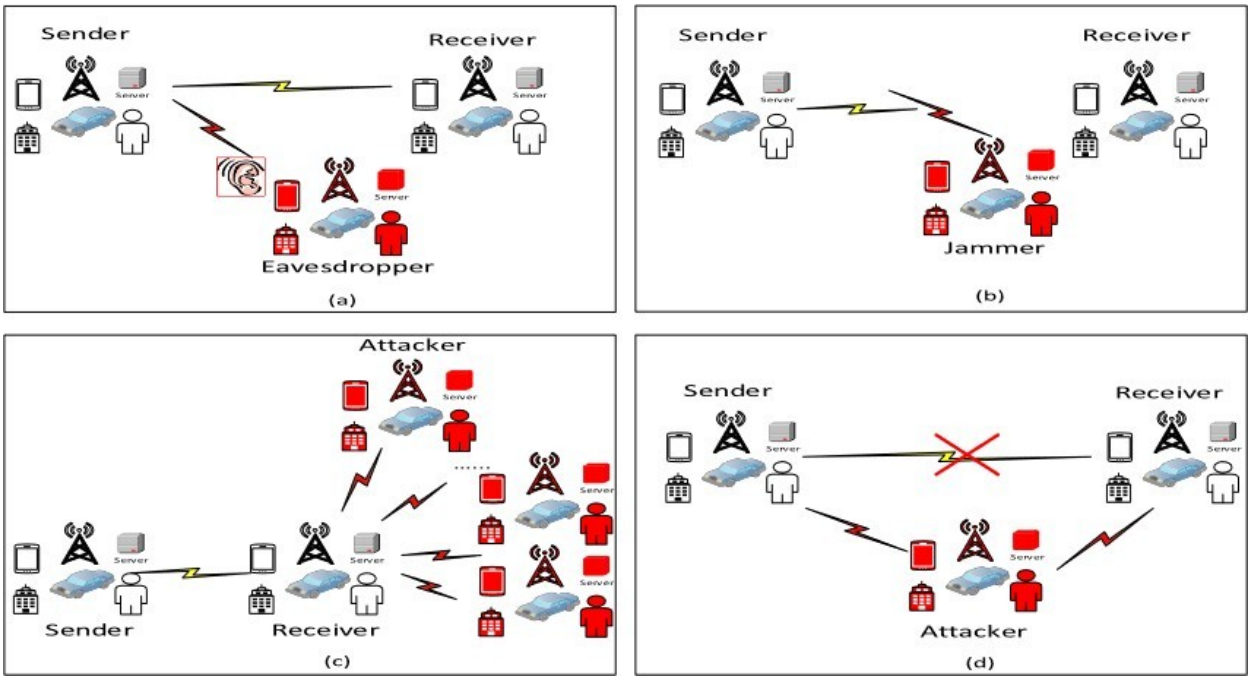
Εκτός από το PLS και τις κρυπτογραφικές τεχνικές, υπήρξαν κάποιες ερευνητικές εργασίες σχετικά με την αρχιτεκτονική ασφάλειας , τους μηχανισμούς αξιολόγησης ευπάθειας και τους μηχανισμούς ανίχνευσης εισβολής βάσει ανάλυσης δεδομένων . Οι μηχανισμοί ασφαλείας πρέπει να συμμορφώνονται με τις απαιτήσεις απόδοσης 5G, όπως εξαιρετικά χαμηλός λανθάνων χρόνος και υψηλός βαθμός ΕΕ. Επομένως, οι απαιτήσεις ασφαλείας 5G πρέπει να λάβουν υπόψη τις λειτουργίες ασφαλείας παλαιού τύπου, τις νέες περιπτώσεις χρήσης και τα νέα πρότυπα δικτύωσης συνολικά. Το Edge cloud εφαρμόζεται για τη βελτίωση της απόδοσης του δικτύου μειώνοντας την καθυστέρηση επικοινωνίας.

ΚΕΦΑΛΑΙΟ 1 / ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ

Λόγω της φύσης μετάδοσης του ασύρματου μέσου, η ασύρματη μετάδοση πληροφοριών είναι ευάλωτη σε διάφορες κακόβουλες απειλές. Σε αυτήν την ενότητα, συζητάμε τέσσερις τύπους επιθέσεων, δηλ. Υποκλοπές και ανάλυση κυκλοφορίας, μπλοκάρισμα, DoS και DDoS και MITM, σε ασύρματα δίκτυα 5G. Επιπλέον υπάρχουν τέσσερις υπηρεσίες ασφαλείας, όπως έλεγχο ταυτότητας, εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα.

Α. ΕΠΙΘΕΣΕΙΣ ΣΕ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΑ 5G

Το παρακάτω σχήμα απεικονίζει και τις τέσσερις επιθέσεις, καθεμία από τις οποίες συζητείται ξεχωριστά στις ακόλουθες παραγράφους, τον τύπο της επίθεσης (παθητική ή ενεργή), τις υπηρεσίες ασφαλείας που παρέχονται για την καταπολέμηση αυτής της επίθεσης και τις αντίστοιχες μεθόδους που εφαρμόζονται για την αποφυγή ή την πρόληψη αυτής της επίθεσης. Επικεντρωνόμαστε στις επιθέσεις ασφαλείας στο επίπεδο PHY και στο επίπεδο MAC, όπου οι βασικές διαφορές στην ασφάλεια μεταξύ ασύρματου και καλωδίου δικτύου (Eavesdropper, Jamming, DdoS, MITM).



1 EAVESDROPPING AND TRAFFIC ANALYSIS

Το Eavesdropping είναι μια επίθεση που χρησιμοποιείται από έναν μη σκόπιμο παραλήπτη για να υποκλέψει ένα μήνυμα από άλλους. Η υποκλοπή είναι μια παθητική επίθεση καθώς η κανονική επικοινωνία δεν επηρεάζεται από την υποκλοπή, όπως φαίνεται στο σχήμα. Λόγω της παθητικότητας, είναι δύσκολο να εντοπιστεί η υποκλοπή. Η κρυπτογράφηση των σημάτων μέσω του ραδιοφωνικού συνδέσμου εφαρμόζεται πιο συχνά για την καταπολέμηση της επίθεσης που παρακολουθεί. Ο υποκλοπής δεν μπορεί να παρακολουθήσει το ληφθέν σήμα απευθείας λόγω της κρυπτογράφησης. Η

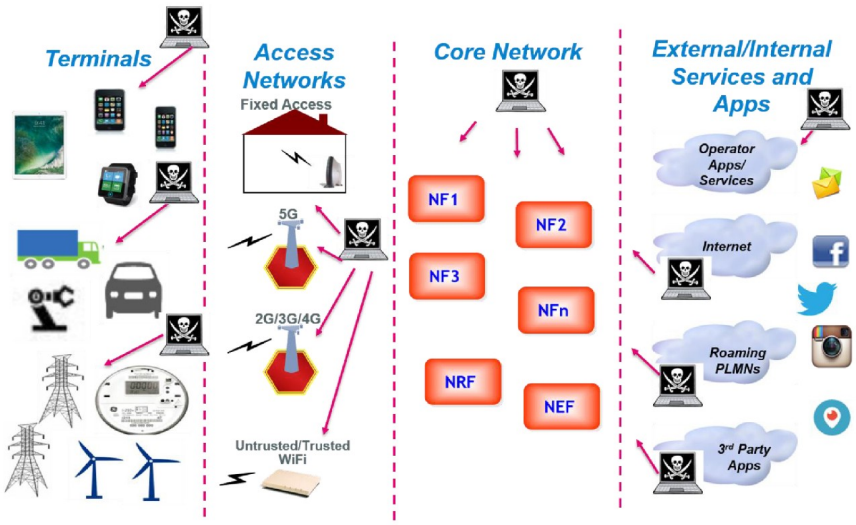
ανάλυση κυκλοφορίας είναι μια άλλη παθητική επίθεση που χρησιμοποιεί ένας ακούσιος δέκτης για να υποκλέψει πληροφορίες όπως η τοποθεσία και η ταυτότητα των μερών επικοινωνίας, αναλύοντας την κίνηση του λαμβανόμενου σήματος χωρίς να κατανοήσει το περιεχόμενο του ίδιου του σήματος. Με άλλα λόγια, ακόμη και το σήμα είναι κρυπτογραφημένο, η ανάλυση κίνησης μπορεί ακόμα να χρησιμοποιηθεί για να αποκαλύψει τα μοτίβα των συμβαλλομένων μερών επικοινωνίας. Η επίθεση ανάλυσης κίνησης δεν επηρεάζει ούτε τις νόμιμες επικοινωνίες.

Η μέθοδος κρυπτογράφησης που χρησιμοποιείται για την αποτροπή της υποκλοπής εξαρτάται σε μεγάλο βαθμό από την ισχύ του αλγορίθμου κρυπτογράφησης και επίσης από την ικανότητα υπολογιστών του υποκλοπής. Με τη γρήγορη κλιμάκωση της υπολογιστικής ισχύος και την ανάπτυξη προηγμένων τεχνολογιών ανάλυσης δεδομένων, οι ωτοασπίδες μπορούν να εκμεταλλευτούν το πλεονέκτημα των νέων τεχνολογιών στις επιθέσεις τους. Οι υφιστάμενοι μηχανισμοί για την αντιμετώπιση της υποκλοπής αντιμετωπίζουν μεγάλη πρόκληση, καθώς πολλοί από αυτούς αναλαμβάνουν έναν μικρό αριθμό ταυτόχρονων υποκλοπών με χαμηλή ικανότητα υπολογιστών χαμηλή ικανότητα ανάλυσης δεδομένων. Επιπλέον, ορισμένες τεχνολογίες που εφαρμόζονται σε ασύρματα δίκτυα 5G όπως το HetNet ενδέχεται να αυξήσουν περαιτέρω τη δυσκολία καταπολέμησης των υποκλοπών. Σε γενικές γραμμές, τα νέα χαρακτηριστικά των ασύρματων δικτύων 5G οδηγούν σε πολλά πιο περίπλοκα σενάρια για την αντιμετώπιση των σταγονόμετρων, για παράδειγμα, στο , λαμβάνονται υπόψη οι υποκλοπές με πολλαπλές κεραίες. Καθώς οι κρυπτογραφικές μέθοδοι για την αντιμετώπιση της ακοής έχουν διερευνηθεί εκτενώς στο παρελθόν και θεωρούνται αρκετά ώριμες, πιο πρόσφατα, η έρευνα PLS για την αντιμετώπιση της υποκλοπής έχει πληρωθεί όλο και περισσότερο

2 JAMMING

Σε αντίθεση με το eavesdropping και την ανάλυση της κυκλοφορίας, το jamming μπορεί να διαταράξει εντελώς τις επικοινωνίες μεταξύ νόμιμων χρηστών. Το 5b είναι ένα παράδειγμα για επιθέσεις μπλοκαρίσματος. Ο κακόβουλος κόμβος δημιουργεί εσκεμμένες παρεμβολές που μπορούν να διαταράξουν τις επικοινωνίες δεδομένων μεταξύ νόμιμων χρηστών. Η εμπλοκή μπορεί επίσης να εμποδίσει την πρόσβαση εξουσιοδοτημένων χρηστών σε πόρους ραδιοφώνου. Οι λύσεις για ενεργές επιθέσεις βασίζονται συνήθως σε ανίχνευση.

Οι τεχνικές Spread Spectrum όπως το Direct Spread Spectrum Spectrum (DSSS) και το Spop Hoping Spectrum Spectrum (FHSS) χρησιμοποιούνται ευρέως ως μέθοδος ασφαλούς επικοινωνίας για την καταπολέμηση της παρεμβολής στο στρώμα PHY με τη διάδοση των σημάτων σε ένα ευρύτερο φάσμα εύρους ζώνης. Ωστόσο, τα προγράμματα αντι-μπλοκαρίσματος με βάση το DSSS και το FHSS ενδέχεται να μην ταιριάζουν σε εσωτερικές εφαρμογές σε ασύρματα δίκτυα 5G.



3 DOS – DDoS

Οι επιθέσεις DoS μπορούν να εξαντλήσουν τους πόρους του δικτύου από έναν διαφημιστικό. Το DoS είναι μια παραβίαση επίθεσης ασφαλείας της διαθεσιμότητας των δικτύων. Η εμπλοκή μπορεί να χρησιμοποιηθεί για να ξεκινήσει μια επίθεση DoS. Το DoS μπορεί να σχηματιστεί όταν υπάρχουν περισσότερα από ένα κατανεμημένα διαφημιστικά. Το Σχήμα 5γ δείχνει ένα μοντέλο DDoS. DoS και DDoS και οι δύο ενεργές επιθέσεις που μπορούν να εφαρμοστούν σε διαφορετικά επίπεδα. Επί του παρόντος, η ανίχνευση χρησιμοποιείται κυρίως για την αναγνώριση επιθέσεων DoS και DDoS. Με υψηλή διείσδυση τεράστιων συσκευών σε ασύρματα δίκτυα 5G, το DoS και το DDoS πιθανότατα θα γίνουν επικίνδυνες απειλές για τους χειριστές. Οι επιθέσεις DoS και DDoS σε 5G ασύρματα δίκτυα μπορούν να επιτεθούν στο δίκτυο πρόσβασης μέσω ενός πολύ μεγάλου αριθμού συνδεδεμένων συσκευών. Με βάση την επίθεση στόχος, μια επίθεση DoS μπορεί να αναγνωριστεί είτε ως επίθεση DoS σε υποδομή δικτύου είτε ως επίθεση DoS συσκευής χρήστη. Μια επίθεση DoS ενάντια στην υποδομή δικτύου μπορεί να χτυπήσει το επίπεδο σηματοδότησης, το επίπεδο χρήστη, το επίπεδο διαχείρισης, τα συστήματα υποστήριξης, τους πόρους ραδιοφώνου , λογικοί και φυσικοί πόροι. Μια επίθεση DoS εναντίον συσκευής / χρήστη μπορεί να στοχεύσει σε μπαταρία, μνήμη, δίσκο, CPU, ραδιόφωνο, ενεργοποιητή και αισθητήρες.

4 MITM

Στην επίθεση MITM, ο εισβολέας παίρνει κρυφά τον έλεγχο του καναλιού επικοινωνίας μεταξύ δύο νόμιμων μερών. Ο εισβολέας MITM μπορεί να υποκλέψει, να τροποποιήσει και να αντικαταστήσει τα μηνύματα επικοινωνίας μεταξύ των δύο νόμιμων μερών. Το 5d δείχνει ένα μοντέλο επίθεσης MITM. Το MITM είναι μια ενεργή επίθεση που μπορεί να ξεκινήσει σε διαφορετικά επίπεδα. Συγκεκριμένα, οι επιθέσεις MITM στοχεύουν στον κίνδυνο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας δεδομένων. Με βάση την αναφορά έρευνας δεδομένων της Verizon , η επίθεση MITM είναι μία από τις πιο κοινές επιθέσεις ασφαλείας. Στο παλαιό κυψελοειδές δίκτυο, το MITM που βασίζεται σε σταθμούς ψευδοβάσεων είναι μια επίθεση που ο εισβολέας αναγκάζει έναν νόμιμο χρήστη να δημιουργήσει μια σύνδεση με έναν ψεύτικο σταθμό basetransceiver . Ο αμοιβαίος έλεγχος ταυτότητας μεταξύ της φορητής συσκευής και του σταθμού βάσης χρησιμοποιείται συνήθως για την αποτροπή του ψευδούς σταθμού βάσης MITM

ΚΕΦΑΛΑΙΟ 2 / ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ 5G

Η νέα αρχιτεκτονική, οι νέες τεχνολογίες και οι θήκες χρήσης σε δίκτυα 5G φέρνουν νέες δυνατότητες και απαιτήσεις των υπηρεσιών ασφαλείας. Σε αυτήν την ενότητα, παρουσιάζονται κυρίως τέσσερις τύπους υπηρεσιών ασφαλείας: έλεγχος ταυτότητας (έλεγχος ταυτότητας οντότητας, έλεγχος ταυτότητας μηνυμάτων), εμπιστευτικότητα (εμπιστευτικότητα δεδομένων, απόρρητο), διαθεσιμότητα και ακεραιότητα.

1 ΠΙΣΤΟΠΟΙΗΣΗ / AUTHENTICATION

Υπάρχουν δύο είδη ελέγχου πιστοποίησης, δηλαδή η πιστοποίηση οντοτήτων και ο έλεγχος ταυτότητας μηνυμάτων. Τόσο ο έλεγχος ταυτότητας οντοτήτων όσο και ο έλεγχος ταυτότητας μηνυμάτων είναι σημαντικοί στα ασύρματα δίκτυα 5G για την αντιμετώπιση των προηγούμενων αναφερόμενων επιθέσεων. Η ταυτότητα οντοτήτων χρησιμοποιείται για να διασφαλίσει ότι η οντότητα επικοινωνίας είναι αυτή που ισχυρίζεται ότι είναι. Στα παλαιά κυψελοειδή δίκτυα, εφαρμόζεται αμοιβαίος έλεγχος ταυτότητας μεταξύ εξοπλισμού χρήστη (UE) και φορέα διαχείρισης κινητικότητας (MME) για δύο μέρη που επικοινωνούν μεταξύ τους. Οι αμοιβαίες επαφές μεταξύ UE

και MME είναι το πιο σημαντικό χαρακτηριστικό ασφαλείας στο παραδοσιακό κυψελοειδές πλαίσιο ασφαλείας. Η πιστοποίηση ταυτότητας και το κλειδί σε 4G κυψελοειδή δίκτυα βασίζεται σε συμμετρικό κλειδί. Ωστόσο, το 5G απαιτεί έλεγχο ταυτότητας όχι μόνο μεταξύ UE και MME, αλλά και μεταξύ άλλων τρίτων, όπως οι πάροχοι υπηρεσιών. Το μοντέλο εμπιστοσύνης διαφέρει από αυτό που χρησιμοποιείται στα παραδοσιακά κυτταρικά δίκτυα, η υβριδική και ευέλικτη διαχείριση ελέγχου ταυτότητας απαιτείται στα 5G. Ο υβριδικός και ευέλικτος έλεγχος ταυτότητας του UE μπορεί να εφαρμοστεί με τρεις διαφορετικούς τρόπους: έλεγχος ταυτότητας μόνο από δίκτυο, έλεγχος ταυτότητας μόνο από πάροχο υπηρεσιών, και έλεγχος ταυτότητας τόσο από το δίκτυο όσο και από τον πάροχο υπηρεσιών . Λόγω του πολύ υψηλού ρυθμού δεδομένων και της εξαιρετικά χαμηλής απαίτησης σε ασύρματο 5G δίκτυα, ο έλεγχος ταυτότητας στο 5G αναμένεται να είναι πολύ πιο γρήγορος από ποτέ. Επιπλέον, η πολυεπίπεδη αρχιτεκτονική του 5G μπορεί να συναντήσει πολύ συχνές μεταβιβάσεις και πιστοποιήσεις μεταξύ διαφορετικών επιπέδων 5G. Για να ξεπεραστούν οι δυσκολίες της διαχείρισης κλειδιών στο HetNets και για να μειωθεί ο περιττός λανθάνων χρόνος που προκαλείται από συχνές μεταβιβάσεις και έλεγχο ταυτότητας μεταξύ διαφορετικών επιπέδων, προτείνεται ένα γρήγορο σύστημα ελέγχου ταυτότητας με δυνατότητα SDN με τη χρήση σταθμισμένης μεταφοράς ασφαλούς περιβάλλοντος-πληροφοριών. αποτελεσματικότητα του ελέγχου ταυτότητας κατά τη διάρκεια της παράδοσης και για την κάλυψη των απαιτήσεων καθυστέρησης 5G. Για την παροχή περισσότερων υπηρεσιών ασφαλείας σε ασύρματα δίκτυα 5G, στα και , προτείνεται ένα AKA που βασίζεται στο δημόσιο κλειδί.

Με τις διάφορες νέες εφαρμογές σε ασύρματα δίκτυα 5G, ο έλεγχος ταυτότητας μηνυμάτων γίνεται όλο και πιο σημαντικός. Επιπλέον, με τις αυστηρότερες απαιτήσεις σχετικά με την ευρυχωρία, την απόδοση φάσματος (SE) και την EE σε 5G, ο έλεγχος ταυτότητας μηνυμάτων αντιμετωπίζει νέες προκλήσεις.

2 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ / CONFIDENTIALITY

Η εμπιστευτικότητα αποτελείται από δύο πτυχές, δηλαδή την εμπιστευτικότητα δεδομένων και το απόρρητο. Η εμπιστευτικότητα δεδομένων προστατεύει τη μετάδοση δεδομένων από παθητικές επιθέσεις περιορίζοντας την πρόσβαση δεδομένων μόνο σε ακούσιους χρήστες και αποτρέποντας την πρόσβαση ή την αποκάλυψη από μη εξουσιοδοτημένους χρήστες. Το απόρρητο αποτρέπει τον έλεγχο και τον επηρεασμό των πληροφοριών που σχετίζονται με νόμιμους χρήστες, όπως το δείγμα, το απόρρητο προστατεύει τις ροές κίνησης από οποιαδήποτε ανάλυση του εισβολέα. Τα μοτίβα κυκλοφορίας μπορούν να χρησιμοποιηθούν για τη διάγνωση ευαίσθητων πληροφοριών, όπως η τοποθεσία αποστολέων / παραληπτών κ.λπ. Με διάφορες εφαρμογές στο 5G, υπάρχουν τεράστια δεδομένα που σχετίζονται με το απόρρητο των χρηστών, π.χ. δεδομένα δρομολόγησης οχήματος, δεδομένα παρακολούθησης της υγείας και ούτω καθεξής.

Η κρυπτογράφηση δεδομένων έχει χρησιμοποιηθεί ευρέως για τη διασφάλιση της εμπιστευτικότητας των δεδομένων, εμποδίζοντας τους μη εξουσιοδοτημένους χρήστες να εξάγουν οποιεσδήποτε χρήσιμες πληροφορίες από τις πληροφορίες μετάδοσης. Η τεχνική συμμετρικού κλειδιού κρυπτογράφησης μπορεί να εφαρμοστεί για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων με ένα ιδιωτικό κλειδί κοινόχρηστο μεταξύ του αποστολέα και του παραλήπτη. Για να μοιραστείτε ένα κλειδί μεταξύ του αποστολέα και του παραλήπτη, απαιτείται ασφαλής μέθοδος διανομής κλειδιού. Η συμβατική μέθοδος κρυπτογραφίας σχεδιάζεται με βάση την υπόθεση ότι οι εισβολείς έχουν περιορισμένες δυνατότητες υπολογισμού. Έτσι, είναι δύσκολο να καταπολεμήσετε τους εισβολείς που είναι εξοπλισμένοι με ισχυρές δυνατότητες υπολογιστών. Αντί να βασίζεται αποκλειστικά σε γενικούς κρυπτογραφικούς μηχανισμούς υψηλότερου επιπέδου, το PLS μπορεί να υποστηρίξει την υπηρεσία εμπιστευτικότητας ενάντια σε παρεμβολές και παραβίαση επιθέσεων. Εκτός από τις υπηρεσίες δεδομένων του 5G, οι χρήστες αρχίζουν να συνειδητοποιούν τη σημασία της υπηρεσίας προστασίας της ιδιωτικής ζωής. Η υπηρεσία απορρήτου στο 5G αξίζει πολύ περισσότερη προσοχή από ό, τι στα παλαιά κυψελοειδή δίκτυα λόγω των βοηθητικών συνδέσεων δεδομένων . Η υπηρεσία

ανωνυμίας είναι μια απαίτηση βασικής ασφάλειας σε πολλές περιπτώσεις χρηστών. Σε πολλές περιπτώσεις, η διαρροή προσωπικού χαρακτήρα μπορεί να προκαλέσει σοβαρές συνέπειες. Για παράδειγμα, τα δεδομένα παρακολούθησης της υγείας αποκαλύπτουν τις ευαίσθητες προσωπικές πληροφορίες για την υγεία . Τα δεδομένα δρομολόγησης του οχήματος μπορούν να εκθέσουν το απόρρητο της τοποθεσίας . Τα ασύρματα δίκτυα 5G προκαλούν σοβαρή ανησυχία στη διαρροή απορρήτου. Στο HetNets, λόγω της υψηλής πυκνότητας μικρών κελιών, ο αλγόριθμος συσχέτισης μπορεί να αποκαλύψει το απόρρητο της τοποθεσίας των χρηστών.

3) ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Η διαθεσιμότητα ορίζεται ως ο βαθμός στον οποίο μια υπηρεσία είναι προσβάσιμη και χρησιμοποιήσιμη σε οποιονδήποτε νόμιμο χρήστη όποτε και οπουδήποτε ζητείται. Η διαθεσιμότητα αξιολογεί πόσο ισχυρό είναι το σύστημα όταν αντιμετωπίζει διάφορες επιθέσεις και είναι μια βασική μέτρηση απόδοσης στο 5G. Η επίθεση διαθεσιμότητας είναι μια τυπική ενεργή επίθεση. Μία από τις σημαντικότερες επιθέσεις στη διαθεσιμότητα είναι η επίθεση DoS, η οποία μπορεί να προκαλέσει άρνηση πρόσβασης στην υπηρεσία σε νόμιμους χρήστες. Η παρεμβολή ή η παρέμβαση μπορεί να διαταράξει τους δεσμούς επικοινωνίας μεταξύ των νόμιμων χρηστών παρεμβαίνοντας στα ραδιοσήματα Με τους μη ασφαλείς κόμβους IoT, τα ασύρματα δίκτυα 5G αντιμετωπίζουν τεράστια πρόκληση για την αποτροπή παρεμβολών και επιθέσεων DDoS για την εξασφάλιση της υπηρεσίας διαθεσιμότητας.

Για τη διαθεσιμότητα στο PHY, το DSSS και το FHSS είναι δύο κλασικές λύσεις PLS. Το DSSS εφαρμόστηκε για πρώτη φορά στον στρατό τη δεκαετία του 1940. Ένας ψευδοκωδικός διάδοσης θορύβου πολλαπλασιάζεται με το φάσμα του αρχικού σήματος δεδομένων στο DSSS. Χωρίς γνώση σχετικά με τον ψευδοκώδικα διάδοσης θορύβου, ένας jammer χρειάζεται πολύ μεγαλύτερη δύναμη για να διαταράξει τη νόμιμη αποστολή. Για το FHSS, ένα σήμα μεταδίδεται με γρήγορη εναλλαγή μεταξύ πολλών καναλιών συχνότητας χρησιμοποιώντας μια ψευδοτυχαία ακολουθία που δημιουργείται από ένα κλειδί που μοιράζεται μεταξύ του πομπού και του δέκτη. Δυναμικό φάσμα εφαρμόζεται σε επικοινωνίες D2D και γνωστικό παράδειγμα για τη βελτίωση του SE στο 5G. Το FHSS μπορεί να προκαλέσει κακή απόδοση με την επίθεση μπλοκαρίσματος. Προτείνεται ένα ψευδοτυχαίο φάσμα εξάπλωσης χρονομέτρου για τη βελτίωση της απόδοσης σχετικά με την πιθανότητα μπλοκαρίσματος, την πιθανότητα αλλαγής και την πιθανότητα σφάλματος. Η κατανομή πόρων υιοθετείται για να βελτιώσει τον εντοπισμό της παραβίασης διαθεσιμότητας .

4) ΑΚΕΡΑΙΟΤΗΤΑ

Παρόλο που ο έλεγχος ταυτότητας μηνυμάτων παρέχει επιβεβαίωση της πηγής του μηνύματος, δεν παρέχεται προστασία έναντι της επανάληψης ή της τροποποίησης του μηνύματος. Το 5G στοχεύει στην παροχή συνδεσιμότητας οποτεδήποτε, οπουδήποτε και οποτεδήποτε και να υποστηρίζει εφαρμογές που σχετίζονται στενά με το ανθρώπινο ον καθημερινά ζωή όπως η μέτρηση της ποιότητας του πόσιμου νερού και ο προγραμματισμός της μεταφοράς. Η ακεραιότητα των δεδομένων είναι μία από τις βασικές απαιτήσεις ασφαλείας σε ορισμένες εφαρμογές.

Η ακεραιότητα αποτρέπει την τροποποίηση των πληροφοριών από προφορικές επιθέσεις από μη εξουσιοδοτημένες οντότητες. Το Data integrity μπορεί να παραβιαστεί από κακόβουλες επιθέσεις εσωτερικών προσώπων όπως έγχυση μηνυμάτων ή τροποποίηση δεδομένων. Δεδομένου ότι οι insider attackers έχουν έγκυρες ταυτότητες, είναι δύσκολο να εντοπιστούν αυτές οι επιθέσεις. Σε περιπτώσεις χρήσης, όπως έξυπνοι μετρητές σε έξυπνο πλέγμα πρέπει να παρέχεται υπηρεσία ακεραιότητας δεδομένων κατά της χειραγώγησης. Σε σύγκριση με τις φωνητικές επικοινωνίες, τα δεδομένα μπορούν εύκολα να επιτεθούν και να τροποποιηθούν . Οι υπηρεσίες ακεραιότητας μπορούν να παρέχονται χρησιμοποιώντας αμοιβαίο έλεγχο ταυτότητας, το οποίο δημιουργεί ένα κλειδί ακεραιότητας. Απαιτείται η υπηρεσία ακεραιότητας των πληροφοριών προσωπικής υγείας . Η ακεραιότητα των μηνυμάτων μπορεί να παρέχεται στα σχήματα ελέγχου ταυτότητας .

ΚΕΦΑΛΑΙΟ 3 / ΣΥΓΧΡΟΝΕΣ ΛΥΣΕΙΣ ΓΙΑ ΑΣΦΑΛΕΙΑ ΣΤΑ ΔΙΚΤΥΑ 5G

Σε αυτήν την ενότητα, συνοψίζουμε τις υπερσύγχρονες λύσεις για την ασφάλεια σε συστήματα ασύρματων δικτύων 5G. Όπως αναφέρεται στην προηγούμενη ενότητα, η κρυπτογραφία και το PLS είναι δύο λύσεις ασφαλείας.

Α. ΕΛΕΓΧΟΣ ΤΑΥΤΟΤΗΤΑΣ

Ο έλεγχος ταυτότητας είναι μια από τις πιο σημαντικές υπηρεσίες ασφαλείας σε ασύρματα δίκτυα 5G. Στα παλαιά δίκτυα κινητής τηλεφωνίας, ένα σύστημα ελέγχου ταυτότητας βασίζεται συνήθως σε συμμετρικό κλειδί. Η εφαρμογή του συστήματος ελέγχου ταυτότητας μπορεί να προσφέρει πολλές απαιτήσεις ασφαλείας. Στα δίκτυα κινητής τηλεφωνίας τρίτης γενιάς (3G), ο αμοιβαίος έλεγχος ταυτότητας πραγματοποιείται μεταξύ ενός κινητού σταθμού και του δικτύου. Μετά την πιστοποίηση, δημιουργείται ένα κλειδί κρυπτογράφησης και ένα κλειδί ακεραιότητας για να διασφαλιστεί τόσο η εμπιστευτικότητα των δεδομένων όσο και η ακεραιότητα μεταξύ του σταθμού κινητής τηλεφωνίας και του σταθμού βάσης.

Λόγω της χαμηλής απαίτησης καθυστέρησης των δικτύων 5G, τα σχήματα ελέγχου ταυτότητας πρέπει να είναι πιο αποτελεσματικά στο 5Gthan από ποτέ. Για να αξιοποιήσει τα πλεονεκτήματα του SDN, Σε σύγκριση με τις μεθόδους ψηφιακού κρυπτογραφικού ελέγχου ταυτότητας, η προτεινόμενη μέθοδος είναι δύσκολο να παραβιαστεί πλήρως, δεδομένου ότι βασίζεται στα χαρακτηριστικά φυσικού επιπέδου του χρήστη. Υπάρχουν περισσότερα από ένα φυσικά χαρακτηριστικά στρώματος που χρησιμοποιούνται στο SCI για τη βελτίωση της αξιοπιστίας ελέγχου ταυτότητας για εφαρμογές που απαιτούν υψηλό επίπεδο ασφάλειας. Το μοντέλο ελέγχου ταυτότητας με δυνατότητα SDN εμφανίζεται στο Σχ. 6. Ο ελεγκτής SDN εφαρμόζει ένα μοντέλο ελέγχου ταυτότητας για την παρακολούθηση και την πρόβλεψη της θέσης του χρήστη προκειμένου να προετοιμάσει τα σχετικά κελιά πριν από την άφιξη του χρήστη. Αυτό βοηθά στην επίτευξη απρόσκοπτης ταυτότητας παράδοσης. Τα χαρακτηριστικά του επιπέδου Physi-cal χρησιμοποιούνται για την παροχή μοναδικών δακτυλικών αποτυπωμάτων του χρήστη και για την απλοποίηση της διαδικασίας ελέγχου ταυτότητας. Τρία είδη δακτυλικών αποτυπωμάτων χρησιμοποιούνται ως χαρακτηριστικά φυσικού επιπέδου για κάθε χρήστη. Τα επικυρωμένα πρωτότυπα χαρακτηριστικά λαμβάνονται μετά από πλήρη έλεγχο ταυτότητας. Οι παρατηρήσεις συλλέγονται μέσω συνεχούς δειγματοληψίας πολλαπλών χαρακτηριστικών φυσικών επιπέδων από τα ληφθέντα πακέτα στον ελεγκτή SDN. Τόσο το πρωτότυπο αρχείο όσο και τα αποτελέσματα παρατήρησης περιέχουν τη μέση τιμή των χαρακτηριστικών και τη διακύμανση των επιλεγμένων χαρακτηριστικών. Στη συνέχεια, η μετατόπιση χαρακτηριστικού μπορεί να υπολογιστεί βάσει των επικυρωμένων αρχικών χαρακτηριστικών και των παρατηρούμενων χαρακτηριστικών. Εάν το χαρακτηριστικό offset είναι μικρότερο από ένα προκαθορισμένο όριο, ο εξοπλισμός χρήστη θεωρείται νόμιμος. Η πιθανότητα ανίχνευσης παρουσιάζεται στο χαρτί.

Για την αξιολόγηση της απόδοσης της προτεινόμενης μεθόδου, προτείνεται ένα μοντέλο δικτύου SDN που χρησιμοποιεί προτεραιότητα στην ουρά. Η καθυστέρηση ελέγχου ταυτότητας συγκρίνεται μεταξύ διαφορετικών σεναρίων χρήσης δικτύου. Το προτεινόμενο πρωτόκολλο γρήγορης πιστοποίησης περιλαμβάνει πλήρη έλεγχο ταυτότητας και σταθμισμένο γρήγορο έλεγχο ταυτότητας βάσει SCI transfer. Μετά τον πρώτο πλήρη έλεγχο ταυτότητας σε ένα κελί, μπορεί να εφαρμοστεί εύκολα σε άλλα κελιά με επαλήθευση διεύθυνσης MAC, η οποία χρειάζεται μόνο τοπική επεξεργασία. Επιπλέον, ο πλήρης έλεγχος ταυτότητας μπορεί ακόμη και να αφαιρεθεί χωρίς να διαταραχθεί η επικοινωνία του χρήστη. Μια παράμετρος διάρκειας έγκυρου χρόνου χρησιμοποιείται για την ευέλικτη προσαρμογή της απαίτησης ασφάλειας. Τα αποτελέσματα της προσομοίωσης συνέκριναν την καθυστέρηση απόδοσης μεταξύ του γρήγορου ελέγχου ταυτότητας με δυνατότητα

SDN και της συμβατικής μεθόδου κρυπτογραφικού ελέγχου ταυτότητας. Ο γρήγορος έλεγχος ταυτότητας με δυνατότητα SDN έχει καλύτερη απόδοση καθυστέρησης λόγω ευελιξίας SDN και δυνατότητας προγραμματισμού σε δίκτυα 5G.

Για την αντιμετώπιση των ζητημάτων που προκαλούνται από την έλλειψη υποδομής ασφαλείας για επικοινωνίες D2D, αναπτύσσεται μια βαθμολογία ασφαλείας βάσει συνεχούς γνησιότητας για την αξιολόγηση και τη βελτίωση της ασφάλειας των ασύρματων συστημάτων D2D. Προτείνεται η αρχή των προτύπων νομιμότητας για την εφαρμογή συνεχούς αυθεντικότητας , που επιτρέπει την ανίχνευση επίθεσης και τη μέτρηση βαθμολογίας ασφάλειας συστήματος Για το legitimacy pattern, μια περιττή ακολουθία bits εισάγεται σε ένα πακέτο για να επιτρέψει τον εντοπισμό της επίθεσης. Τα αποτελέσματα της προσομοίωσης δείχνουν τη σκοπιμότητα εφαρμογής των προτεινόμενων βαθμολογιών ασφαλείας χρησιμοποιώντας πρότυπα νομιμότητας. Οι συγγραφείς επεσήμαναν ότι τα νόμιμα μοτίβα που εξετάζουν τεχνικές προοπτικές και ανθρώπινες συμπεριφορές θα μπορούσαν να βελτιώσουν την απόδοση.

Συνδυάζοντας την υψηλή ασφάλεια και τη μέγιστη απόδοση στη χρήση εύρους ζώνης και την κατανάλωση ενέργειας σε 5G, Έγινε πρόταση για έναν νέο έλεγχο ταυτότητας μηνυμάτων βάσει κυκλικού ελέγχου πλεονασμού (CRC) που μπορεί να ανιχνεύσει τυχόν σφάλματα διπλού bit σε ένα μόνο μήνυμα. Καθορίζονται οι κρυπτογραφικές συναρτήσεις κατακερματισμού που βασίζονται στους κωδικούς CRC. Ένας γραμμικός καταχωρητής αλλαγής ταχυτήτων (LFSR) χρησιμοποιείται για την αποτελεσματική εφαρμογή της CRC κωδικοποίησης και αποκωδικοποίησης. Ο αλγόριθμος ελέγχου ταυτότητας μηνύματος εξάγει μια ετικέτα ελέγχου ταυτότητας με βάση ένα μυστικό κλειδί και το μήνυμα. Υποτίθεται ότι ο αντίπαλος έχει την οικογένεια των λειτουργιών κατακερματισμού αλλά όχι το συγκεκριμένο polynomialg και τα pads που χρησιμοποιούνται για τη δημιουργία της ετικέτας ελέγχου ταυτότητας. Το γεννητικό πολυώνυμο αλλάζει περιοδικά στην αρχή κάθε συνεδρίας και το padsis αλλάζει για κάθε μήνυμα.

Η αναγνώριση ραδιοσυχνοτήτων (RFID) έχει εφαρμοστεί ευρέως και μία μόνο ετικέτα RFID μπορεί να ενσωματώσει πολλαπλές εφαρμογές. Λόγω διαφόρων περιορισμών στις ετικέτες RFID χαμηλού κόστους, οι αλγόριθμοι κρυπτογράφησης και οι μηχανισμοί ελέγχου ταυτότητας που εφαρμόζονται σε συστήματα RFID πρέπει να είναι πολύ αποτελεσματικοί. Η απλή και γρήγορη λειτουργία κατακερματισμού θεωρείται για τους μηχανισμούς πιστοποίησης. Επιπλέον, με πολλαπλές εφαρμογές ενός RFID, η ανάκληση θα πρέπει να λαμβάνεται υπόψη στο σύστημα ελέγχου ταυτότητας. Χρησιμοποιείται μια συνάρτηση κατακερματισμού και ένας τυχαίος αριθμός για τη δημιουργία της αντίστοιχης μονάδας μέσω ενός τυπικού μηχανισμού απόκρισης πρόκλησης. Ο αναγνώστης περιέχει έναν ψευδο-τυχαίο αριθμό generator και ο διακόπτης κρατά μια συνάρτηση hash και database (HFD). Ο διακομιστής δημιουργεί μια εγγραφή ετικέτας για κάθε νόμιμη ετικέτα ως (IDS, IDi) και μια ομάδα αντίστοιχων εγγραφών εφαρμογής ως (Koldi, j, Knowi, j). Είναι το αίτημα ελέγχου ταυτότητας που δημιουργείται από τον αναγνώστη. R1 είναι ο πρώτος τυχαίος αριθμός που δημιουργήθηκε από το PNG στον αναγνώστη. Αφού λάβει το αίτημα ελέγχου ταυτότητας, η ετικέτα δημιουργεί τον δεύτερο τυχαίο αριθμό2 και υπολογίζει δύο μηνύματα ελέγχου ταυτότητας κατακερματισμού M1, M2 και την τιμή των πληροφοριών ελέγχου ταυτότητας XOR για ανάκληση ή πιστοποίηση της εφαρμογής. Τα αποτελέσματα ασφάλειας και πολυπλοκότητας παρουσιάζονται, τα οποία δείχνουν ότι το προτεινόμενο σχήμα έχει υψηλότερο επίπεδο ασφάλειας και το ίδιο επίπεδο πολυπλοκότητας σε σύγκριση με τα υπάρχοντα.

Λαμβάνοντας υπόψη την ανοιχτή φύση των επικοινωνιών D2D μεταξύ των ιατρικών αισθητήρων και των υψηλών απαιτήσεων απορρήτου των ιατρικών δεδομένων, , χρησιμοποιώντας την τεχνική χωρίς γενικευμένη σήμανση (CLGSC), οι συγγραφείς πρότειναν μια ελαφριά και ισχυρή ασφάλεια (LRSA) D2D- βοηθητικό πρωτόκολλο μετάδοσης δεδομένων σε ένα σύστημα m-health. Το σύστημα m-health διαμορφώνεται όπου το S δείχνει τον κόμβο πηγής και το R αντιπροσωπεύει τον κόμβο ρελέ. Ο ανώνυμος και αμοιβαίος έλεγχος ταυτότητας εφαρμόζεται ένα ασύρματο σώμα για την προστασία του

απορρήτου τόσο της πηγής δεδομένων όσο και του σκοπούμενου προορισμού. Η κρυπτογράφηση του μηνύματος Sand encryption της ταυτότητάς του SHare εφαρμόζεται στον πελάτη προέλευσης για έλεγχο ταυτότητας του ιατρού. Ένας αλγόριθμος υπογραφής χωρίς πιστοποιητικό εφαρμόζεται στα δεδομένα πελάτη προέλευσης προτού εκδοθούν. Η ταυτότητα των δεδομένων προέλευσης μπορεί να ανακτηθεί μόνο από τον αυτόν που έχει το ιδιωτικό κλειδί (xH, zH). Το κείμενο κρυπτογράφησης A πρέπει να αποκρυπτογραφηθεί μετά την ανάκτηση της ταυτότητας προέλευσης με το σωστό κλειδί συνεδρίας. Επομένως, ακόμη και το ιδιωτικό κλειδί έχει διαρρεύσει, χωρίς το κλειδί περιόδου λειτουργίας, το κρυπτογραφημένο κείμενο εξακολουθεί να είναι ασφαλές. Από την άλλη πλευρά, επαληθεύοντας το κείμενο κρυπτογράφησης S, μπορεί να γίνει η πιστοποίηση του πελάτη προέλευσης. Οι κόμβοι ρελέ μπορούν να επαληθεύσουν την υπογραφή και, στη συνέχεια, να αποφύγουν τα δεδομένα με τις δικές τους υπογραφές. Τα υπολογιστικά και τα γενικά έξοδα επικοινωνίας του προτεινόμενου CLGSC συγκρίνονται με άλλα τέσσερα σχήματα. Τα αποτελέσματα προσομοίωσης δείχνουν ότι το προτεινόμενο σχήμα CLGSC έχει χαμηλότερο υπολογισμό σε σχέση με τα άλλα τέσσερα σχήματα.

Το 5G είναι μια πολλά υποσχόμενη λύση για την παροχή υπηρεσιών σε πραγματικό χρόνο για δίκτυα οχημάτων. Ωστόσο, η ασφάλεια και η ιδιωτικότητα πρέπει να ενισχυθούν προκειμένου να διασφαλιστεί η ασφάλεια των μεταφορών. Το σύστημα περιλαμβάνει ένα δίκτυο πυρήνα κινητής τηλεφωνίας (MCN), μια αξιόπιστη αρχή (TA), ένα τμήμα μηχανοκίνητων οχημάτων (DMV) και μια υπηρεσία επιβολής του νόμου (LEA). Τεχνικές επικοινωνίας D2D και mmWave υιοθετούνται στις επικοινωνίες οχημάτων 5G. Το HetNet εφαρμόζεται χωρητικότητα δικτύου για να επιτυγχάνει υψηλούς ρυθμούς δεδομένων χρήστη. Η πλατφόρμα cloud παρέχει μαζική αποθήκευση και πρόσβαση σε πανταχού παρούσα δεδομένα. Οι προτεινόμενοι κρυπτογραφικοί μηχανισμοί περιλαμβάνουν ένα σύστημα ψευδώνυμου ελέγχου ταυτότητας, μια κρυπτογράφηση δημόσιου κλειδιού με αναζήτηση λέξεων- κλειδιών, μια κρυπτογράφηση βασισμένων σε χαρακτηριστικά ciphertext και σχήματα κατωφλίου που βασίζονται σε μυστική κοινή χρήση. Το ψευδώνυμο σύστημα ελέγχου ταυτότητας με ισχυρή διατήρηση της ιδιωτικότητας εφαρμόζεται για τη βελτιστοποίηση του μεγέθους λίστας ανάκλησης πιστοποίησης, το οποίο είναι σε γραμμική μορφή σε σχέση με τον αριθμό των ανακληθέντων οχημάτων, έτσι ώστε η επικύρωση της επικύρωσης πιστοποίησης να είναι η χαμηλότερη. Οι απαιτήσεις ελέγχου ταυτότητας περιλαμβάνουν έλεγχο ταυτότητας οχήματος και ακεραιότητα μηνυμάτων, όπου ο έλεγχος ταυτότητας οχήματος επιτρέπει στο LEA και στα επίσημα οχήματα να ελέγχουν την αυθεντικότητα του αποστολέα. Ο έλεγχος ταυτότητας επιτυγχάνεται με τη χρήση ψηφιακής υπογραφής που βασίζεται στο δημόσιο κλειδί και δεσμεύει ένα βίντεο κρυπτογραφημένου ατυχήματος με ένα ψευδώνυμο και την ταυτότητα του αποστολέα. Η τεχνική ψευδώνυμου ελέγχου ταυτότητας μπορεί να επιτύχει την υπό όρους ανωνυμία και το απόρρητο του αποστολέα.

Β. ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Η διαθεσιμότητα είναι βασική μέτρηση για τη διασφάλιση των εξαιρετικά αξιόπιστων επικοινωνιών στο 5G. Ωστόσο, εκπέμποντας τυχαία ασύρματα ηχητικά σήματα, ένας jammer μπορεί να υποβαθμίσει σημαντικά την απόδοση των χρηστών κινητής τηλεφωνίας και μπορεί ακόμη και να αποκλείσει τη διαθεσιμότητα των υπηρεσιών. Η εμπλοκή είναι ένας από τους τυπικούς μηχανισμούς που χρησιμοποιούνται από επιθέσεις DoS. Τα περισσότερα από τα προγράμματα καταπολέμησης της παρεμβολής χρησιμοποιούν την τεχνική hopping, στην οποία οι χρήστες ανεβάζουν πολλαπλά κανάλια για να αποφύγουν την επίθεση μπλοκαρίσματος και να διασφαλίσουν τη διαθεσιμότητα υπηρεσιών.

Προτάθηκε ένα μυστικό προσαρμοστικό πρόγραμμα συχνότητας ως πιθανή τεχνική 5G ενάντια σε DoS που βασίζεται σε μια ραδιοφωνική πλατφόρμα καθορισμένη από λογισμικό Ο προτεινόμενος εκτιμητής ρυθμού σφάλματος bit (BER) με βάση τις πληροφορίες φυσικών επιπέδων εφαρμόζεται για να αποφασίσει τη μαύρη λίστα συχνότητας υπό επίθεση DoS. Δεδομένου ότι η τεχνική hopping

συχνότητας απαιτεί από τους χρήστες να έχουν πρόσβαση σε πολλά κανάλια, ενδέχεται να μην λειτουργεί αποτελεσματικά για χρήστες με δυναμική πρόσβαση φάσματος λόγω του υψηλού ρυθμού μεταγωγής και υψηλή πιθανότητα μπλοκαρίσματος. Για την μείωση του ρυθμού αλλαγής και η πιθανότητα μπλοκαρίσματος, προτάθηκε ένα ψευδοτυχαίο σχήμα αντι-μπλοκαρίσματος για γνωστικούς χρήστες σε 5G για την αντιμετώπιση των επιθέσεων εμπλοκής. Ο αντίκτυπος της δυναμικής του φάσματος στην απόδοση των κινητών γνωστικών χρηστών διαμορφώνεται με την παρουσία ενός γνωστικού jammer με περιορισμένους πόρους. Παρουσιάζονται οι αναλυτικές λύσεις πιθανότητας μπλοκαρίσματος, ρυθμός μεταγωγής και πιθανότητα σφάλματος. Η πιθανότητα μπλοκαρίσματος σχετίζεται με την απόδοση καθυστέρησης και την πιθανότητα σφάλματος. Η πιθανότητα μπλοκαρίσματος είναι χαμηλή όταν το jammer στερείται ευκαιριών πρόσβασης. Η πιθανότητα εναλλαγής του συστήματος χρονικής αναπήδησης ξεπερνά το σύστημα συχνότητας μετάβασης. Με την ίδια μέση ενέργεια symbol ανά joule, το time-hopping έχει χαμηλότερη πιθανότητα σφάλματος από το hopping και η απόδοση αυξάνεται σε ένα συγκεκριμένο επίπεδο ενέργειας συμβόλου. Οι συγγραφείς επεσήμαναν ότι η προτεινόμενη τεχνική time-hopping είναι ένας ισχυρός υποψήφιος για συνδέσεις D2D σε ασύρματα δίκτυα 5G λόγω της καλής απόδοσης EE και SE, καθώς και της ικανότητάς του να παρέχει ανθεκτικότητα στις παρεμβολές με μια μικρή επικοινωνία. Ωστόσο, απαιτείται ένα προ-κοινόχρηστο κλειδί για την τεχνική αντι-μπλοκαρίσματος. Η μετατόπιση τόσο της συχνότητας όσο και η αναπήδηση χρόνου απαιτούν ένα κοινόχρηστο κλειδί για τον προσδιορισμό της ακολουθίας μετάβασης.

Λαμβάνοντας υπόψη τις περιορισμένες υπολογιστικές δυνατότητες σε ορισμένους κόμβους, στο , ένα κέντρο σύντηξης χρησιμοποιείται για την υπεράσπιση αυτών των κόμβων από μια κακόβουλη επίθεση ραδιοφωνικής παρεμβολής σε δίκτυο χωρίς καλώδια 5G. Ένα μη συνεργατικό παιχνίδι Colonel Blotto συνδυάζεται μεταξύ του jammer και του κέντρου σύντηξης ως άσκηση στην στρατηγική διανομή πόρων. Το jammer στοχεύει να θέσει σε κίνδυνο το τότε δίκτυο χωρίς να εντοπιστεί, διανέμοντας έξυπνα τους κόμβους του. Από την άλλη πλευρά, το κέντρο σύντηξης ως υπερασπιστής στοχεύει να ανιχνεύσει μια τέτοια επίθεση από ένα σχέδιο ανίχνευσης που δεν έχει εγκριθεί σε ένα συγκεκριμένο σύνολο κόμβων. Το fusion center μπορεί να εκχωρήσει περισσότερα bits σε αυτούς τους κόμβους για την αναφορά των μετρημένων παρεμβολών. Ένας ιεραρχικός βαθμός εκχωρείται σε κάθε κόμβο με βάση την κεντρικότητα μεταξύ τους. Μόλις ανιχνευθεί η επίθεση, το κέντρο σύντηξης θα δώσει εντολή στον κόμβο στόχου να αυξήσει την ισχύ εκπομπής του για να διατηρήσει ένα κατάλληλο SINR για κανονικές επικοινωνίες. Τα αποτελέσματα της προσομοίωσης δείχνουν ότι η απόδοση του ποσοστού σφαλμάτων βελτιώνεται σημαντικά με το κέντρο σύντηξης να έχει περισσότερα bits για κατανομή μεταξύ των κόμβων. Ο προτεινόμενος μηχανισμός κατανομής πόρων ξεπερνά τον μηχανισμό που εκχωρεί τα διαθέσιμα bits σε τυχαίο τρόπο.

Γ. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΔΕΔΟΜΕΝΩΝ

Η υπηρεσία εμπιστευτικότητας δεδομένων απαιτείται συνήθως για την αντιμετώπιση επιθέσεων που παραβλέπουν. Τα συγκεκριμένα μοντέλα συστήματος μπορεί να διαφέρουν στον αριθμό των κεραιών πομπού / δέκτη / υποκλοπής και στον αριθμό των υποκλοπών / ρελέ / συνεργατών. Τα ρελέ ή οι συνεργάτες είναι προαιρετικά στο σύστημα. Σε αυτήν την υποενότητα, συζητάμε την εμπιστευτικότητα δεδομένων με βάση τον έλεγχο ισχύος, το ρελέ, τον τεχνητό θόρυβο, την επεξεργασία σήματος και τις κρυπτογραφικές μεθόδους.

1 RELAY .

Η συνεργασία με το ρελέ μπορεί να χρησιμοποιηθεί για να βοηθήσει τον αποστολέα να εξασφαλίσει τη μετάδοση σήματος. Το power beacon είναι εξοπλισμένο με πολλαπλές κεραίες, οι οποίες μπορούν να χρησιμοποιηθούν για την ενίσχυση της ενέργειας που συλλέγεται. Το ORS επιλέγει το βοηθητικό

ρελέ για να μεγιστοποιήσει τη χωρητικότητα μυστικότητας του συστήματος υποθέτοντας ότι η πηγή έχει πλήρη γνώση των πληροφοριών κατάστασης καναλιού (CSI) σε κάθε σύνδεσμο. Το PRS επιλέγει το ρελέ βοήθειας βάσει μερικού CSI. Το σύστημα περιλαμβάνει ένα φάρο ισχύος με πολλαπλές κεραίες, πολλά ρελέ, έναν κόμβο προορισμού και ένα υποκλοπές με μία κεραία. Διερευνήθηκαν δύο σενάρια συλλογής ενέργειας που στοχεύουν στη μεγιστοποίηση της συλλογής ενέργειας για πηγή και επιλεγμένο ρελέ. Παρουσιάζονται οι αναλυτικές και ασυμπτωτικές εκφράσεις της πιθανότητας διακοπής μυστικότητας και για τα δύο πρωτόκολλα επιλογής ρελέ. Τα αριθμητικά αποτελέσματα δείχνουν ότι το ORS μπορεί να βελτιώσει σημαντικά την ασφάλεια του προτεινόμενου μοντέλου συστήματος και μπορεί να επιτύχει πλήρη σειρά ποικιλομορφίας απορρήτου, ενώ το PRS επιτυγχάνει μόνο τη σειρά ποικιλομορφίας μυστικότητας ανεξαρτήτως των στρατηγικών συγκομιδής ενέργειας. Το PRS που μεγιστοποιεί την ενεργειακή συγκομιδή για τη στρατηγική ρελέ έχει καλύτερη απόδοση μυστικότητας από εκείνη που βασίζεται στη μεγιστοποίηση της ενεργειακής συλλογής πόρων. Επιπλέον, τα αποτελέσματα δείχνουν ότι η απόρρητη απόδοση του υπό εξέταση συστήματος επηρεάζεται σημαντικά από τη διάρκεια της διαδικασίας συλλογής ενέργειας.

Για να αντιμετωπίσετε το ζήτημα της πολυπλοκότητας της επιλογής ρελέ σε ασφαλή αμφίδρομα ρελέ μεγάλης κλίμακας 5-συστημάτων ενίσχυσης και προώθησης (TWR-AF) με τεράστια ρελέ και υποκλοπές, Προτάθηκε ένα κατανεμημένο κριτήριο επιλογής αναμετάδοσης που δεν απαιτεί τις πληροφορίες των πηγών SNR, την εκτίμηση καναλιού ή τη γνώση των αναμεταδοτών συνδέσμων ρελέ. Η προτεινόμενη επιλογή ρελέ γίνεται με βάση την ισχύ των ρελέ και τη γνώση των μέσων πληροφοριών καναλιού μεταξύ της πηγής και του υποκλοπίου. Το μοντέλο του συστήματος περιλαμβάνει δύο κόμβους πηγής, έναν αριθμό νόμιμων κόμβων ρελέ και πολλαπλούς παθητικούς υποκλοπές. Κάθε κόμβος έχει μονή κεραία. Λαμβάνεται υπόψη η συνεργασία των μαρκίζων. Στο TWR-AF, τα λαμβανόμενα σήματα από τις δύο πηγές στο υποκλοπές σε κάθε κουλοχέρη επικαλύπτονται, όπου το σήμα μιας πηγής ενεργεί ως jamming noise. Τα αναλυτικά αποτελέσματα δείχνουν ότι ο αριθμός των σταγονόμετρων έχει σοβαρές επιπτώσεις στην απόδοση του απορρήτου. Τα αποτελέσματα της προσομοίωσης δείχνουν ότι η απόδοση του προτεινόμενου κριτηρίου χαμηλής πολυπλοκότητας είναι πολύ κοντά σε εκείνη του αντίστοιχου της βελτιστοποιημένης επιλογής.

Λαμβάνοντας υπόψη τους υποκλοπές και το ρελέ με μία και πολλές κεραίες, το , μελετά το σχεδιασμό μετάδοσης για ασφαλείς επικοινωνίες ρελέ σε δίκτυα 5G, υποθέτοντας ότι δεν υπάρχει καμία γνώση σχετικά με τον αριθμό ή τις θέσεις των σταγονόμετρων. Οι τοποθεσίες των υποκλοπών σχηματίζουν μια ομοιόμορφη Poisson Point Process. Προτείνεται μια αναμετάδοση τυχαιοποίησης και προώθησης για την εξασφάλιση επικοινωνιών πολλαπλών λυκίσκων. Η πιθανότητα διακοπής της μυστικότητας της μετάδοσης δύο λυκίσκων έχει προκύψει. Διατυπώνεται ένα πρόβλημα μεγιστοποίησης του ποσοστού απορρήτου με περιορισμό πιθανότητας διακοπής απορρήτου. Δίνει την βέλτιστη κατανομή ισχύος και ρυθμό κωδικής λέξης. Τα αποτελέσματα της προσομοίωσης δείχνουν ότι η πιθανότητα διακοπής της μυστικότητας μπορεί να βελτιωθεί με τον εξοπλισμό κάθε ρελέ με πολλαπλές κεραίες. Το απόρρητο αποτέλεσμα βελτιώνεται και η ασφαλής κάλυψη επεκτείνεται καταλλήλως χρησιμοποιώντας στρατηγικές αναμετάδοσης

2 ΤΕΧΝΗΤΟΣ ΘΟΡΥΒΟΣ

Μπορεί να εισαχθεί τεχνητός θόρυβος για την εξασφάλιση της προβλεπόμενης μετάδοσης σήματος. Με την ασφαλή μετάδοση πολλαπλών κεραιών με τεχνητό θόρυβο υπό στοχαστική γεωμετρία, Wanget al. πρότεινε μια πολιτική συσχέτισης που χρησιμοποιεί ένα όριο πρόσβασης για κάθε χρήστη για να συσχετιστεί με το BS, έτσι ώστε να μεγιστοποιηθεί η περικομμένη μέση ισχύς σήματος πέραν του ορίου και να μπορεί να αντιμετωπίσει τους υποκλοπείς που βρίσκονται σε κυρίαρχη θέση σε ένα ετερογενές κυψελοειδές δίκτυο. Εξετάζεται η ανιχνεύσιμη έκφραση πιθανότητας σύνδεσης και πιθανότητας μυστικότητας για έναν τυχαία εντοπισμένο χρήστη. Κάτω από τους περιορισμούς της σύνδεσης και της απόρρητης απόδοσης, παρουσιάζεται η απόδοση απορρήτου δικτύου και η ελάχιστη απόδοση

μυστικότητας κάθε χρήστη. Τα αριθμητικά αποτελέσματα παρουσιάζονται για την επαλήθευση της αναλυτικής ακρίβειας.

Υποθέτοντας ότι ο αποστολέας είναι οπλισμένος με πολλαπλές κεραίες, στο , προτείνεται μια τεχνητή στρατηγική μετάδοσης θορύβου για να ασφαλιστεί η μετάδοση έναντι ενός υποκλοπίου με μία κεραία σε συστήματα κυμάτων χιλιοστών. Το χιλιοστό κύμα καναλιού διαμορφώνεται με ένα μοντέλο χωρικού καναλιού που βασίζεται σε συστάδες ακτίνων. Ο αποστολέας έχει μερική γνώση CSI για εσάς. Η προτεινόμενη στρατηγική μετάδοσης εξαρτάται από τις κατευθύνσεις του προορισμού και τις διαδρομές διάδοσης του υποκλοπίου. Η πιθανότητα διακοπής της μυστικότητας χρησιμοποιείται για την ανάλυση του συστήματος μετάδοσης. Παρουσιάζεται μια βελτιστοποίηση που βασίζεται στην ελαχιστοποίηση της πιθανότητας διακοπής της μυστικότητας με περιορισμό του ποσοστού μυστικότητας. Για την επίλυση του προβλήματος βελτιστοποίησης, προκύπτει μια βέλτιστη κατανομή ισχύος κλειστής μορφής μεταξύ του σήματος πληροφοριών και του τεχνητού θορύβου. Αυτή η απόδοση του συστήματος κύματος χιλιοστών επηρεάζεται σημαντικά από τη σχέση μεταξύ των διαδρομών προορισμού του προορισμού και του υποκλοπίου. Τα αριθμητικά αποτελέσματα δείχνουν ότι η διακοπή της μυστικότητας συμβαίνει κυρίως εάν οι συχνές διαδρομές είναι μεγάλες ή ο υποκλοπής είναι κοντά στον μεταδότη.

Για να βελτιωθεί το ΕΕ της μεθόδου ασφαλείας χρησιμοποιώντας τεχνητό θόρυβο, διαμορφώνεται ένα πρόβλημα βελτιστοποίησης για τη μεγιστοποίηση του απορρήτου ΕΕ υποθέτοντας το ατελές CSI του υποκλοπής ανά πομπό. Το σύστημα είναι μοντελοποιημένο με έναν πομπό legal-mate με πολλαπλές κεραίες και έναν νόμιμο δέκτη και έναν υποκλοπέα, το καθένα με μία μόνο κεραία. Ο πομπός χρησιμοποιείται τεχνητός θόρυβος. Η ασφάλεια για αλγόριθμους ασύρματων δικτύων κινητής τηλεφωνίας 5G χρησιμοποιούνται για την επίλυση του προβλήματος βελτιστοποίησης με συσχέτιση μεταξύ κεραιών εκπομπής. Με τον συνδυασμό κλασματικού προγραμματισμού και διαδοχικής κυρτής βελτιστοποίησης, οι βέλτιστες λύσεις πρώτης τάξης υπολογίζονται με πολυωνυμική πολυπλοκότητα.

4) ΜΕΘΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Εκτός από τις λύσεις PLS που εισήχθησαν παραπάνω, κρυπτογραφικές μέθοδοι χρησιμοποιούνται επίσης για την εφαρμογή της εμπιστευτικότητας δεδομένων με κρυπτογράφηση δεδομένων με μυστικά κλειδιά. Η ασύμμετρη κρυπτογραφία μπορεί να εφαρμοστεί σε βασικές κατανομές. Για τη μείωση του κόστους κρυπτογράφησης, υιοθετείται συμμετρική κρυπτογραφία για κρυπτογράφηση δεδομένων.

Ένα συμμετέχον όχημα μπορεί να στείλει το τυχαίο συμμετρικό κλειδί του, το οποίο είναι κρυπτογραφημένο χρησιμοποιώντας το δημόσιο κλειδί της ΤΑ. Αυτό το συμμετρικό κλειδί χρησιμοποιείται για την κρυπτογράφηση του μηνύματος μεταξύ ΤΑ, DMV και συμμετεχόντων οχημάτων. Ένα εφάπαξ κλειδί κρυπτογράφησης κρυπτογραφείται επίσης από ένα δημόσιο κλειδί. Το εφάπαξ κλειδί κρυπτογράφησης χρησιμοποιείται για την κρυπτογράφηση του βίντεο. Ενα αρχικό κλειδί συμμετρίας διαπραγματεύεται μεταξύ του πελάτη και ενός γιατρού αφού καθορίσει τη σχέση πελάτη / διακομιστή. Το symmetric key στη συνέχεια χρησιμοποιείται για τη μετάδοση δεδομένων μεταξύ του πελάτη και του ιατρού.

Δ. ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

Η βασική διαχείριση είναι η διαδικασία ή η τεχνική που υποστηρίζει τη δημιουργία και τη διατήρηση σχέσεων κλειδιού μεταξύ εξουσιοδοτημένων μερών, όπου η σχέση κλειδιού είναι ο τρόπος κοινής χρήσης κοινών δεδομένων μεταξύ επικοινωνιών. Τα κοινά δεδομένα μπορεί να είναι δημόσια ή

μυστικά κλειδιά, τιμές αρχικοποίησης και άλλες μη μυστικές παραμέτρους. Για την παροχή ευέλικτης ασφάλειας, τρία πρωτόκολλα ανταλλαγής κλειδιών, τα οποία έχουν διαφορετικά επίπεδα υπολογιστικού χρόνου, υπολογιστικής πολυπλοκότητας και ασφάλειας, προτείνονται επικοινωνίες για D2D με βάση το σχήμα Diffie-Hellman (DH). Παρουσιάζεται η ανάλυση απειλών και των τριών προτεινόμενων προτύπων υπό κοινή ωμή δύναμη και επιθέσεις MITM Παρέχεται μελέτη απόδοσης για τα προτεινόμενα πρωτόκολλα για την αξιολόγηση της εμπιστευτικότητας, της ακεραιότητας, της εξουσιοδότησης και της μη αποποίησης των υπηρεσιών ασφαλείας με βάση τη θεωρητική ανάλυση. Η ανάλυση αποδεικνύει ότι τα προτεινόμενα πρωτόκολλα είναι εφικτά με λογική επικοινωνία γενικά και υπολογιστικό χρόνο. Για περιπτώσεις χρήσης ομάδας D2D, ένας μηχανισμός διαχείρισης κλειδιών ομάδας (GKM) για τη διασφάλιση της ανταλλαγής μηνυμάτων D2D, οι φάσεις ανακάλυψης και επικοινωνίας. Υπάρχουν πέντε απαιτήσεις ασφαλείας στο προτεινόμενο GKM, δηλαδή το εμπιστευτικό εμπρός (χρήστες που έχουν έφυγε από την ομάδα δεν πρέπει να έχει πρόσβαση στο μελλοντικό κλειδί), το απόρρητο απόρρητο (οι νέοι που συμμετέχουν στη συνεδρία δεν θα πρέπει να έχουν πρόσβαση στο παλιό κλειδί), η ελευθερία συμπαιγνίας (οι απατηλοί χρήστες δεν μπορούσαν να αφαιρέσουν την τρέχουσα κρυπτογράφηση κίνησης), ανεξαρτησία κλειδιού (τα κλειδιά σε μια ομάδα δεν πρέπει να είναι ικανός να ανακαλύψει κλειδιά σε άλλη ομάδα) και σχέση εμπιστοσύνης (δεν αποκαλύπτουν τα κλειδιά για οποιοδήποτε άλλο μέρος στον ίδιο τομέα ή οποιοδήποτε μέρος σε διαφορετικό τομέα). Σχέδιο κρυπτογράφησης (IBC) που βασίζεται σε ID που βασίζεται στην ελλειπτική καμπύλη κρυπτογράφησης (ECC) για Παρουσιάζεται η διασφάλιση της επικοινωνίας πολλαπλών ομάδων. Τα βήματα του προτεινόμενου πρωτοκόλλου περιλαμβάνουν τη δημιουργία μυστικών κλειδιών, τον αλγόριθμο ψηφιακής υπογραφής ελλειπτικής καμπύλης, την επαλήθευση υπογραφής, τη διαδικασία σχηματισμού ομάδας, τη δημιουργία κλειδιών, τη διαδικασία συμμετοχής και τη διαδικασία αποχώρησης. Οι γενιές κλειδιών και ιδιωτικών κλειδιών βασίζονται σε σχήματα IBC και ECC. Αξιολογούνται τα γενικά έξοδα για επικοινωνίες, επανασύνδεση μηνυμάτων και αποθήκευση κλειδιών. Η αδυναμία του σχήματος IBC και οι τρόποι δημιουργίας και χρήσης του GKMare συγκρίθηκαν. Οι συνολικές συγκρίσεις απόδοσης δείχνουν ότι το προτεινόμενο GKM έχει μια βελτίωση τόσο στην πολυπλοκότητα των προτύπων όσο και στο επίπεδο ασφάλειας σε σύγκριση με άλλα έργα. Το ECC υιοθετείται επίσης για το προτεινόμενο πρωτόκολλο LRSA. Ο διαχειριστής δικτύου δημιουργεί ένα μερικώς ιδιωτικό και μερικώς δημόσιο κλειδί για τον πελάτη και τον ιατρό μετά την εγγραφή. Και όταν ο πελάτης και ο γιατρός καθορίσουν τη σχέση πελάτη / διακομιστή, πρέπει να ρυθμιστεί μια αρχική συστηματική συνάντηση για τη μετάδοση δεδομένων.

Ε. ΙΔΙΩΤΙΚΟΤΗΤΑ

Όπως συζητήθηκε στις προηγούμενες ενότητες, τα ασύρματα δίκτυα 5G εγείρουν σοβαρές ανησυχίες σχετικά με τη διαρροή απορρήτου κατά την υποστήριξη περισσότερων και περισσότερων κάθετων βιομηχανιών όπως η υγειονομική περίθαλψη και η έξυπνη μεταφορά . Οι ροές δεδομένων σε ασύρματα δίκτυα 5G μεταφέρουν εκτενείς προσωπικές πληροφορίες απορρήτου όπως ταυτότητα, θέση και ιδιωτικό περιεχόμενο. Σε ορισμένες περιπτώσεις, το privacy leakage μπορεί να προκαλέσει σοβαρές συνέπειες. Ανάλογα με τις απαιτήσεις απορρήτου των εφαρμογών, η προστασία της ιδιωτικής ζωής είναι μια μεγάλη πρόκληση σε ασύρματα δίκτυα 5G. Έχουν ήδη πραγματοποιηθεί ερευνητικές εργασίες σχετικά με το απόρρητο της τοποθεσίας και την ιδιωτικότητα. Όσο αφορά το απόρρητο της τοποθεσίας, στο, για την προστασία της τοποθεσίας και των προτιμήσεων των χρηστών που μπορούν να αποκαλυφθούν με σχετικούς αλγόριθμους στο HetNets, προτείνεται ένας αποκεντρωμένος αλγόριθμος για επιλογή σημείου πρόσβασης με βάση ένα πλαίσιο παιχνιδιού που ταιριάζει μετρήστε τις προτιμήσεις των χρηστών κινητών συσκευών και των σταθμών βάσης με τις παραμέτρους του συστήματος φυσικών παικτών. Ο αλγόριθμος “Gale-Shapley” ταιριάζει με διαφορετικό τρόπο αναπτύσσεται με βάση τη διαφορετική προτεραιότητα. Τα βοηθητικά

προγράμματα των χρηστών κινητής τηλεφωνίας και τα σημεία πρόσβασης προτείνονται με βάση το ποσοστό επιτυχίας πακέτου. Τα αποτελέσματα προσομοίωσης δείχνουν ότι ο διαφορικά ιδιωτικός αλγόριθμος μπορεί να προστατεύσει το απόρρητο της τοποθεσίας με μια καλή ποιότητα υπηρεσιών με βάση τη χρησιμότητα των χρηστών κινητών. Μια αρχιτεκτονική συστήματος πρόληψης παρεμβολών για κινητά (mIPS) με γνώμονα τη βελτίωση της ιδιωτικής ζωής. Οι συγγραφείς παρουσίασαν τις απαιτήσεις mIPS, πιθανή διαρροή απορρήτου από διαχειριζόμενες υπηρεσίες ασφαλείας.

Το απόρρητο με βάση τα συμφραζόμενα ορίζεται ως το απόρρητο της πηγής δεδομένων και του προορισμού. Η ταυτότητα του πηγαίου πελάτη κρυπτογραφείται από μια ψευδο ταυτότητα του πελάτη προέλευσης με το δημόσιο κλειδί του γιατρού χρησιμοποιώντας τη λειτουργία κρυπτογράφησης χωρίς πιστοποίηση. Εν τω μεταξύ, η ταυτότητα του επιδιωκόμενου φυσικού κρυπτογραφείται επίσης με το δημόσιο κλειδί του διαχειριστή τότε. Μέσω αυτών των δύο βημάτων κρυπτογράφησης, μπορεί να επιτευχθεί το απόρρητο των συμφραζομένων. Για την προτεινόμενη υπηρεσία αναφοράς σ η προστασία της ιδιωτικής ζωής είναι απαραίτητη προϋπόθεση για την απόκτηση αποδοχής και συμμετοχής ατόμων. Οι πληροφορίες ταυτότητας και τοποθεσίας ενός οχήματος πρέπει να διατηρούνται κατά της παράνομης ανίχνευσης. Εν τω μεταξύ, ένα όργανο αναφοράς θα πρέπει να μπορεί να αποκαλύπτει την ταυτότητά του στις αρχές για ειδικές περιστάσεις. Τα ψευδώνυμα προγράμματα ελέγχου ταυτότητας εφαρμόζονται για την επίτευξη της υπό όρους ανωνυμίας και της ιδιωτικότητας

ΚΕΦΑΛΑΙΟ 4 / ΑΣΦΑΛΕΙΑ ΓΙΑ ΤΕΧΝΟΛΟΓΙΕΣ ΠΟΥ ΕΦΑΡΜΟΖΟΝΤΑΙ ΣΤΑ ΣΥΣΤΗΜΑΤΑ 5G

Σε αυτήν την ενότητα, παρουσιάζουμε τις ερευνητικές δραστηριότητες ασφάλειας από τις προοπτικές των τεχνολογιών που εφαρμόζονται στο 5G. Πρώτα παρουσιάζονται σύντομα οι τεχνολογίες που εφαρμόζονται στο 5G. Παρουσιάζονται οι δραστηριότητες ασφάλειας κάθε τεχνολογίας. Οι τεχνολογίες που εφαρμόζονται σε ασύρματα δίκτυα 5G που συζητούνται σε αυτήν την ενότητα είναι τα HetNet, τεράστια MIMO, D2D, SDN και IoT.

Α HETNET

Το HetNet είναι μια πολλή υποσχόμενη τεχνική για την παροχή κάλυψης ασύρματης κάλυψης και υψηλής απόδοσης σε ασύρματα δίκτυα 5G. Είναι ένα σύστημα πολλαπλών επιπέδων στο οποίο οι κόμβοι σε διαφορετικά επίπεδα έχουν διαφορετικά χαρακτηριστικά, όπως η ισχύς μετάδοσης, το κάλυμμα και οι τεχνολογίες ραδιοπρόσβασης. Με τα ετερογενή χαρακτηριστικά, το HetNet επιτυγχάνει υψηλότερη χωρητικότητα, ευρύτερη κάλυψη και καλύτερη απόδοση σε EE και SE. Ωστόσο, το HetNet architecture, σε σύγκριση με το κυψελοειδές δίκτυο ενός επιπέδου, καθιστά την UE πιο ευάλωτη στην υποκλοπή. Επιπλέον, με την υψηλή πυκνότητα μικρών κυττάρων στο HetNet, οι παραδοσιακοί μηχανισμοί μεταβίβασης θα μπορούσαν να αντιμετωπίσουν σημαντικά ζητήματα απόδοσης λόγω υπερβολικά συχνών μεταβιβάσεων μεταξύ διαφορετικών κυττάρων. Το ζήτημα της ιδιωτικότητας στο HetNet αντιμετωπίζει επίσης μια μεγάλη πρόκληση. Οι πληροφορίες τοποθεσίας γίνονται πιο ευάλωτες λόγω της υψηλής πυκνότητας των μικρών κυττάρων. Ο συμβατικός μηχανισμός συσχέτισης αποκάλυψε τις πληροφορίες απορρήτου τοποθεσίας.

Για την αντιμετώπιση των παραβίασης των επιθέσεων στο HetNet, προτείνεται μια πολιτική σύνδεσης μυστικού αυτοκινήτου με βάση τη μέγιστη περικομμένη μέση ισχύ σήματος (ARSP). Το maximum ARSP θα πρέπει να είναι υψηλότερο από ένα προκαθορισμένο όριο πρόσβασης ώστε το κινητό να παραμένει ενεργό. Διαφορετικά, η κινητή συσκευή παραμένει αδρανής. Έχει αναλυθεί η πιθανότητα σύνδεσης χρήστη και μυστικότητας της μετάδοσης τεχνητού θορύβου με την προτεινόμενη πολιτική σύνδεσης, η οποία βασίζεται σε ένα όριο πρόσβασης. Η απόδοση της απόρρητης απόδοσης μπορεί να βελτιωθεί σημαντικά με το κατάλληλο όριο πρόσβασης που χρησιμοποιείται στην πολιτική σύνδεσης

Για την ενίσχυση της κάλυψης επικοινωνίας στο HetNet, μπορεί να εφαρμοστεί συντονισμένη μετάδοση πολλαπλών σημείων (CoMP). Ωστόσο, το CoMP μπορεί να αυξήσει τον κίνδυνο να παρακολουθείται για τους νόμιμους χρήστες. Σε άλλη έρευνα, επιλέγονται πολλαπλά BS για τη μετάδοση του μηνύματος. Προτείνεται ένα δυναμικό σχήμα επιλογής BS βάσει της πιθανότητας ασφαλούς κάλυψης. Με βάση τα θεωρητικά και τα αποτελέσματα προσομοίωσης, οι συγγραφείς κατέληξαν στο συμπέρασμα ότι το κατάλληλο όριο επιλογής BS για το CoMP μπορεί να βελτιώσει την ασφαλή απόδοση κάλυψης.

Η διαχείριση πόρων βάσει ασφάλειας έχει χρησιμοποιηθεί για την εφαρμογή της ασφάλειας στο HetNet. Μελετήθηκε μια περίπτωση για τη βελτίωση του υπάρχοντος μπλοκαρίσματος και την αναμετάδοση των μηχανισμών προτείνοντας ένα σχήμα συνεργασίας πολλαπλών επιπέδων με τη βοήθεια των SBS για την προστασία του απορρήτου των επικοινωνιών χρηστών macrocell. Τα SBS παρακινούνται από το μπόνους ή το μπόνους πόρων για να γίνουν jammers για να βοηθήσουν τις ασφαλείς επικοινωνίες κάτω από τους περιορισμούς των δικών τους QoS

Λόγω της υψηλής πυκνότητας των μικρών κυψελών, η γνώση του κυττάρου με τον οποίο συσχετίζεται ένας χρήστης μπορεί εύκολα να αποκαλύψει τις πληροφορίες τοποθεσίας αυτού του χρήστη. Διερευνήθηκε το απόρρητο της τοποθεσίας βάσει φυσικού επιπέδου συσχετισμού αλγορίθμων στο 5G. Ένας διαφορικός ιδιωτικός αλγόριθμος Gale-Shapley προτείνεται για να

αποτρέψει τη διαρροή πληροφοριών τοποθεσίας με ορισμένο QoS για τους χρήστες. Η αξιολόγηση του αλγορίθμου που βασίζεται σε διαφορετικά επίπεδα απορρήτου παρουσιάζεται με την επίδραση στη χρησιμότητα των χρηστών.

Η προσέγγιση που βασίζεται στην ανίχνευση εισβολής θεωρείται ένας μόνος τρόπος παροχής ασφαλών επικοινωνιών. Σε έρευνα, εισάγονται τεχνικές ανίχνευσης παρεμβολών για φορητό υπολογιστικό νέφος, ανομοιογενής 5G. Διάφορες μέθοδοι ανίχνευσης-ολιγοί μελετώνται ως ανίχνευση βάσει υπογραφής, ανίχνευση βάσει ανωμαλιών, ανίχνευση βάσει προδιαγραφών, ανάλυση stateful protocol, ανιχνεύσεις υβριδικής εισβολής με αρχές αυτών των προσεγγίσεων. Η παραδοσιακή επικύρωση βάσει κωδικού πρόσβασης και ο βιομετρικός έλεγχος ταυτότητας συζητούνται για την παροχή διαφορετικών επιπέδων ασφάλειας.

B D2D

Σε επικοινωνίες D2D, οι συσκευές μπορούν να επικοινωνούν με κάθε άλλο χωρίς να περνούν BS Οι επικοινωνίες D2D επιτρέπουν την αποτελεσματική χρήση φάσματος σε 5G. Επιπλέον, οι επικοινωνίες D2D μπορούν αποτελεσματικά να εκφορτώσουν την κυκλοφορία από BS. Ωστόσο, η έλλειψη υποδομής ασφαλείας D2D καθιστά τις επικοινωνίες D2D λιγότερο ασφαλείς από τη συσκευή σε επικοινωνίες δικτύου. Για τη βελτίωση της SE, η πρόσβαση δυναμικών φασμάτων συνήθως υιοθετείται για συνδέσμους D2D, οι οποίοι απειλούν την ασφάλεια, όπως η παρεμβολή. Η έκδοση ασφαλείας αποτελεί μείζονα ανησυχία για τις άμεσες ραδιοεπικοινωνίες και την ανάπτυξη μεγάλης κλίμακας ομάδων D2D.

Η συνεργασία μεταξύ των κόμβων D2D είναι ένας δημοφιλής τρόπος για τη διασφάλιση των επικοινωνιών D2D εναντίον των υποκλοπών. Οι νόμιμοι πομποί με έναν κοινό δέκτη μπορούν να βελτιώσουν τον αξιόπιστο ρυθμό μετάδοσης μέσω της συνεργασίας. Πρόταση έγινε για ένα σχέδιο συνεργασίας για τη διασφάλιση των επικοινωνιών D2D λαμβάνοντας υπόψη την απόσταση. Πριν από τη συνεργασία, οι συσκευές μπορούν να ελέγξουν την απόσταση για να ελέγξουν εάν η συνεργασία μπορεί να βελτιώσει την ασφάλεια των επικοινωνιών. Οι περιορισμοί απόστασης μπορούν να χρησιμοποιηθούν για τον καθορισμό της από κοινού συνεργασίας, της συνεργασίας από τη μία πλευρά ή της μη συνεργασίας για τη μεγιστοποίηση του επιτεύξιμου ποσοστού απορρήτου. Χωρίς συγκεκριμένες απαιτήσεις για τις επικοινωνίες D2D, το προτεινόμενο σχέδιο μπορεί να εφαρμοστεί σε όλα τα σενάρια επικοινωνίας D2D.

Εκτός από τη συνεργασία, ο έλεγχος ισχύος και η πρόσβαση στα κανάλια θεωρούνται επίσης ασφαλείς επικοινωνίες D2D. Ο βέλτιστος έλεγχος ισχύος και η πρόσβαση στο κανάλι του συνδέσμου D2D προτείνονται για τη μεγιστοποίηση του επιτεύξιμου ρυθμού των κυψελοειδών χρηστών και του ποσοστού μυστικότητας φυσικού επιπέδου των συνδέσμων D2D.. Η λειτουργία χρησιμότητας ενός χρήστη D2D διαμορφώνεται λαμβάνοντας υπόψη την απαίτηση PLS και την πληρωμή παρεμβολών από άλλους χρήστες D2D. Χρησιμοποιείται μια προσέγγιση Stackelberg, όπου η τιμή από τους χρήστες κινητής τηλεφωνίας και η ισχύς μετάδοσης των χρηστών D2D είναι οπαδοί. Το πρόβλημα πρόσβασης στο κανάλι των συνδέσμων D2D συζητείται για τη μεγιστοποίηση του επιτεύξιμου ποσοστού μυστικότητας των συνδέσμων D2D και την ελαχιστοποίηση των παρεμβολών στους χρήστες κινητής τηλεφωνίας.

Η βαθμολογία ασφαλείας με βάση την πιθανότητα ανίχνευσης επίθεσης εφαρμόζεται για την πρόληψη, την αντίδραση και τον εντοπισμό επιθέσεων. Το μοτίβο συνεχούς νομιμότητας εισάγεται σε πακέτα για τον έλεγχο ταυτότητας της ακεραιότητας και της αυθεντικότητας των μεταδόσεων.

Λαμβάνοντας υπόψη τη βοήθεια του δικτύου, στο, προτείνονται πρωτόκολλα ανταλλαγής κλειδιών με τους δύο χρήστες D2D και κόμβο B. Εξετάζονται δύο σενάρια. Για το σενάριο offload κυκλοφορίας, οι χρήστες D2D είναι συνδεδεμένοι στο ίδιο κόμβο B. Για το σενάριο κοινωνικής δικτύωσης, απαιτείται

σύνδεσμος D2D για τις εφαρμογές σε κάθε χρήστη D2D. Το δημόσιο κανάλι κρυπτογραφημένο αποκλειστικό κανάλι εφαρμόζεται στη διαδικασία ανταλλαγής κλειδιών. Ο κόμβος Β εμπλέκεται στην αρχική ανταλλαγή κλειδιών και στον αμοιβαίο έλεγχο ταυτότητας των χρηστών D2D. Με βάση το ρόλο του κόμβου Β στη διαδικασία ελέγχου ταυτότητας, προτείνονται διαφορετικά πρωτόκολλα ανταλλαγής κλειδιών με διαφορετικό χρόνο και πολυπλοκότητα. Οι αλγόριθμοι ασφαλείας και οι λύσεις για δημόσια κυτταρικά συστήματα δεν είναι προσαρμοσμένοι στις επικοινωνίες D2D μικρής ραδιοφωνικής εμβέλειας. Τα ζητήματα ασφαλείας τόσο στις φάσεις εξυπηρέτησης όσο και στις επικοινωνίες για την επικοινωνία D2D παρουσιάζονται και αντιμετωπίζονται προτείνοντας έναν μηχανισμό διαχείρισης κλειδιών ομάδας χρησιμοποιώντας το IBC. Διανομές κλειδιών και ανάκληση κλειδιών είναι δύο προβλήματα στη διαχείριση κλειδιών ομάδας (GKM). Ορίζονται πέντε απαιτήσεις ασφάλειας του GKM και παρέχονται αντίστοιχες λύσεις.

Με την ανάπτυξη της τεχνικής D2D, οι εφαρμογές m-health υιοθετούνται για τη βελτίωση της αποτελεσματικότητας και της ποιότητας των υπηρεσιών υγειονομικής περίθαλψης. Οι απαιτήσεις ασφαλείας για επικοινωνίες D2D που χρησιμοποιούνται στο σύστημα m-health αναλύονται σε [45]. Το πρωτόκολλο πρέπει να ασφαλίζει τα δεδομένα που δεν είναι προσπελάσιμα από ρελέ και να επιτυγχάνει αμοιβαίο έλεγχο ταυτότητας μεταξύ της πηγής και του επιδιωκόμενου ιατρού χωρίς αλληλεπίδραση. Απαιτεί επίσης μικρό βάρος για τερματικά κινητής τηλεφωνίας με περιορισμούς ενέργειας και αποθήκευσης και πρέπει να είναι ισχυρός για την καταπολέμηση των απειλών, καθώς μέρος των κλειδιών μπορεί να εκτεθεί. Μια κρυπτογραφία δημόσιου κλειδιού χωρίς πιστοποιητικό εφαρμόζεται για την επίτευξη των απαιτήσεων ασφάλειας. Το ιδιωτικό κλειδί του χρήστη δημιουργείται τόσο από το κέντρο γεννήτριας κλειδιού όσο και από το χρήστη, γεγονός που καθιστά το κέντρο γεννήτριας κλειδιών αγνόητο για το ιδιωτικό κλειδί του χρήστη. Ο έλεγχος ταυτότητας επιτυγχάνεται αναγνωρίζοντας το δημόσιο κλειδί. Οι στόχοι ασφαλείας του δικτύου m-health ορίζονται ως εμπιστευτικότητα και ακεραιότητα δεδομένων, αμοιβαία εξουσιοδότηση, ανωνυμία σε οποιονδήποτε εκτός από τον προοριζόμενο γιατρό, αποσύνδεση, ασφάλεια προς τα εμπρός και προστασία της ιδιωτικής ζωής.

Γ. MASSIVE MIMO

Χρησιμοποιώντας μεγάλο αριθμό κεραιών σε BS, το massMIMO μπορεί να παρέχει υψηλό EE και SE για να υποστηρίζει περισσότερους χρήστες ταυτόχρονα. Ο μεγάλος αριθμός κεραιών στα BS μπορεί να βελτιώσει σημαντικά την απόδοση, την απόδοση EE και να μετατοπίσει στο έπακρο την επεξεργασία σήματος και τον υπολογισμό από τα τερματικά χρήστη σε BSs. Επιπλέον, το τεράστιο MIMO μπορεί να βελτιώσει την ασφάλεια των επικοινωνιών. Θεωρείται PLS για ένα σύστημα HetNet K-tier κάτω σύνδεσης με multiple eavesdroppers. Κάθε MBS είναι εξοπλισμένο με μεγάλες συστοιχίες κεραιών που χρησιμοποιούν γραμμική μηδενική διαμόρφωση δέσμης. Τόσο τα θεωρητικά αποτελέσματα ανάλυσης όσο και τα αποτελέσματα προσομοίωσης δείχνουν ότι το τεράστιο MIMO μπορεί να βελτιώσει σημαντικά την πιθανότητα διακοπής της μυστικότητας των χρηστών macrocell.

Ωστόσο, το eavesdropper μπορεί να χρησιμοποιήσει μαζικό MIMO για να επιτεθεί στις νόμιμες επικοινωνίες. Στο μοντέλο συστήματος θεωρείται τεράστιο MIMO τόσο στο BS όσο και στο υποκλοπές. Οι συστοιχίες κεραιών του υποκλοπίου είναι πολύ πιο ισχυρές. Παρουσιάζεται η προσέγγιση OSPR. Η θεωρητική ανάλυση και η ανάλυση προσομοίωσης δείχνουν ότι το antenna number στο BS μπορεί να επηρεάσει σημαντικά την απόδοση ασφαλείας. Με τον αριθμό των κεραιών στο BS να είναι αρκετά υψηλός, το τεράστιο υποκλοπές MIMO αποτυγχάνει να αποκωδικοποιήσει την πλειοψηφία των αρχικών συμβόλων, ενώ οι νόμιμοι χρήστες μπορούν να ανακτήσουν τα αρχικά σύμβολα με περιορισμένο μόνο αριθμό κεραιών. Σε σύγκριση με άλλες προσεγγίσεις που εμπλέκονται στο jamming, η προτεινόμενη μέθοδος έχει υψηλότερο EE.

Δ. SDN

Αποσυνδέοντας το επίπεδο ελέγχου από το επίπεδο δεδομένων, το SDN συγκεντρώνει τον έλεγχο του δικτύου και φέρνει υποσχόμενες μεθόδους για να κάνει τη διαχείριση του δικτύου απλούστερη, πιο προγραμματιζόμενη και πιο ελαστική. Οι πληροφορίες μπορούν να μοιραστούν μεταξύ κελιών χρησιμοποιώντας SDN. Το SDN μπορεί να παρέχει ιδιότητες, δηλαδή λογικά συγκεντρωτική νοημοσύνη, προ-προγραμματισμό και αφαίρεση, έτσι ώστε η επεκτασιμότητα και η ευελιξία του δικτύου να μπορούν να βελτιωθούν πολύ και να μειωθεί σημαντικά το κόστος.

Στην πηγή 9 συζήτησαν τα πλεονεκτήματα και τα μειονεκτήματα του SDNsecurity. Τα πλεονεκτήματα της ασφάλειας SDN σε παραδοσιακά δίκτυα φαίνονται στον Πίνακα. 1. Εκτός από τα πλεονεκτήματα του SDN που φέρνει τα ασύρματα δίκτυα 5G, τα νέα ζητήματα ασφαλείας που προκαλούνται από το SDN παρουσιάζονται στον Πίνακα. 3, μαζί με πιθανά αντίμετρα.

Στην πηγή 22 συζήτησαν τους περιορισμούς στα δίκτυα κινητής τηλεφωνίας. Προτείνεται μια αρχιτεκτονική SDMN που αποτελείται από εφαρμογή, επίπεδο ελέγχου και επίπεδο δεδομένων, που ενσωματώνει SDN, NFV και cloud computing. Οι μηχανισμοί ασφαλείας στα κλασικά κυψελοειδή δίκτυα παρουσιάζονται με τους περιορισμούς τους. Εισάγονται τα αναμενόμενα πλεονεκτήματα ασφαλείας του SDMN. Παρατίθενται οι προοπτικές ασφαλείας που μπορούν να βελτιωθούν μέσω του SDMN. Εκτός από τα πλεονεκτήματα του SDMN, παρουσιάζονται επίσης φορείς απειλής για την αρχιτεκτονική SDMN. Στο [35], αναπτύσσονται τα ανοιχτά ζητήματα ασφαλείας 5G και βασίζονται στην εμπιστοσύνη NFV και SDN Προτείνονται αντίστοιχα πλαίσια ασφάλειας και εμπιστοσύνης, τα οποία χρησιμοποιούν το NFV TrustPlatform ως υπηρεσία, τη λειτουργία ασφαλείας ως υπηρεσία και τις λειτουργίες εμπιστοσύνης ως υπηρεσία (Πλεονεκτήματα της sdn ασφάλειας).

SDN characteristic	Attributed to	Security use
Global network view	Centralization Traffic statistics collection	Network-wide intrusion detection Detection of switch's malicious behavior Network forensics
Self-healing mechanisms	Conditional rules Traffic statistics collection	Reactive packet dropping Reactive packet redirection
Increased control capabilities	Flow-based forwarding scheme	Access control

Λόγω της υψηλής πυκνότητας των μικρών κυττάρων σε 5G, η διαχείριση των κλειδιών είναι δύσκολη με τον χρήστη να συνδέεται συχνά και να αφήνει αυτά τα μικρά κελιά. Επιπλέον, η επιτάχυνση της διαδικασίας ελέγχου ταυτότητας είναι απαραίτητη για την εξασφάλιση της απαίτησης χαμηλού λανθάνοντος χρόνου σε 5G.ο SDN εισάγεται στο μοντέλο συστήματος για να επιτρέψει τον συντονισμό μεταξύ διαφορετικών ετερογενών κυττάρων. Χρησιμοποιείται ένας ελεγκτής SDN για την παρακολούθηση και την πρόβλεψη των τοποθεσιών των χρηστών. Τα χαρακτηριστικά πολλαπλών φυσικών επιπέδων λαμβάνονται συνεχώς δείγματα από τον ελεγκτή SDN για να δείξει την απόδοση του συνδυασμού πολλαπλών SCI. Προτείνονται οι σταθμισμένοι κανόνες σχεδιασμού και απόφασης SCI. Η λειτουργία SDN χρησιμοποιεί την προτεραιότητα στην ουρά και η κυκλοφορία που φθάνει διαμορφώνεται ως παράδοση. Η απόδοση λανθάνουσας κατάστασης της πιστοποίησης βάσει SDN φαίνεται να είναι καλύτερη από την απόδοση παραδοσιακών κρυπτογραφικών μεθόδων που βασίζονται σε διαφορετικές τοποθεσίες φόρτωσης. Με κοινόχρηστο SCI μέσω SDN, το πλαίσιο ασφαλείας μπορεί να έχει υψηλότερο επίπεδο ανοχής για να αντιμετωπίσει τις αποτυχίες του τότε δικτύου.

E. IoTD

Λόγω της περιορισμένης δυνατότητας υπολογισμού των κόμβων IoT, οι υπηρεσίες ασφαλείας σε συσκευές 5G IoT πρέπει να είναι αποτελεσματικές και ελαφριές. Η αναμετάδοση θεωρείται ως αποτελεσματικός μηχανισμός στα δίκτυα IoT για εξοικονόμηση ενέργειας των κόμβων IoT και επίσης επέκταση της κάλυψης μετάδοσης.

Σε έρευνα, ένα κέντρο σύντηξης χρησιμοποιείται για την προστασία κόμβων IoT με απεριόριστη ισχύ υπολογισμού από το jammer. Κάθε κόμβος IoT είναι εξοπλισμένος με αισθητήρα για την ανίχνευση των παρεμβολών. Η κεντρική σχέση μεταξύ κάθε κόμβου IoT λαμβάνεται υπόψη για τη μέτρηση της σημασίας του κόμβου μέσω του δικτύου. Οι αποκεντρωμένες μετρήσεις παρεμβολών συλλέγονται στο κέντρο σύντηξης σε τακτά χρονικά διαστήματα σε ένα κοινό κανάλι ελέγχου. Χρησιμοποιείται ένα ορισμένο κατώφλι επιπέδου και συγκεντρωτικό επίπεδο ισχύος παρεμβολής για να προσδιοριστεί εάν υπάρχει επίθεση jamming ή όχι. Οι συγγραφείς υπέθεσαν ότι ο jammer γνωρίζει την τοπολογία του δικτύου και εκχωρεί σωστά συγκεκριμένη ισχύ παρέμβασης στους IoT nodes για να μειώσει το SINR τους. Το κέντρο σύντηξης μπορεί επίσης να κατανείμει το εύρος ζώνης σε ορισμένους κόμβους για να μετρήσει το επίπεδο παρεμβολής προκειμένου να ανιχνεύσει την επίθεση jammer. Επομένως, ένα μη συνεργαζόμενο παιχνίδι συνταγματάρχης Blotto μεταξύ του jammer και του κέντρου σύντηξης σχηματίζεται ως πρόβλημα διανομής πόρων.

Σε άλλη έρευνα, η ασφάλεια των επικοινωνιών ρελέ στα δίκτυα IoT καθιερώνεται λαμβάνοντας υπόψη την κατανομή ισχύος και τη σχεδίαση ρυθμού κωδικών μέσω μετάδοσης δύο λυκίσκων έναντι κατανεμημένων υποκλοπών. Το πρόβλημα διατυπώνεται για μεγιστοποίηση του ποσοστού απορρήτου. Λαμβάνονται υπόψη και οι θήκες μονής και πολλαπλής κεραίας σε ρελέ και υποκλοπές. Αποδεικνύεται ότι η σωστή μετάδοση ρελέ μπορεί να επεκτείνει την ασφαλή κάλυψη και η αύξηση του αριθμού των κεραιών στους ρελέ συνδέσεων μπορεί να βελτιώσει το επίπεδο ασφάλειας.

Το RFID είναι μια τεχνολογία αυτόματης αναγνώρισης και συλλογής δεδομένων που χρησιμοποιείται ευρέως σε δίκτυα IoT. Προτείνεται ένα πρόγραμμα ανάκλησης ασφαλούς εφαρμογής RFID για αποτελεσματική και ασφαλή χρήση RFID πολλαπλών εφαρμογών και ανάκληση εφαρμογών στην ετικέτα. Με βάση τη θεωρητική ανάλυση, το προτεινόμενο σχήμα μπορεί να επιτύχει υψηλότερο επίπεδο ασφάλειας από άλλα υπάρχοντα προγράμματα.

ΕΠΙΛΟΓΟΣ

Τα ασύρματα δίκτυα 5ης γενιάς αναμένεται ήδη παρέχουν προηγμένη απόδοση για να επιτρέψουν πολλές νέες εφαρμογές να αναπτυχθουν. Σε αυτό το άρθρο, παρουσιάσαμε μια ολοκληρωμένη μελέτη για την πρόσφατη ανάπτυξη της ασύρματης ασφάλειας 5G. Οι τρέχουσες λύσεις ασφαλείας βασίζονται κυρίως στις παρεχόμενες υπηρεσίες ασφαλείας, όπως πιστοποίηση, διαθεσιμότητα, εμπιστευτικότητα δεδομένων, διαχείριση κλειδιών και απόρρητο. Πολλά νέα χαρακτηριστικά ασφαλείας στο 5G αναμένονται λόγω των εφαρμογών τεχνολογιών όπως HetNet, D2D, τεράστιο MIMO, SDN και IoT. Η ασφάλεια που περιλαμβάνει αυτές τις τεχνολογίες έχει συνοψιστεί. Τέλος, παρουσιάσαμε τις προκλήσεις και τις μελλοντικές κατευθύνσεις της ασύρματης ασφάλειας 5G.

ΒΙΒΛΟΓΡΑΦΙΚΕΣ ΠΗΓΕΣ

1 N. Panwar, S. Sharma, and A. K. Singh, ‘‘A survey on 5G: The next generation of mobile communication,’’Phys. Commun., vol. 18,pp. 64–84, Mar. 2016.

2 5G Vision, 5G PPP, Feb. 2015.

3 NGMN 5G White Paper, NGMN Alliance, Frankfurt, Germany, Feb. 2015.

4 J. G. Andrewset al., ‘‘What will 5G be?’’IEEE J. Sel. Areas Commun.,vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

5 Understanding 5G: Perspectives on Future Technological Advancementsin Mobile, GSMA Intelligence, London, U.K., Dec. 2014.

6 M. Agiwal, A. Roy, and N. Saxena, ‘‘Next generation 5G wireless net-works: A comprehensive survey,’’IEEE Commun. Surveys Tuts., vol. 18,no. 3, pp. 1617–1655, 3rd Quart., 2016.

7 J. Qiao, X. Shen, J. Mark, Q. Shen, Y. He, and L. Lei, ‘‘Enabling device-to-device communications in millimeter-wave 5G cellular networks,’’IEEECommun. Mag., vol. 53, no. 1, pp. 209–215, Jan. 2015.

8 L. Wei, R. Q. Hu, Y. Qian, and G. Wu, ‘‘Energy efficiency and spectrumefficiency of multihop device-to-device communications underlaying cel-lular networks,’’IEEE Trans. Veh. Technol., vol. 65, no. 1, pp. 367–380,Jan. 2016.

9 M. Dabbagn, B. Hu, M. Guizani, and A. Rayes, ‘‘Software-defined net-working security: Pros and cons,’’IEEE Commun. Mag., vol. 53, no. 6,pp. 73–79, Jun. 2015.

10 J. Zhang, W. Xie, and F. Yang, ‘‘An architecture for 5G mobile networkbased on SDN and NFV,’’ inProc. 6th Int. Conf. Wireless, Mobile Multi-Media (ICWMMN), Nov. 2015, pp. 87–92.

[11]5G Security Recommendations Package: Network Slicing, NGMNAlliance, Glasgow, U.K., Apr. 2016.

12 ‘‘5G security,’’ Ericsson, Stockholm, Sweden, White Paper, Jun. 2015.

13 The Road to 5G: Drivers, Applications, Requirements and TechnicalDevelopment, GSA, Washington, DC, USA, Nov. 2015.

14 Leading the World to 5G, QualComm, San Diego, CA, USA, Feb. 2016.

15 ‘‘5G security: Forward thinking Huawei white paper,’’ Huawei, Shenzhen,China, White Paper, 2015.

16 S. Vij and A. Jain, ‘‘5G: Evolution of a secure mobile technology,’’ inProc.3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom), Mar. 2015,pp. 2192–2196.

17 J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, ‘‘A survey on security aspectsfor LTE and LTE-A networks,’’IEEE Commun. Surveys Tuts., vol. 16,no. 1, pp. 283–302, 1st Quart., 2014.

18 A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, ‘‘SeDS: Secure data sharing strat-egy for D2D communication in LTE-advanced networks,’’IEEE Trans.Veh. Technol., vol. 65, no. 4, pp. 2659–2672, Apr. 2016.

19 M. Wang, Z. Yan, and V. Niemi, ‘‘UAKA-D2D: Universal authenticationand key agreement protocol in D2D communications,’’Mobile Netw. Appl.,vol. 22, no. 3, pp. 510–525, 2017.

20 Security Challenges and Opportunities for 5G Mobile Networks, Nokia,Espoo, Finland, 2017.

[21]5G Security Recommendations Package #1, NGMN Alliance, Glasgow,U.K., May 2016.

22 M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, ‘‘Opportunitiesand challenges of software- defined mobile networks in network security,’’IEEE Security Privacy, vol. 14, no. 4, pp. 34–44,
Jul./Aug. 2016

23 V. G. Vassilakis, I. D. Moscholios, and B. A. Alzahrani, ‘‘On the securityof software-defined next- generation cellular networks,’’ inProc. IEICE Inf.Commun. Technol. Forum (ICTF), 2016, pp. 61–65.

24 H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, ‘‘Physicallayer security in heterogeneous cellular networks,’’IEEE Trans. Commun.,vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

25 Y. Deng, L. Wang, K. K. Wong, A. Nallanathan, M. Elkashlan, andS. Lambotharan, ‘‘Safeguarding massive MIMO aided HetNets usingphysical layer security,’’ inProc. Int. Conf. Wireless Commun. SignalProcess. (WCSP), Oct. 2015, pp. 1–5.

26 M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang,‘‘Software-defined mobile networks security,’’Mobile Netw. Appl.,vol. 21, no. 5, pp. 729–743, 2016.

27 F. Tian, P. Zhang, and Z. Yan, ‘‘A survey on C-RAN security,’’IEEEAccess, vol. 5, pp. 13372–13386, 2017.

28 Q. Fang, Z. WeiJie, W. Guojun, and F. Hui, ‘‘Unified security architectureresearch for 5G wireless system,’’ inProc. 11th Web Inf. Syst. Appl. Conf.,2014, pp. 91–94.

29 P. Schneider and G. Horn, ‘‘Towards 5G Security,’’ inProc.Trustcom/BigDataSE/ISPA, Aug. 2015, pp. 1165–1170.

30 W. Stallings,Cryptography and Network Security: Principles and Prac-tice, 6th ed. London, U.K.: Pearson, 2014.