Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Κρυπτογραφία και Ασφάλεια στο Διαδίκτυο των Πραγμάτων (IoT): Αλγόριθμοι, Μηχανισμοί και Υλοποιήσεις

Ιωάννης Χρυσάιδος

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Δεκέμβριος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Κρυπτογραφία και Ασφάλεια στο Διαδίκτυο των Πραγμάτων (IoT): Αλγόριθμοι, Μηχανισμοί και Υλοποιήσεις

Ιωάννης Χρυσάιδος

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά και Επικοινωνιακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2017

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Στη σημερινή εποχή η ανάπτυξη της τεχνολογίας επιτρέπει την διασύνδεση όλο και περισσότερων συσκευών ή συστημάτων. Έτσι δημιουργήθηκε το Διαδίκτυο των Πραγμάτων, το Internet of Things (IoT), που είναι ο άξονας για να μπορούν να συνδεθούν ετερόκλητες συσκευές με διαφορετικές ιδιότητες για να προσφέρουν ποικίλες υπηρεσίες. Όλα αυτά πρέπει να γίνονται με ασφαλή τρόπο. Σε αυτήν την διατριβή θα δούμε πως η κρυπτογράφηση μπορεί να προσφέρει ασφάλεια στη διασύνδεση. Γίνεται επισκόπηση των αρχών της κρυπτογραφίας, αναφερόμενοι στην κλασική και στη σύγχρονη κρυπτογραφία, και στην ασφάλεια των κρυπτογραφικών συστημάτων. Στη συνέχεια αναφερόμαστε στο Διαδίκτυο των Πραγμάτων, και γίνεται παρουσίαση των αλγόριθμων κρυπτογράφησης. Έχουμε μετά μια σύντομη αναφορά στους μηχανισμούς ασφάλειας και στα πρωτόκολλα ασφάλειας. Βλέπουμε αναλυτικά αρχιτεκτονικές και πρωτόκολλα στο IoT, και τρόπους αντιμετώπισης επιθέσεων. Γίνεται μια παρουσίαση σχεδιασμών και υλοποιήσεων, ενώ στο τέλος γίνεται εισήγηση μιας νέας πρότασης με αυξημένη ασφάλεια.

Summary

In today's times the development of technology allows the interconnection of more and more devices or systems. This created the Internet of Things, the Internet of Things (IoT), which is the basis for connecting heterogeneous devices with different properties to offer a variety of services. All this must be done in a safe way. In this thesis we will see how encryption can provide security for the interconnection. An overview of the principles of cryptography is given, referring to classical and modern cryptography, and to the security of cryptographic systems. Then we refer to the Internet of Things, and we present the encryption algorithms. We then have a brief reference to security mechanisms and security protocols. We analyze architectures and protocols in IoT, and how to deal with attacks. A presentation of designs and implementations is made, while in the end a new combination having increased security is introduced.

Ευχαριστίες

Με εκτίμηση θα ήθελα να ευχαριστήσω τον καθηγητή μου Κον Νικόλαο Σκλάβο.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Από τα πρώτα χρόνια που οι άνθρωποι άρχισαν να ζουν σε οργανωμένα κράτη υπήρχε η ανάγκη να επικοινωνούν μεταξύ τους. Αρχικά αυτή η επικοινωνία γινόταν προφορικά, και μεταγενέστερα με γραπτό λόγο. Πολλές φορές αυτή η επικοινωνία δεν έπρεπε να γίνει γνωστή σε γειτονικές-εχθρικές κοινωνίες, ακόμη και αν έπεφτε στα χέρια των αντιπάλων ο κομιστής της αλληλογραφίας. Από τότε υπάρχει η έννοια της κρυπτογραφίας, δηλαδή ένα μήνυμα να τροποποιείται-μετασχηματίζεται με τέτοιο τρόπο ώστε να είναι κατανοητό μόνο από τον αποδέκτη, ο οποίος γνωρίζει τον τρόπο απομετασχηματισμού. Ένας από τους γνωστότερους αλγόριθμους κρυπτογράφησης είναι ο αλγόριθμος του Ιούλιου Καίσαρα [1], που χρησιμοποιείτο για επικοινωνία ανάμεσα στις λεγεώνες. Αυτό είναι ένας αλγόριθμος αντικατάστασης, σε επόμενα κεφάλαια θα δούμε αναλυτικά μεθόδους-αλγορίθμους κρυπτογράφησης, δηλαδή κάθε γράμμα του κειμένου αντικαθίσταται από το γράμμα του λατινικού αλφαβήτου που βρίσκεται τρεις θέσεις μετά αν έχουμε διατάξει με αλφαβητική σειρά τα γράμματα. Για να διαβάσουμε το κρυπτοκείμενο, δηλαδή το κρυπτογραφημένο κείμενο, αντικαθιστούμε κάθε γράμμα αυτού με εκείνο που βρίσκεται τρεις θέσεις πριν στη σειρά του αλφαβήτου.

Την κρυπτογραφία τη χρησιμοποιήσαμε για την ασφαλή μεταφορά ή και αποθήκευση δεδομένων, παρακάτω θα δούμε ότι δεν είναι μόνο αυτή η χρήση της κρυπτογραφίας, αλλά δεν έχουμε διευκρινίσει τι είναι ασφάλεια. Η ασφάλεια είναι ο όρος της προστασίας από τον κίνδυνο ή την απώλεια. Πιο συγκεκριμένα η Επιτροπή Εθνικών Συστημάτων Ασφαλείας των ΗΠΑ (Committee on National Security Systems, CNSS) ορίζει την ασφάλεια των πληροφοριών ως την προστασία των πληροφοριών και των κρίσιμων στοιχείων τους, συμπεριλαμβανομένων των συστημάτων και του υλικού που χρησιμοποιεί, αποθηκεύει και μεταδίδει αυτές τις πληροφορίες [2]. Η ασφάλεια

πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές αρχές: Ακεραιότητα (Integrity), Διαθεσιμότητα (Availability), Εμπιστευτικότητα (Confidentiality).

Η **ακεραιότητα** αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

Η **διαθεσιμότητα** των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Η **εμπιστευτικότητα** σημαίνει ότι ευαίσθητες πληροφορίες δεν θα πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα [1].

Λέγοντας διαδίκτυο των πραγμάτων (Internet of Things - IoT) εννοούμε 'Το Internet of Things' είναι μία έννοια που αφορά τη διασύνδεση αντικειμένων της καθημερινότητας μας, από βιομηχανικές μηχανές μέχρι συσκευές που μπορούν να φορεθούν (wearable), οι οποίες χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων, και την ανάληψη δράσης κάποιων από αυτά, μέσα σε ένα δίκτυο. Κάπως έτσι λειτουργεί ένα κτίριο που χρησιμοποιεί αισθητήρες (sensors) και ελεγκτές (controlers) για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού. Άλλο παράδειγμα είναι ένας εξοπλισμός παραγωγής που προειδοποιεί το προσωπικό συντήρησης για μία επικείμενη βλάβη. Με απλά λόγια το Internet of Things είναι το τεχνολογικό μέλλον που θα κάνει τη ζωή μας πιο εύκολη [3]. Επίσης 'Το IoT επιτρέπει οποιαδήποτε προς οποιαδήποτε συνδεσιμότητα. Έξυπνα κτίρια, HVAC (Κεντρικές Θερμάνσεις, Εξαερισμοί, Αιρ Κοντίσιον) και ακόμη φυσικές τεχνολογίες ασφαλείας είναι πλέον συνδεδεμένα, όπως είναι φορητές έξυπνες συσκευές και περισσότερα. Το τελευταίο κύμα του «πράγματα» που συνδέονται με χρήστες, επιχειρήσεις και άλλα «πράγματα», που χρησιμοποιούν μείγμα ενσύρματης και ασύρματης συνδεσιμότητας, περιλαμβάνει αλλά δεν περιορίζεται σε αυτοκίνητα, αεροπλάνα, ιατρικά μηχανήματα, προσωπικές (εμφυτευμένες) ιατρικές συσκευές και τα συστήματα SCADA (supervisory control and data acquisition, συστήματα αυτόματου ελέγχου και τηλεμετρίας) πχ ανεμόμυλους, περιβαλλοντικούς αισθητήρες, πλατφόρμες εξόρυξης φυσικού αέριου, υδροηλεκτρικά συστήματα, και οτιδήποτε άλλο μπορούμε να φανταστούμε' [4].

Είναι προφανές ότι η έννοια του διαδικτύου των πραγμάτων είναι κάτι πολύ ευρύ και περιλαμβάνει σχεδόν οτιδήποτε μπορεί να διασυνδεθεί, γεγονός που έρχεται φυσικά σε

συμφωνία με τον ορισμό της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunication Union- ITU) που ορίζει: 'Διαδίκτυο των πραγμάτων (IoT): Μια παγκόσμια υποδομή για την κοινωνία της πληροφορίας, που επιτρέπει προηγμένες υπηρεσίες που διασυνδέουν (φυσικά και εικονικά) αντικείμενα που βασίζονται σε υπάρχουσες και εξελισσόμενες διαλειτουργικές τεχνολογίες πληροφοριών και επικοινωνιών' [5] [6]. Όπως είπαμε η ασφάλεια είναι κάτι πολύ σημαντικό, επομένως και στο IoT θα πρέπει να φροντίζουμε να υπάρχει ασφάλεια στα διάφορα διασυνδεόμενα αντικείμενα ή συσκευές, η οποία υλοποιείται και με χρήση κρυπτογραφίας [7], ενώ θα πρέπει, όπως και σχεδόν σε οποιαδήποτε θέμα, να λαμβάνουμε υπ' όψη και το κόστος που έχει η ασφαλής 'παρουσία' των συμμετεχόντων στο τεράστιο δίκτυο που αποτελεί το IoT [8].

Κεφάλαιο 2
Θεωρητικό Υπόβαθρο

Η μετάβαση από αναλογικά και έντυπα μέσα και διαδικασίες στα ψηφιακά αντίστοιχα τους, κάτι που συμβαίνει συνεχώς και σε όλους σχεδόν τους τομείς της ανθρώπινης δραστηριότητας, είναι μια διαδικασία σύνθετη. Ο αναλογικός και έντυπος κόσμος είχε πετύχει ένα ικανοποιητικό επίπεδο προστασίας και ασφαλείας, π.χ. χειρόγραφες υπογραφές, σφραγίδες, χαρακτηριστικά ασφαλείας χαρτονομισμάτων κ.λ.π. προσφέροντας μια βεβαιότητα για την αυθεντικότητα τους. Αυτά τα χαρακτηριστικά ασφάλειας και σιγουριάς προσπαθεί να συνεχίσει η κρυπτογραφία στην ψηφιοποιημένη πληροφορία.

2.1 Κρυπτογραφία

Κρυπτογραφία σύμφωνα με τη βιβλιογραφία είναι η επιστήμη της απόκρυψης ενός μηνύματος. Πιο συγκεκριμένα κρυπτογραφία είναι η μαθηματική επιστήμη που αναφέρεται στο μετασχηματισμό δεδομένων, ώστε να μετατραπούν σε ακατάληπτα (απόκρυψη σημειολογικού περιεχομένου), να εμποδιστούν τροποποιήσεις που δεν μπορούν να εντοπιστούν, να εμποδιστεί η μη εξουσιοδοτημένη χρήση τους. Αν η μετατροπή είναι αναστρέψιμη, η κρυπτογραφία αναφέρεται και στην επαναφορά των κρυπτογραφημένων δεδομένων σε κατανοητή μορφή [9].

Αυτά φανερώνουν ότι η κρυπτογραφία αφορά την προστασία και εξασφάλιση των δεδομένων. Η διαδικασία που ακολουθείται είναι:

Το αρχικό-απλό μήνυμα-κείμενο (plaintext) με την κρυπτογράφηση (encryption) , που κάνει ο αποστολέας-δημιουργός, γίνεται κρυπτογραφημένο κείμενο ή κρυπτοκείμενο ή κρυπτογράφημα (ciphertext) και με την αποκρυπτογράφηση που κάνει ο παραλήπτης (decryption) ανακτάται το αρχικό μήνυμα.

Αντίστοιχα η κρυπτανάλυση (cryptanalysis) είναι η μελέτη μαθηματικών τεχνικών με σκοπό την αναίρεση των κρυπτογραφικών μεθόδων, δηλαδή να ‘διαβάσουμε’ το μήνυμα-κείμενο ενώ δεν είμαστε οι πραγματικοί παραλήπτες και δεν γνωρίζουμε τον

αλγόριθμο κρυπτογράφησης. Στεγανογραφία χαρακτηρίζουμε την πρακτική της ενσωμάτωσης ενός μηνύματος σε ένα φορέα, μεταβάλλοντας τον φορέα με μη εμφανή και ανεπαίσθητο τρόπο, με στόχο την απόκρυψη του μηνύματος από τρίτους. Η ψηφιακή υδατογράφηση είναι επίσης η ενσωμάτωση ενός μηνύματος σχετικού με ένα φορέα, με ανεπαίσθητη μεταβολή του φορέα. Εδώ σκοπός δεν είναι τόσο η απόκρυψη του μηνύματος αλλά η αυθεντικοποίηση, ή η απόδειξη αδιαβλητότητας ή εγκυρότητας του φορέα-μηνύματος. Δηλαδή η κρυπτογραφία, η κρυπτανάλυση, η στεγανογραφία και η Ψηφιακή υδατογράφηση αποτελούν τους κλάδους της κρυπτολογίας [1].

2.1.1 Κλασική Κρυπτογραφία

Πολύ πριν τον αλγόριθμο του Καίσαρα, που αναφέρθηκε στην εισαγωγή, οι άνθρωποι χρησιμοποιούσαν τεχνικές για να μπορούν να επικοινωνούν με μυστικότητα. Εικάζεται ότι γύρω στα 1900 π.Χ. οι αρχαίοι Αιγύπτιοι χρησιμοποιούσαν κατάλληλα τροποποιημένα ιερογλυφικά για να κρύψουν τα μηνύματα τους. Η πρώτη επίσημη καταγραφή χρήσης κρυπτογραφίας αφορά μια πήλινη πινακίδα, γραμμένη σε σφηνοειδή γραφή που βρέθηκε στον Τίγρη ποταμό (1500-1700 π.Χ.), έχοντας οδηγίες για την εφυάλωση (κάλυψη με υαλώδες επίχρισμα) κεραμικών, με χρήση σπάνιων και δυσνόητων συμβόλων παράλληλα με χρήση αμφισημιών και βραχυγραφιών [1].

Η κλασική κρυπτογραφία χρησιμοποιεί την αντικατάσταση και μετάθεση των χαρακτήρων του αρχικού κειμένου (plaintext) για να προκύψει το κρυπτογραφημένο κείμενο (shiphertext).

Αλγόριθμους αντικατάστασης λέμε εκείνους που κάθε σύμβολο του αρχικού κειμένου αντικαθίσταται από κάποιο άλλο σύμβολο με βάση κάποιους κανόνες. Στην κλασική κρυπτογραφία έχουμε του παρακάτω αλγόριθμους αντικατάστασης:

- **Απλός ή μονοαλφαβητικός** αλγόριθμος αντικατάστασης (κάθε χαρακτήρας του αρχικού κειμένου αντικαθίσταται από ένα αντίστοιχο στο κρυπτογράφημα).
- **Ομοφωνικός** αλγόριθμος αντικατάστασης (ένας χαρακτήρας του αρχικού κειμένου μπορεί να αντικατασταθεί από δυο ή περισσότερους χαρακτήρες στο κρυπτογράφημα).
- **Πολυγραμμικός** αλγόριθμος αντικατάστασης (ομάδες χαρακτήρων του αρχικού αντικαθίστανται από αντίστοιχες ομάδες στο κρυπτογράφημα).
- **Πολυαλφαβητικός** αλγόριθμος αντικατάστασης (αποτελεί εφαρμογή περισσοτέρων του ενός αλγορίθμων αντικατάστασης, που χρησιμοποιούνται με

κάποια κριτήρια, π.χ. σύμφωνα με τη θέση κάθε χαρακτήρα στο αρχικό κείμενο χρησιμοποιείται ο αντίστοιχος απλός αλγόριθμος αντικατάστασης).

Αλγόριθμους μετάθεσης-αντιμετάθεσης λέμε εκείνους στους οποίους το αρχικό μήνυμα παραμένει ίδιο, με διαφοροποίηση της αλληλουχίας των συμβόλων.

Χαρακτηριστικό των κλασικών αλγόριθμων κρυπτογράφησης είναι ότι η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης είναι η ίδια (αντίστροφη).

2.1.2 Σύγχρονη Κρυπτογραφία

Πολύ εύκολα έγινε αντιληπτό ότι η ασφάλεια ενός αλγορίθμου κρυπτογράφησης δεν μπορεί να βασίζεται στη μυστικότητα αυτού του ίδιου του αλγόριθμου, αργά η γρήγορα θα διαρρεύσει . Η λύση για αυτό είναι η χρήση μιας μυστικής-κρυφής ποσότητας που λέγεται κλειδί (key) και ανάλογα με την τιμή αυτού παράγεται από τον ίδιο αλγόριθμο διαφορετικό αποτέλεσμα. Η ασφάλεια ενός αλγορίθμου έγκειται στη μυστικότητα του κλειδιού του (Αρχή του Kerckhoff, Ο Φλαμανδός Auguste Kerckhoff είχε δημοσιεύσει το άρθρο 'La Cryptographie Militaire' το 1883). Στον αλγόριθμο του Καίσαρα το 'κλειδί' είναι η μετατόπιση κατά τρία γράμματα προς τα δεξιά. Με διαφορετικό κλειδί , μετατόπιση κατά π.χ. επτά χαρακτήρες προκύπτει διαφορετικό κρυπτοκείμενο.

Η κρυπτογραφία σαν επιστήμη ξεκίνησε στο τέλος του Β' Παγκοσμίου Πολέμου μαζί με τη θεωρία πληροφορίας από τον Claude E. Shannon [1].

Στη σύγχρονη κρυπτογραφία διακρίνονται τρία βασικά αρχέτυπα:

- **Τα αρχέτυπα χωρίς κλειδί (unkeyed primitives)**: Οι συναρτήσεις κατακερματισμού (Hash Functions), οι μονόδρομες συναρτήσεις (one way functions) και οι τυχαίες συναρτήσεις (randon functions).
- **Τα αρχέτυπα συμμετρικού ή μυστικού κλειδιού (symmetric or secret key primitives)**: Τα αρχέτυπα αυτά διαφοροποιούν την έξοδο τους ανάλογα με το κλειδί που χρησιμοποιείται, το οποίο είναι το ίδιο κατά την κρυπτογράφηση και κατά την αποκρυπτογράφηση. Σε αυτά ανήκουν οι αλγόριθμοι κρυπτογράφησης τμήματος (block ciphers), κρυπτογράφησης ροής (stream ciphers) και οι κώδικες αυθεντικοποίησης μηνύματος (message authentication codes MAC) .
- **Τα αρχέτυπα ασύμμετρου ή δημοσίου κλειδιού (asymmetric or public key primitives)**: Επίσης και εδώ η έξοδος εξαρτάται από το κλειδί, με τη διαφορά ότι το κλειδί κρυπτογράφησης διαφέρει από το κλειδί αποκρυπτογράφησης. Σε αυτά ανήκουν οι αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού, π.χ. ο RSA (από τα ονόματα των δημιουργών **R**ivest Ron, **S**hamir Adi, **A**dleman Leonard, ο

οποίος βασίζεται στο δύσκολο μαθηματικό πρόβλημα της παραγοντοποίησης μεγάλων αριθμών, χρησιμοποιεί κλειδιά μήκους 1024 έως 4096 bits, με συνιστώμενο μήκος τα 2048 bits).

Μονόδρομες είναι οι συναρτήσεις που μπορούν εύκολα να υπολογιστούν, αλλά είναι δύσκολο να αντιστραφούν, δηλαδή ο υπολογισμός της τιμής f(x) από το x είναι εύκολος, αλλά ο υπολογισμός του x από το f(x) έχει πρακτικά αμελητέα πιθανότητα [1].

Οι τυχαίες συναρτήσεις είναι αυτές που μπορούν να παράγουν ακολουθίες από τυχαία ψηφία (bits). Στην πράξη δεν μπορεί να συμβεί αυτό, οπότε έχουμε τις ψευδοτυχαίες συναρτήσεις οι οποίες παράγουν μεγάλες ακολουθίες από bits ξεκινώντας από μια μικρή ακολουθία τυχαίων bits, η οποία καλείται τυχαίος σπόρος (random seed). Οι παραγόμενες ακολουθίες φαινομενικά έχουν όλα τα απαραίτητα χαρακτηριστικά για να χαρακτηριστούν τυχαίες αποκρύπτοντας το γεγονός ότι έχουν δημιουργηθεί νε ένα σαφή ντετερμινιστικό κανόνα από ένα μικρό αριθμό τυχαίων bit [1].

Η συνάρτηση κατακερματισμού ή σύνοψης δέχεται σαν είσοδο ένα κείμενο οποιουδήποτε μεγέθους και επιστρέφει ένα πλήθος δυαδικών χαρακτήρων σταθερού προκαθορισμένου μεγέθους, που λέγεται σύνοψη ή ίχνος ή αποτύπωμα, και δεν εξαρτάται από το αρχικό κείμενο αλλά από την ίδια τη συνάρτηση. Προφανώς μπορεί σε διαφορετικό κείμενο να αντιστοιχηθεί η ίδια σύνοψη, πράγμα μη επιθυμητό. Έτσι ορίστηκαν οι μονόδρομες συναρτήσεις κατακερματισμού για τις οποίες είναι υπολογιστικά ανέφικτο να υπολογιστεί η αντιστροφή της. Δηλαδή γνωρίζοντας την τιμή σύνοψης είναι ανέφικτο υπολογιστικά να ανακτήσουμε το αρχικό κείμενο. Αν μάλιστα είναι υπολογιστικά ανέφικτο να βρεθούν δύο κείμενα που δημιουργούν την ίδια σύνοψη, αυτές ονομάζονται μονόδρομες συναρτήσεις κατακερματισμού ανθεκτικές σε συγκρούσεις. Γνωστές συναρτήσεις κατακερματισμού είναι η οικογένεια των MD2, MD4, MD5 (Message Digest) που θεωρούνται ανασφαλείς. Η οικογένεια των SHA-1, SHA-2 (Secure Hash Algorithm) είναι διαδεδομένες με τη SHA-2 να είναι το προτεινόμενο πρότυπο για συναρτήσεις κατακερματισμού κατά το NIST (National Institute of Standards and Technology). Έχει ‘βγει’ και η SHA-3, με πρότυπο τον αλγόριθμο Keccak, που αποτελεί παράλληλο πρότυπο από το 2015, για τις συναρτήσεις κατακερματισμού [1] [10] [11].

Οι συναρτήσεις κατακερματισμού μπορούν να χρησιμοποιηθούν για την επαλήθευση της προέλευσης (data origin authentication) και την επαλήθευση της ακεραιότητας του περιεχομένου (data integrity) ενός μηνύματος, δηλαδή επαληθεύει την αυθεντικότητα του. Μια τέτοια διαδικασία, πέραν μιας ασφαλούς συνάρτησης κατακερματισμού απαιτεί και ένα διαμοιραζόμενο μυστικό κλειδί, και ονομάζεται κώδικας αυθεντικοποίησης μηνύματος (message authentication code – MAC). Ένας αλγόριθμος MAC ή διαφορετικά μια συνάρτηση κατακερματισμού με κλειδί δέχεται δύο εισόδους, ένα μυστικό κλειδί και το προς αυθεντικοποίηση μήνυμα. Για παράδειγμα, έχουμε δύο χρήστες που γνωρίζουν ένα μυστικό κλειδί και θέλουν να επικοινωνήσουν. Όταν ο πρώτος θέλει να στείλει ένα μήνυμα στον δεύτερο, τότε υπολογίζει το MAC σαν συνάρτηση του μηνύματος και του μυστικού κλειδιού, και το επισυνάπτει στο μήνυμα που στέλνει στον δεύτερο. Ο παραλήπτης εκτελεί τον ίδιο υπολογισμό και συγκρίνει τα MAC ,εάν είναι ίδια τότε ο παραλήπτης επιβεβαιώνει την ακεραιότητα του μηνύματος, ότι δηλαδή δεν έχει αλλαχθεί κατά την μετάδοση του, επιβεβαιώνει ακόμα ότι το μήνυμα προέρχεται από τον συγκεκριμένο αποστολέα που μοιράζονται το μυστικό κλειδί. Έχουμε επομένως τον έλεγχο ακεραιότητας και αυθεντικότητας του μηνύματος [1].

Ο πλέον διαδεδομένος αλγόριθμος συμμετρικού κλειδιού ήταν ο DES - Data Encryption Standard και οι παραλλαγές του, που είναι ένα αλγόριθμος τμήματος. Διαπιστώθηκε ότι τελικά ήταν ευάλωτος σε κρυπτανάλυση και δεν έχει πλέον συχνή χρήση (η παραλλαγή – εξέλιξη αυτού, ο αλγόριθμος 3DES, θεωρείται και σήμερα ασφαλής λύση). Ένας άλλος αλγόριθμος συμμετρικού κλειδιού είναι ο αλγόριθμος Rijndael που αποτέλεσε, και εξακολουθεί να αποτελεί το πρότυπο κρυπτογράφησης, Advanced Encryption Standard (AES), με το όνομα AES/Rijndael. Μέχρι αυτή τη στιγμή τα αποτελέσματα προσπαθειών κρυπτανάλυσης δεν προκαλούν λόγους σοβαρής ανησυχίας. Γνωστός αλγόριθμος ροής είναι ο RC4 – Rivest Cipher 4, με ικανοποιητική ασφάλεια μέχρι το 2013. Οι αλγόριθμοι συμμετρικού κλειδιού προσφέρουν μεγάλη ασφάλεια, είναι γρήγοροι. Η αδυναμία τους είναι να μπορέσει να παραμείνει μυστικό το κλειδί, το οποίο πρέπει να το γνωρίζουν μόνο οι δυο που επικοινωνούν. Οι ασύμμετροι αλγόριθμοι είναι πιο αργοί από τους συμμετρικούς και για αυτό δεν χρησιμοποιούνται σε μεγάλου μεγέθους μηνύματα, αλλά κυρίως για την κρυπτογράφηση κλειδιών. Οι συμμετρικοί αλγόριθμοι χρησιμοποιούνται για κρυπτογράφηση δεδομένων, υλοποιούνται σχετικά εύκολα σε ολοκληρωμένα κυκλώματα [12].

Το πρόβλημα της μυστικότητας του κλειδιού λύνεται μέσω έμπιστης τρίτης οντότητας, ενός κέντρου διανομής κλειδιών (Key Distribution Center- KDC) με χρήση ενός κλειδιού συνόδου (session key) που είναι το συμμετρικό κλειδί κρυπτογράφησης που χρησιμοποιείται μόνο μια φορά, και ένα κύριο κλειδί (master key) που είναι ένα για κάθε ζεύγος χρηστών, δεν μεταβάλλεται και χρησιμοποιείται για την ασφαλή διανομή του κλειδιού μεταξύ των χρηστών με τη μεσολάβηση του KDC. Σε μεγάλα δίκτυα η ύπαρξη ενός μόνο KDC είναι δυσλειτουργική, οπότε χρησιμοποιείται ιεραρχία από KDC όπου το ένα εμπιστεύεται το άλλο. Τα κέντρα διανομής κλειδιών δημιουργήθηκαν για να λυθεί το θέμα της μυστικότητας του κοινού κλειδιού. Επίσης η διανομή μπορεί να γίνει μέσω αλγόριθμων δημόσιου κλειδιού [13].

Για να λειτουργήσει ένα σύστημα ασύμμετρης κρυπτογραφίας χρησιμοποιείται ένα ζεύγος κλειδιών. Τα ένα ονομάζεται δημόσιο κλειδί (public key) και είναι γνωστό σε όλους τους πιθανούς χρήστες του συστήματος. Το άλλο ονομάζεται ιδιωτικό κλειδί (private key) και είναι γνωστό μόνο σε ένα συγκεκριμένο χρήστη του συστήματος. Το δημόσιο και το ιδιωτικό έχουν πολύπλοκη μαθηματική σχέση μεταξύ τους (παραγοντοποίηση μεγάλων ακέραιων αριθμών, διακριτός λογάριθμος, διακριτός λογάριθμος σε ελλειπτικές καμπύλες ανάλογα με τον αλγόριθμο που χρησιμοποιείται), και η γνώση του δημόσιου κλειδιού δεν επιτρέπει με οποιοδήποτε τρόπο τον υπολογισμό του ιδιωτικού κλειδιού. Η διαδικασία είναι ότι ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το δημόσιο κλειδί. Η αποκρυπτογράφηση του μηνύματος μπορεί να γίνει μόνο από τον δικαιούχο χρησιμοποιώντας το ιδιωτικό του κλειδί. Και εδώ υπάρχει το πρόβλημα της αυθεντικότητας του δημόσιου κλειδιού.

Αυτό λύνεται με τη χρήση αξιόπιστων αρχών, TTP - Trusted Third Party , μια οντότητα που διευκολύνει τις αλληλεπιδράσεις μεταξύ δύο μερών που εμπιστεύονται αυτό το τρίτο μέρος. Οι βασικές λειτουργίες των TTP είναι, η δημιουργία ζεύγους ιδιωτικού δημόσιου κλειδιού, αποθήκευση και διαχείριση του ζεύγους κλειδιών, υπηρεσίες διαπιστοποίησης, υπηρεσίες χρονοσήμανσης, υπηρεσίες επίλυσης διαφορών, υπηρεσίες διατήρησης αποδεικτικών στοιχείων.
Μια αρχή πιστοποίησης - CA Certificate ή Certification Authority είναι μια οντότητα-αρχή έμπιστη από τους συναλλασσόμενους, η οποία εκδίδει ψηφιακά πιστοποιητικά,

ανανεώνει πιστοποιητικά, κάνει ανάκληση πιστοποιητικών, αναστέλλει ή ενεργοποιεί πιστοποιητικά και κάποιες επιπρόσθετες λειτουργίες οπότε αναφέρεται ως TTP, την οποία αναφέραμε παραπάνω [14].

Ένα ψηφιακό πιστοποιητικό πιστοποιεί την κατοχή ενός δημόσιου κλειδιού, ότι δηλαδή ανήκει σε μόνο μια συγκεκριμένη οντότητα και συνεπώς η οντότητα αυτή είναι ο νόμιμος κάτοχος του αντίστοιχου ιδιωτικού κλειδιού. Ο κάτοχος ενός ψηφιακού πιστοποιητικού μπορεί να υπογράψει ψηφιακά. Ένα ψηφιακό πιστοποιητικό βασίζεται στο πρότυπο X.509 και τα βασικότερα στοιχεία που περιλαμβάνει είναι, το αναγνωριστικό του πιστοποιητικού (τύπος-πρότυπο, έκδοση, σειριακός αριθμός, αλγόριθμος υπογραφής), περίοδος ισχύος (από-έως), πληροφορίες εκδότη (διακριτικό όνομα, σημείο πρόσβασης, αναγνωριστικό κλειδιού), υποκείμενο, δηλαδή ποιον αφορά (πλήρες διακριτικό όνομα του κατόχου του πιστοποιητικού), δημόσιο κλειδί που αντιστοιχεί στο υποκείμενο, ψηφιακή υπογραφή του εκδότη σε όλη τη δομή.

Το σύνολο των πρωτόκολλων, προτύπων, ρόλων, πολιτικών και διαδικασιών που χρειάζονται για τη διαχείριση-στήριξη εφαρμογών κρυπτογραφίας δημόσιου κλειδιού, λέγεται υποδομή δημόσιου κλειδιού (Public Key Infrastructure-PKI). Μια υποδομή PKI περιλαμβάνει εκτός από την αρχή πιστοποίησης (CA), την αρχή εγγραφής (Registration Authority) η οποία επαληθεύει την ταυτότητα των οντοτήτων που ζητούν ψηφιακά πιστοποιητικά, το αποθετήριο πιστοποιητικών (Certificate Repository) στο οποίο αποθηκεύονται με ασφάλεια τα πιστοποιητικά, ένα σύστημα διαχείρισης για την πρόσβαση ή διανομή των πιστοποιητικών ενώ παράλληλα επιτρέπει σε απομακρυσμένες οντότητες να πιστοποιούν η μία την ταυτότητα της άλλης. Σε μια δομή PKI εκδίδονται, διαχειρίζονται (πχ. ανακαλούνται ή ανανεώνονται), διανέμονται, ψηφιακά πιστοποιητικά τα οποία περιέχουν ψηφιακές υπογραφές, επιτρέποντας σε απομακρυσμένες οντότητες να πιστοποιεί η μια την ταυτότητα της άλλης. Μια Αρχή Πιστοποίησης δεν είναι μόνη της αλλά συμμετέχει σε ένα ιεραρχικό δίκτυο από αντίστοιχες αρχές, όπου η μια μπορεί να πιστοποιεί την άλλη (διαπιστοποίηση), μέσα από ένα μονοπάτι πιστοποίησης, μια αλυσίδα Αρχών Πιστοποίησης. Ένας χρήστης που αναγνωρίζει και αποδέχεται μια Αρχή Πιστοποίησης, αποδέχεται και τα πιστοποιητικά που έχουν εκδοθεί από μια άλλη για την οποία υπάρχει ένα μονοπάτι εμπιστοσύνης με την αρχή που ο χρήστης αποδέχεται.

Η ψηφιακή υπογραφή είναι δεδομένα που επισυνάπτονται σε ένα ηλεκτρονικό κείμενο με στόχο την επαλήθευση της ταυτότητας του αποστολέα και της ακεραιότητας του μηνύματος. Μια ψηφιακή υπογραφή έχει ιδιότητες όπως, μόνο ο υπογράφων μπορεί να την δημιουργήσει, παρέχει την δυνατότητα αναγνώρισης του υπογράφοντα, είναι μονοσήμαντα συνδεδεμένη με το σχετικό κείμενο με τρόπο ώστε να διασφαλίζεται η ακεραιότητα του χωρίς να μπορεί να μεταφερθεί σε άλλο κείμενο, ο υπογράφων δεν μπορεί εκ των υστέρων να αρνηθεί ότι δημιούργησε την υπογραφή, και περιλαμβάνει μια χρονοσφραγίδα. [14].

Έχοντας αναφερθεί στα κλειδιά, η διαχείριση τους είναι ένα σύνθετο πρόβλημα, το οποίο για να λυθεί απαιτεί εκτός από τεχνολογικές λύσεις, εφαρμογή πολιτικών (policy) διαχείρισης, και νομικών οδηγιών. Η διαχείριση των κλειδιών περιλαμβάνει επιγραμματικά:
Παραγωγή κλειδιών, ανταλλαγή κλειδιών, επιβεβαίωση κατοχής κλειδιού, ανανέωση κλειδιών, χρήση κλειδιών, αποθήκευση κλειδιών, διαφύλαξη κλειδιών, τον κύκλο ζωής των κλειδιών και την καταστροφή των κλειδιών [1].

2.2 Ασφάλεια

Για να έχουμε μια πιο ολοκληρωμένη άποψη για την ασφάλεια των κρυπτογραφικών συστημάτων θα πρέπει να δούμε ποιες απαιτήσεις ασφαλείας πρέπει να τηρούνται, τι είναι ασφαλές σύστημα, και ποιες μέθοδοι υπάρχουν για να μπορέσουν να ‘σπάσουν’ την ασφάλεια που προσφέρουν τα κρυπτογραφικά συστήματα, δηλαδή η κρυπτανάλυση όπως αναφέραμε και παραπάνω. Αναφέρουμε κάποιους όρους που σχετίζονται με την ασφάλεια και είναι καλό να τους κατανοήσουμε. Όταν γίνεται μια προσπάθεια μη εξουσιοδοτημένης πρόσβασης ή χρήσης, ή καταστροφής ή τροποποίησης ή κλοπής ενός αγαθού, που εκμεταλλεύεται συνήθως μια ευπάθεια, λέμε ότι έχουμε μια επίθεση (attack). Μια πιθανή αιτία που μπορεί να προκαλέσει ζημιά σε ένα αγαθό ονομάζεται απειλή (threat) [15].

2.2.1 Ασφάλεια Κρυπτογραφικών Συστημάτων

Σε συνέχεια αυτών που αναφέραμε στην εισαγωγή, εκτός των τριών βασικών απαιτήσεων ασφαλείας, έχουμε και μερικές άλλες, οι οποίες δεν είναι απόλυτες γιατί οι ανάγκες ασφαλείας καθορίζονται από το εκάστοτε περιβάλλον [1].

Ταυτοποίηση-Αυθεντικοποίηση οντότητας (entity identification-authentication). Οι ταυτότητες των υποκειμένων (χρηστών) θα πρέπει να μπορούν να επιβεβαιωθούν. Ένας μη εξουσιοδοτημένος χρήστης ή ένας επιτιθέμενος δεν πρέπει να μπορεί να παραστήσει ένα νόμιμο χρήστη ή οντότητα. Στην πραγματικότητα αυτές οι δύο έννοιες δεν είναι ταυτόσημες. Με την ταυτοποίηση μια οντότητα-χρήστης μας λέει ποια είναι, και με την αυθεντικοποίηση μας αποδεικνύει ότι είναι αυτή που λέει (όνομα χρήστη, κωδικός χρήστη).

Αυθεντικοποίηση μηνύματος (message authentication, data origin authentication). Ο παραλήπτης θα πρέπει να μπορεί να επιβεβαιώσει την πηγή προέλευσης του μηνύματος. Η 'ορθότητα' του μηνύματος αφορά την απαίτηση της ακεραιότητας.

Μη αποποίηση ευθύνης (non repudiation). Αποτροπή άρνησης πρότερης δέσμευσης ή πράξης. Πιο συγκεκριμένα στην επικοινωνία οντοτήτων. Ο αποστολέας θα πρέπει να μη μπορεί να αρνηθεί, εκ των υστέρων, ότι απέστειλε ένα μήνυμα, ενώ ο παραλήπτης θα πρέπει να μη μπορεί να αρνηθεί, εκ των υστέρων, ότι έλαβε ένα μήνυμα.

Ο Claude E. Shannon εκτός από θεμελιωτής της Θεωρίας της Πληροφορίας, περιέγραψε και τις βασικές ιδιότητες ενός τέλειου κρυπτογραφικού συστήματος. Η ύπαρξη των ιδιοτήτων σε ένα κρυπτοσύστημα είναι υποχρεωτική, αλλά συγχρόνως και αντιφατική, με αποτέλεσμα να μην υπάρχει στην πραγματικότητα κρυπτοσύστημα το οποίο να ικανοποιεί όλα τα μέτρα στο μέγιστό τους [10]. Δηλαδή δεν είναι δυνατό να υπάρξει ένα τέλειο κρυπτογραφικό σύστημα, σύμφωνα με αυτά. Έτσι πρότεινε κάποιες βασικές ιδιότητες που πρέπει να έχουν τα κρυπτογραφικά συστήματα για να προσφέρουν ασφάλεια:

- **Διάχυση** (Diffusion): Η ικανότητα του συστήματος-αλγόριθμου κρυπτογράφησης όπου ένα τμήμα του απλού κειμένου να έχει την ευκαιρία να επηρεάζει όσο το δυνατόν περισσότερα τμήματα του κρυπτοκειμένου, δηλαδή κάθε ψηφίο (bit) του αρχικού μηνύματος πρέπει να επηρεάζει όσο γίνεται περισσότερα ψηφία του κρυπτοκειμένου.
- **Σύγχυση** (Confusion): είναι η ικανότητα του συστήματος-αλγόριθμου κρυπτογράφησης όπου ο αντίπαλος δεν είναι σε θέση να προβλέψει ποιες μεταβολές θα συμβούν στο κρυπτοκείμενο, δεδομένης μιας μεταβολής στο απλό κείμενο, δηλαδή η σχέση μεταξύ του κρυπτοκειμένου και του μυστικού κλειδιού πρέπει να είναι σύνθετη, έτσι ώστε ακόμα από τα στατιστικά χαρακτηριστικά του κρυπτοκειμένου να μην είναι εφικτή η ανάκτηση του κλειδιού λόγω ακριβώς

του σύνθετου τρόπου με τον οποίο επέδρασε το κλειδί κατά την παραγωγή του κρυπτοκειμένου.

Οι αρχές αυτές εφαρμόζονται σήμερα στην πράξη, αφού λαμβάνονται υπ' όψιν στην κατασκευή κρυπτογραφικών αλγορίθμων. Σύνθετες (όχι απλές) αντικαταστάσεις εισάγουν σύγχυση. Πολλαπλές αντιμεταθέσεις εισάγουν διάχυση.

Οι έννοιες της διάχυσης και της σύγχυσης αποτελούν τον ακρογωνιαίο λίθο στη σχεδίαση κρυπτογραφικών αλγορίθμων[10].

Η αποτίμηση της ασφάλειας ενός κρυπτογραφικού συστήματος με καθορισμό αντικειμενικών μέτρων μέτρησης είχε σαν αποτέλεσμα τον καθορισμό μοντέλων[10].

- **Απεριόριστη (άνευ όρων) ασφάλεια** (Unconditional security). Ένα κρυπτοσύστημα είναι άνευ όρων ασφαλές όταν το κρυπτοκείμενο δεν δίνει καμία πληροφορία στον αντίπαλο σχετικά με το απλό κείμενο. Η υπόθεση απαιτεί ότι ο αντίπαλος έχει άπειρη υπολογιστική ισχύ στη διάθεσή του, δηλαδή ανεξάρτητα του πόσο μεγάλο τμήμα του κρυπτοκειμένου είναι γνωστό, δεν υπάρχει αρκετή πληροφορία για την ανάκτηση του αρχικού μηνύματος, τονίζοντας πάλι ότι ο επίδοξος υποκλοπέας διαθέτει άπειρη υπολογιστική ισχύ.
- **Υπολογιστική ασφάλεια** (computationally security). Σε αυτό το μοντέλο εισάγεται πλέον η παράμετρος της δυνατότητας χρήσης υπολογιστικής ισχύος του αντιπάλου. Ένα κρυπτοσύστημα είναι υπολογιστικά ασφαλές, όταν προκειμένου να το σπάσει ο αντίπαλος απαιτείται υπολογιστική ισχύς πέραν των δυνατοτήτων του. Δηλαδή είναι αδύνατον με τους υπάρχοντες υπολογιστικούς πόρους (ισχύ υπολογιστών, δυνατότητα αλγορίθμων) να ανακτήσει ένας υποκλοπέας το αρχικό μήνυμα, εάν γνωρίζει το κρυπτοκείμενο.

Υπάρχουν και άλλα μοντέλα αλλά είτε δεν έχουν πρακτική αξία είτε είναι υποσύνολα των ήδη αναφερομένων. Παρατηρούμε ότι το μοντέλο που έχει πρακτική αξία είναι αυτό της υπολογιστικής ασφάλειας. Φροντίζουμε το κρυπτογραφικό σύστημα να προσφέρει ασφάλεια πέραν της υπάρχουσας υπολογιστικής αξίας. Αυξανομένης όμως της ισχύος συστήματα που εθεωρούντο ασφαλή, παύουν να είναι. Αυτό μπορεί να δημιουργήσει προβλήματα ασφαλείας μέχρι να γίνει αντιληπτό ότι έχει 'σπάσει' το σύστημα. Έτσι συνεχώς θα έχουμε αυτόν τον κύκλο βελτίωσης-ενίσχυσης των συστημάτων μέχρι να καταστούν μη αξιόπιστα λόγω των εξελίξεων και της εκ νέου βελτίωσης-αλλαγής αυτών.

2.2.2 Κρυπτανάλυση

Η ασφάλεια ενός κρυπτογραφικού συστήματος έγκειται στη μυστικότητα του κλειδιού του, όπως ήδη έχουμε αναφέρει. Επομένως κάποιος επιτιθέμενος που θέλει να ανακτήσει από το κρυπτοκείμενο το αρχικό κείμενο, χωρίς φυσικά να ξέρει το κλειδί κρυπτογράφησης, θεωρούμε ότι γνωρίζει αναλυτικά τον αλγόριθμο κρυπτογράφησης. Έχουμε τις παρακάτω κατηγορίες κρυπτανάλυσης-κρυπτογραφικών επιθέσεων που αφορούν τον αλγόριθμο [16] [1]:

- **Επιθέσεις κρυπτογραφήματος** (ciphertext-only attack): Ο κρυπταναλυτής έχει πρόσβαση στα κρυπτογραφήματα πολλών απλών κειμένων που έχουν κρυπτογραφηθεί με τον ίδιο αλγόριθμο, και προσπαθεί να αναγνωρίσει τα στατιστικά της γλώσσας (συχνότητα εμφάνισης γραμμάτων) στο κρυπτογραφημένο κείμενο.
- **Επιθέσεις γνωστού απλού κειμένου** (known plaintext attack): Ο κρυπταναλυτής έχει πρόσβαση όχι μόνο στα κρυπτοκείμενα αλλά και στα αντίστοιχα αρχικά κείμενα. Προσπαθεί να υπολογίσει το κλειδί ή τα κλειδιά που χρησιμοποιήθηκαν ή να δημιουργήσει ένα αλγόριθμο αποκρυπτογράφησης κάθε κειμένου που έχει κρυπτογραφηθεί με το ίδιο κλειδί.
- **Επιθέσεις επιλεγμένου απλού κειμένου** (chosen plaintext attack): Ο κρυπταναλυτής όχι μόνο έχει πρόσβαση σε ζευγάρια κρυπτοκειμένου-κειμένου, αλλά μπορεί να επιλέξει τα προς κρυπτογράφηση κείμενα, δηλαδή έχει πρόσβαση στη συνάρτηση κρυπτογράφησης (ή σε κάποια προσομοίωση της) και προσπαθεί να υπολογίσει το κλειδί ή τα κλειδιά που χρησιμοποιήθηκαν ή να δημιουργήσει ένα αλγόριθμο αποκρυπτογράφησης κάθε κειμένου που έχει κρυπτογραφηθεί με το ίδιο κλειδί.
- **Επιθέσεις προσαρμοσμένου επιλεγμένου απλού κειμένου** (adaptive chosen plaintext attack): Είναι μια ειδική κατηγορία της προηγούμενης. Ο κρυπταναλυτής έχει μεγαλύτερη ευχέρεια στην επιλογή των προς κρυπτογράφηση κειμένων, τα οποία μπορεί να διαφοροποιήσει και να συγκρίνει τα αντίστοιχα κρυπτοκείμενα.
- **Επιθέσεις επιλεγμένου κρυπτογραφήματος** (chosen ciphertext attack) : Ο κρυπταναλυτής μπορεί να επιλέξει διάφορα κρυπτογραφήματα που θα αποκρυπτογραφήσει και έχει πρόσβαση σε αυτά τα αποτελέσματα. Πάλι προσπαθεί να βρει το κλειδί ή τα κλειδιά.

- **Επιθέσεις προσαρμοσμένου επιλεγμένου κρυπτογραφήματος (**adaptive chosen ciphertext attack): Είναι μια ειδική κατηγορία της προηγούμενης. Ο κρυπταναλυτής έχει μεγαλύτερη ευχέρεια στην επιλογή των προς αποκρυπτογράφηση κρυπτοκειμένων, τα οποία μπορεί να διαφοροποιήσει και να συγκρίνει τα αντίστοιχα αρχικά κείμενα.

Αναφέρουμε επίσης και την επίθεση γραμμικής κρυπτανάλυσης, που βασίζεται στην εύρεση παραπλήσιων προσεγγίσεων στην διαδικασία που ακολουθεί ο κρυπταλγόριθμος, στην ουσία είναι επίθεση γνωστού αρχικού κειμένου. Αρχικά δημιουργεί γραμμικές εξισώσεις που συσχετίζουν γνωστό κείμενο, κρυπτοκείμενο, και bits του κλειδιού. Στη συνέχεια χρησιμοποιώντας αυτές τις εξισώσεις σε συνδυασμό με τα ζευγάρια κειμένου-κρυπτοκειμένου προσπαθεί να παράγει bits του κλειδιού. Κάνοντας αυτή την προσέγγιση με εξισώσεις όχι πρώτου αλλά μικρού βαθμού, συνήθως δεύτερου ή τρίτου, έχουμε την μη γραμμική κρυπτανάλυση. Είναι γνωστές και σαν αλγεβρικές επιθέσεις.

Πέραν των εξειδικευμένων επιθέσεων, που αφορούν την αντιστοιχία κειμένου-κρυπτοκειμένου, υπάρχουν και οι κλασικές μέθοδοι επίθεσης που προσπαθούν να 'μαντέψουν' το κλειδί ή τα κλειδιά. Σύντομα αναφέρουμε τις σημαντικότερες[16] [1]:

- **Επιθέσεις εξαντλητικής αναζήτησης** (Brute force attacks): Σε αυτές τις περιπτώσεις, ο επιτιθέμενος μμπορεί να δοκιμάσει όλα τα δυνατά κλειδιά αποκρυπτογράφησης μέχρι να βρει το κλειδί που έχει χρησιμοποιηθεί.
- **Επιθέσεις επιλεγμένου-γνωστού κλειδιού** (chosen-known key attack): Ο κρυπταναλυτής δεν μπορεί να επιλέξει το κλειδί κρυπτογράφησης-αποκρυπτογράφησης, αλλά έχει κάποια γνώση για τη σχέση διαφορετικών κλειδιών και χρησιμοποιώντας αυτή τη γνώση προσπαθεί να καθορίσει νέα κλειδιά.
- **Επιθέσεις λεξιλογίου** (dictionary attacks) : Η επίθεση αυτή συνήθως αφορά τους κωδικούς (passwords), χρησιμοποιώντας κωδικούς μέσα από γνωστές λίστες.

Υπάρχουν και οι λεγόμενες επιθέσεις **παράπλευρου καναλιού** (side channel attacks) και αφορούν οποιοδήποτε σύστημα. Αυτές αφορούν πληροφορίες που δεν έχουν άμεση σχέση με το ίδιο το σύστημα αλλά με το χρόνο που λειτουργεί (για να παράγει συγκεκριμένο αποτέλεσμα), την ενέργεια που καταναλώνει, την ηλεκτρομαγνητική ακτινοβολία που εκπέμπει κλπ. Προσαρμοζόμενες αυτές οι επιθέσεις στα κρυπτοσυστήματα έχουμε την κρυπτανάλυση παράπλευρου καναλιού, που φυσικά δεν

‘ψάχνει’ τη μαθηματική λογική αλλά τυχόν αδυναμίες της φυσικής υλοποίησης του συστήματος . Σημαντικότερες είναι [1]:

- **Επιθέσεις χρονομέτρησης** (timing attacks) : Αυτές εκμεταλλεύονται τη συσχέτιση μεταξύ ενός κρυπτογραφικού κλειδιού και τη χρονική διάρκεια μιας κρυπτογραφικής πράξης που χρησιμοποιεί το συγκεκριμένο κλειδί. Επειδή η διάρκεια υπολογισμού μιας πράξης συχνά εξαρτάται από τα δεδομένα εισόδου, π.χ. το πλήθος των 1 στο κλειδί, η χρονομέτρηση αποκαλύπτει κάποια πληροφορία για αυτά.
- **Διαφορική ανάλυση σφαλμάτων** (differential fault analysis) : Βασίζονται στο γεγονός ότι διάφορα σφάλματα σε κρυπτογραφικές πράξεις που συσχετίζονται με ένα συγκεκριμένο κρυπτογραφικό κλειδί, μπορεί να διαρρεύσουν πληροφορίες για το εν λόγω κλειδί.
- **Ανάλυση σφάλματος** (fault analysis) : Έχουν κοινά με την προηγούμενη κατηγορία αλλά είναι διαφορετική οικογένεια. Βασίζεται στο γεγονός ότι πολλές υλοποιήσεις κρυπτογραφικών πράξεων επιστρέφουν μηνύματα λάθους σε περίπτωση αποτυχίας.
- **Διαφορική ανάλυση ενέργειας** (differential power analysis) : Εκμεταλλεύονται το γεγονός ότι η εκτέλεση μιας υπολογιστικής πράξης καταναλώνει ένα ποσό ενέργειας. Ο κρυπταναλυτής μετράει και αναλύει την κατανάλωση κατά την εκτέλεση ενός κρυπταλγόριθμου. Επειδή η κατανάλωση ενέργειας ποικίλει κατά τα διάφορα στάδια της κρυπτογραφικής πράξης, μπορεί να αντλήσει πληροφορίες σχετικά με το αξιοποιούμενο κρυπτογραφικό κλειδί.
- **Ηλεκτρομαγνητικές επιθέσεις** (electromagnetic attacks): Εκμεταλλεύονται την εκπομπή ακτινοβολίας που εκπέμπεται από το σύστημα και μπορεί να γίνει ανάλυση αυτής, όπως και με την ενέργεια.

Φυσικά, δεν χρειάζεται πάντα να καταφύγουμε σε κρυπταναλυτικές μεθόδους για να παραβιάσουμε ένα κρυπτογραφικό σύστημα. Πολλές φορές οι κωδικοί ή τα ίδια τα αναζητούμενα κείμενα βρίσκονται πάνω σε γραφεία, οθόνες, τυπωμένες σελίδες, πεταμένα χαρτιά στα σκουπίδια, ή σε υπολογιστές που έχουν δοθεί για ανακύκλωση χωρίς να έχει διαγραφεί το ευαίσθητο περιεχόμενο τους, οπότε κάποιος μπορεί να τα αντιγράψει. Επίσης μπορούμε με δόλιες μεθόδους (ξεγελώντας, υποκλέπτοντας) να αποκτήσουμε αυτά. Επομένως πρέπει να ακολουθείται μια διαδικασία που αφορά τον

χειρισμό κρισίμων δεδομένων, δηλαδή να ακολουθείται μια πολιτική ασφαλείας που πρέπει να υπακούει σε αναγνωρισμένα πρότυπα.

2.3 Διαδίκτυο των πραγμάτων

Η επικοινωνία μεταξύ μηχανών, που συνδύαζαν τηλεφωνία και υπολογιστές, M2M (Machine to Machine), είναι κάτι που ξεκινά από πολύ παλαιά. Εννοιολογικά αναφέρθηκε για πρώτη φορά, από τον Θεόδωρο Παρασκευάκο για το σύστημα αναγνώρισης καλούντος που εργαζόταν το 1968, το οποίο πήρε Αμερικάνικη πατέντα το 1973 [17]. Στα σύγχρονα δίκτυα επικοινωνίας πέραν του κλασικού τρόπου επικοινωνίας, βάση-με-σταθμό (base to station), έχουμε και την επικοινωνία συσκευής με συσκευή, όταν είναι σε κοντινή απόσταση, χωρίς τη μεσολάβηση του σταθμού βάσης Device to Device (D2D) στο εύρος συχνοτήτων του δικτύου. Αυτή η επικοινωνία έχει σαν αποτέλεσμα να βελτιώσει την απόδοση, την κατανάλωση ενέργειας, την καθυστέρηση κ.λ.π. Η πρώτη αναφορά του όρου 'Internet of Things' έγινε από τον Kevin Ashton λέγοντας ότι η χρήση ραδιοσυχνοτήτων για ταυτοποίηση (RFID) είναι προαπαιτούμενο για τη χρήση του IoT σε μια παρουσίαση το 1999 [18]. 'Το Internet of Things είναι μία έννοια που αφορά τα αντικείμενα της καθημερινότητας μας – από βιομηχανικές μηχανές μέχρι wearable συσκευές που χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων & την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο' [3]. Αυτά τα δεδομένα λέγονται δεδομένα συνεχούς ροής (streaming data), οι αισθητήρες συνεχώς ή σε μικρά τακτά διαστήματα 'ακούν', βλέπουν', 'καταλαβαίνουν μετατόπιση' κλπ. Η ανάληψη δράσης, εκμεταλλευόμενοι τη συλλογή δεδομένων, γίνεται μέσα από τη χρήση τεχνικών analytics. Οι τεχνικές αυτές είναι η ανακάλυψη, η ερμηνεία και η επικοινωνία σημαντικών προτύπων στα δεδομένα. Μπορούμε να δούμε που και πως χρησιμοποιείται ή πως θα χρησιμοποιηθεί [3].

- **Υγειονομική Περίθαλψη**. Πολλοί άνθρωποι έχουν ήδη υιοθετήσει wearable συσκευές για να παρακολουθούν την φυσική τους άσκηση, τον ύπνο ή άλλες συνήθειες τους – και αυτά είναι το πιο απλό δείγμα του πώς το IoT συνδυάζεται με τον κλάδο της υγείας. Συσκευές παρακολούθησης ασθενών, ηλεκτρονικά αρχεία και άλλα έξυπνα αξεσουάρ μπορούν να σώσουν ζωές.
- **Εκπαίδευση**. Η ωφέλεια είναι μεγάλη, αποστασιοποίηση από το παραδοσιακό βιβλίο-τετράδιο, προσφορά εξατομικευμένης μάθησης, αλλά και χρήση συστημάτων STEM (Science, Technology, Engineering and Math - Επιστήμη,

Τεχνολογία, Μηχανική και Μαθηματικά), με αποτέλεσμα να έχουμε καινοτόμες παιδαγωγικές μεθόδους και νέες εκπαιδευτικές υπηρεσίες [19].

- **Βιομηχανική Παραγωγή**. Πρόκειται για τον κλάδο που επωφελείται περισσότερο από το IoT. Αισθητήρες συλλογής δεδομένων ενσωματωμένοι σε μηχανήματα εργοστασίων ή στα ράφια των αποθηκών μπορούν να 'επικοινωνήσουν' προβλήματα ή να παρακολουθούν τη χρήση των πόρων τους σε πραγματικό χρόνο, καθιστώντας το εύκολο να εργαστούν πιο αποτελεσματικά και να μειώσουν το κόστος.
- **Λιανεμπόριο**. Τόσο οι καταναλωτές όσο και τα καταστήματα μπορούν να επωφεληθούν από IoT. Τα καταστήματα, για παράδειγμα, θα μπορούσαν να χρησιμοποιήσουν IoT για σκοπούς παρακολούθησης των αποθεμάτων ή της ασφάλειας. Οι καταναλωτές μπορεί να έχουν μία εξατομικευμένη εμπειρία αγορών μέσω των δεδομένων που συλλέγονται από τους αισθητήρες ή τις κάμερες. Επίσης οικιακές συσκευές (πχ. ψυγείο) μπορούν να ειδοποιούν για τυχούσα μείωση αγαθών (πχ. φέτα).
- **Τηλεπικοινωνίες**. Ο κλάδος των τηλεπικοινωνιών θα επηρεαστεί σημαντικά από το IoT, αρκεί να σκεφτεί κανείς ότι αυτός θα είναι ο κλάδος που θα διατηρεί όλα τα δεδομένα που χρησιμοποιεί το IoT. Smartphones και άλλες προσωπικές συσκευές πρέπει να είναι σε θέση να διατηρούν μια αξιόπιστη σύνδεση στο Διαδίκτυο για να λειτουργήσει αποτελεσματικά το Internet of Things.
- **Μεταφορές**. Το IoT επηρεάζει επίσης το κλάδο των μεταφορών σε μεγάλη κλίμακα: οι εταιρείες διανομής μπορούν να παρακολουθούν το στόλο τους με τη χρήση GPS λύσεων. Και οι δρόμοι μπορούν να παρακολουθούνται μέσω αισθητήρων για να είναι όσο το δυνατόν ασφαλέστεροι, να επιταχύνουν την ροή της κυκλοφορίας , μειώνοντας την κατανάλωση καυσίμων.
- **Ενέργεια**. Οι έξυπνοι μετρητές (smart meters, smart grid), όχι μόνο συλλέγουν δεδομένα αυτόματα, αλλά καθιστούν και δυνατή την εφαρμογή analytics για την παρακολούθηση και τη διαχείριση της χρήσης της ενέργειας. Παρομοίως, αισθητήρες σε συσκευές όπως οι ανεμόμυλοι μπορούν να παρακολουθούν τα δεδομένα και να χρησιμοποιούν προγνωστική μοντελοποίηση ώστε να προγραμματιστεί η διακοπή λειτουργίας για πιο αποδοτική χρήση της ενέργειας.

Στην παραδοσιακή ανάλυση τα δεδομένα αποθηκεύονται και μετά αναλύονται, όπως αναφέρεται [3]. Στο IoT που έχουμε, όπως είπαμε, δεδομένα συνεχούς ροής τα μοντέλα και οι αλγόριθμοι είναι αυτοί που αποθηκεύονται και τα δεδομένα περνούν μέσα από

αυτά για ανάλυση. Αυτό το είδος της ανάλυσης καθιστά δυνατό τον εντοπισμό και την εξέταση μοτίβων καθώς τα δεδομένα δημιουργούνται (σε πραγματικό χρόνο). Προχωρώντας πέρα από την απλή παρακολούθηση συνθηκών και ορίων μπορούμε να προχωρήσουμε στην εκτίμηση πιθανών μελλοντικών γεγονότων και στον προγραμματισμό τους για αμέτρητα what-if σενάρια [3].

Ο συνδυασμός των παραπάνω χρήσεων σε ένα ενιαίο περιβάλλον αποτελούν τις λεγόμενες "Έξυπνες Πόλεις (Smart Cities)' όπου σχεδόν όλοι και όλα αλληλοσυνδέονται και αλληλεπικοινωνούν για να δώσουν ή να πάρουν πληροφορίες για την καλύτερη και συντομότερη εξυπηρέτηση, με τον όρο εξυπηρέτηση να καλύπτει και την πρόληψη. Η εξέλιξη της τεχνολογίας αλλάζει και τη δυναμική του IoT, έτσι η αρχιτεκτονική του βασίζεται σε τέσσερις κύριους πυλώνες [20].

- **Ταυτοποίηση μέσω ραδιοσυχνοτήτων** (Radio Frequency Identification – RFID), που είναι η πλέον διάχυτη τεχνολογία με σκοπό την ταυτοποίηση και παρακολούθηση αντικειμένων μέσω ετικετών (tags) που βρίσκονται στο περιβάλλον ή σε αντικείμενα (η προτυποποίηση του ηλεκτρονικού κωδικού προϊόντος (EPC-Electronic Product Code) συνετέλεσε στη διάδοση του RFID στις βιομηχανίες).
- **Επικοινωνία μηχανής με μηχανή** (Machine to Machine-M2M-communication), τώρα ο όρος έχει αποκτήσει μια ευρύτερη έννοια, αρχικά το 2004 είχε περιοριστεί στην επικοινωνία μεταξύ μιας συσκευή-προϊόντος με μια απομακρυσμένη (και αποκλειστική) πλατφόρμα εφαρμογής ή διακομιστή, μέσω κυψελοειδών δικτύων (κινητής) ή με σταθερά δίκτυα ευρείας περιοχής (WAN-Wide Area Networks).
- **Δίκτυα ασύρματων αισθητήρων** (WSNs-Wireless Sensor Networks), που αποτελούνται από αρκετούς αισθητήρες ευρέως κατανεμημένους στο περιβάλλον ικανούς να παρακολουθήσουν διάφορες τιμές (θερμοκρασία, υγρασία, κίνηση, πίεση, ρύπους κλπ.) και να τις επικοινωνούν σε πολυαλματική (multi-hop) λειτουργία. Το πρότυπο αναφοράς του WSN είναι το IEEE 802.15.4 στο οποίο αναφέρονται πολλές συσκευές που υπάρχουν στην αγορά. Επιπλέον τα σύγχρονα δίκτυα ασύρματων αισθητήρων μπορούν να είναι αμφίδρομα, επιτρέποντα στους κόμβους αισθητήρων να δρουν τοπικά ακόμα και με μη κρίσιμα χρονικά χαρακτηριστικά. Η πλήρως αμφίδρομη επικοινωνία επιτρέπει δίκτυα ασύρματων αισθητήρων και εκκινητήρων-ενεργοποιητών (WSANs-Wireless Sensor Actuator Networks).

- Τα συστήματα **SCADA**, λέγοντας λίγα επιπλέον των ήδη λεχθέντων, τα οποία είναι αυτόνομα συστήματα ικανά να παρακολουθούν έξυπνα συστήματα (πχ. σύνθετες βιομηχανικές διαδικασίες), τα περισσότερα των οποίων έχουν απαιτήσεις ελέγχων πραγματικού χρόνου, με χρήση της θεωρίας κλειστών βρόγχων ελέγχου, όπου ο ανθρώπινος έλεγχος ή αλληλεπίδραση δεν είναι εφικτή.

Ένα θέμα που πρέπει οπωσδήποτε να λάβουμε υπ‘ όψη είναι ο τεράστιος όγκος δεδομένων που θα παράγονται από πολλά δισεκατομμύρια αντικειμένων (κάθε άνθρωπος ένας αισθητήρας, και πολλοί αισθητήρες σε μηχανές κτήρια κλπ.) από το περιβάλλον στο διαδίκτυο. Μια πλατφόρμα νέφους (cloud platform) είναι απαραίτητη για να αποθηκεύει, να υπολογίζει και να οπτικοποιεί τα δεδομένα, μετατρέποντας τα σε ουσιαστικές πληροφορίες. Επίσης θα πρέπει να λάβουμε υπ’ όψη για την περαιτέρω ανάπτυξη του IoT την έλλειψη κοινών και τυποποιημένων πλατφορμών που να εξαναγκάζουν τους προγραμματιστές να υλοποιούν κάθετες και αυστηρές αρχιτεκτονικές για να παρέχουν συγκεκριμένες υπηρεσίες, την ανάγκη διευθυνσιοδότησης κάθε αντικειμένου, την ετερογένεια των συσκευών, και την ανάγκη για εγγύηση της ασφάλειας των συλλεγομένων δεδομένων από κάθε αντικείμενο ή συσκευή[21], και της μετάδοσης στην πλατφόρμα εφαρμογής, που είναι θεμελιώδες για τη διάχυση του και προτυποποίηση των διαδικασιών [20].

Κεφάλαιο 3
Αλγόριθμοι Κρυπτογραφίας

Έχουμε αναφερθεί στους συμμετρικούς αλγόριθμους τμήματος, και ροής και στους ασύμμετρους αλγόριθμους. Εδώ θα δούμε αναλυτικά τον τρόπο λειτουργίας των αλγόριθμων αυτών.

3.1 Χαρακτηριστικά, Λειτουργία των Αλγόριθμων Τμήματος

Οι κρυπταλγόριθμοι τμήματος, όπως φαίνεται και από το όνομα τους, χωρίζουν ένα μήνυμα M σε διαδοχικά τμήματα M_1,M_2,… ίσου μεγέθους n. Κάθε τμήμα (block) M_i κρυπτογραφείται ξεχωριστά, δίνοντας ως αποτέλεσμα ένα τμήμα κρυπτοκειμένου C_i ίσου μεγέθους n, με χρήση ενός κλειδιού κρυπτογράφησης K ($C_i = E_K(M_i)$). Η αποκρυπτογράφηση γίνεται επίσης κατά τμήματα, δηλαδή $M_i = D_K(E_i)$. Η λειτουργία των κρυπταλγόριθμων τμήματος είναι επαναληπτική. Το αρχικό τμήμα μηνύματος Mi κρυπτογραφείται μέσα από διάφορα στάδια (γύρους), όπου σε κάθε γύρο συντελείται ο ίδιος κρυπτογραφικός μετασχηματισμός, προκειμένου να σχηματιστεί το τελικό τμήμα κρυπτοκειμένου Ci. Για κάθε γύρο, χρησιμοποιείται διαφορετικό τμήμα κλειδιού, με τέτοιο τρόπο ώστε τελικά όλα τα bit του κλειδιού να υπεισέρχονται στη διαδικασία της κρυπτογράφησης. Σε όλους τους αλγόριθμους τμήματος υπεισέρχεται στη λειτουργία τους μια δομική μονάδα που λέγεται μονάδα αντικατάστασης (Substitution Box - SBox), η οποία πραγματοποιεί αντικαταστάσεις bit, και έτσι εισάγει σύγχυση στον αλγόριθμο. Επίσης όλοι οι αλγόριθμοι τμήματος περιέχουν δομικές μονάδες που επιτελούν αντιμεταθέσεις bit, τις μονάδες αντιμετάθεσης (Permutation Box - PBox). Πολλαπλά στάδια αντιμεταθέσεων εισάγουν διάχυση στην κρυπτογραφική διαδικασία [1]. Ένας κρυπταλγόριθμος τμήματος μπορεί να περιλαμβάνει και ένα δίκτυο ή αλγόριθμο Feistel (Feistel network ή cipher), που είναι ένας συνδυασμός από αντικαταστάσεις και αντιμεταθέσεις που εφαρμόζονται (η διαδικασία αυτή ονομάζεται συνάρτηση F) στο

δεξιό τμήμα από τα δυο που χωρίζεται το μήνυμα και αυτό το αποτέλεσμα αυτό προστίθεται (xor) στο αριστερό. Ότι προκύπτει σαν αποτέλεσμα θα αποτελέσει το δεξιό τμήμα του νέου τροποποιημένου τμήματος. Το αριστερό τμήμα του νέου τροποποιημένου τμήματος ταυτίζεται με το δεξί τμήμα του αρχικού τμήματος. Η διαδικασία αυτή επαναλαμβάνεται πολλές φορές.

Ο κρυπταλγόριθμος DES και οι παραλλαγές του χρησιμοποιούν τα δίκτυα Festel, αλλά όπως είπαμε και παραπάνω ο συγκεκριμένος αλγόριθμος δεν παρέχει πλέον ασφάλεια. Ο 3DES , τριπλή εφαρμογή του DES με διαφορετικό κλειδί κάθε φορά, είναι ασφαλής.
Ένας κρυπταλγόριθμος τμήματος πραγματοποιεί αντικαταστάσεις τμημάτων από bit. Αν το μήκος τμήματος είναι πολύ μικρό, ο αλγόριθμος θα είναι ευάλωτος σε κρυπτανάλυση στατιστικής φύσης, αν είναι πολύ μεγάλο θα δυσχεραίνει την υλοποίηση του αλγόριθμου. Το τυπικό μέγεθος τμήματος σήμερα είναι 128 bit. Το πλήθος όλων των πιθανών αντιστοιχίσεων του μηνύματος σε κρυπτοκείμενο είναι $2^n!$, για τμήμα μήκους n. Με δεδομένο ότι σε μια κρυπτογράφηση το κλειδί είναι ουσιαστικά η επιλογή μιας συγκεκριμένης αντιστοίχισης, θα απαιτείτο κλειδί μήκους $n*2^n$ bit για να περιγράψει μια τέτοια κρυπτογραφική αντιστοίχιση. Το μέγεθος αυτό τον καθιστά πρακτικά μη υλοποιήσιμο. Έτσι επιλέγεται ένα κλειδί μήκους k με αποτέλεσμα οι αντιστοιχίσεις να είναι το πολύ 2^k [1].
Λόγω της ασφάλειας, της σχετικής ταχύτητας λειτουργίας και σχετικής ευκολίας υλοποίησης χρησιμοποιούνται σε πολλές εφαρμογές όπως [22]:

- Διαδίκτυο (πρωτόκολλο https για κρυπτογραφημένες συνδέσεις)
- Email (πρωτόκολλο S-MIME για κρυπτογράφηση ηλεκτρονικών μηνυμάτων)
- Συναλλαγές στα ATM τραπεζών
- Εικονικά Ιδιωτικά Δίκτυα (VPNs)
- Λογισμικά κρυπτογράφησης σκληρών δίσκων Η/Υ

Ο αλγόριθμος AES/ Rijndael, από τα ονόματα των δημιουργών του Joan Daemen και Vincent Rijmen, είναι κρυπταλγόριθμος που χρησιμοποιεί αντικαταστάσεις και αντιμεταθέσεις. Αναλυτικά [1] [23]:

- Το αρχικό μήνυμα, που αποτελεί την είσοδο στον αλγόριθμο, θεωρείται πίνακας τεσσάρων γραμμών, αποτελούμενος από byte, αριθμούμενες κατά σειρά 0,1,2,3. Το πλήθος των στηλών καθορίζεται από το μέγεθος του τμήματος (block) του μηνύματος. Στον AES(πρότυπο), που το τμήμα έχει μέγεθος 128 bit, το πλήθος

των στηλών είναι 4 (4*4*8=128). Ένας τέτοιος πίνακας ονομάζεται κατάσταση (state).

- Μήκη κλειδιού: 128, 192, 256 bits (υποστηρίζονται και τα τρία αυτά μεγέθη)
- Μήκη blocks δεδομένων: 128, 192, 256 bits Στο πρότυπο AES, υιοθετήθηκε ως μόνο δυνατό μέγεθος block τα 128 bits
- Εύκολη υλοποίηση hardware
- 10-15 γύροι, ανάλογα με το μήκος του κλειδιού
- Κάθε γύρος αποτελείται από 4 βασικές πράξεις:

- **Αντικατάσταση byte** (Byte substitution – SubBytes) – χρήση SBoxes με καλά χαρακτηριστικά. Κάθε ένα byte του πίνακα κατάστασης αντικαθίσταται από κάποιο άλλο byte μέσω ενός μη γραμμικού μετασχηματισμού. Οι λεπτομέρειες του συγκεκριμένου SBox βασίζονται σε ιδιότητες των πεπερασμένων σωμάτων. Αποδεικνύεται πάντως ότι είναι μία ισχυρά μη γραμμική συνάρτηση, που ταυτόχρονα υλοποιείται εύκολα. Είναι το μόνο τμήμα του αλγορίθμου που είναι μη γραμμικό, συνεπώς αυτό που καθορίζει σε μεγάλο βαθμό την ασφάλεια.
- **Ολίσθηση** (ShiftRows). Εδώ τα byte κάθε γραμμής του πίνακα κατάστασης υφίστανται μια κυκλική ολίσθηση προς τα αριστερά. Στο πρότυπο AES η πρώτη γραμμή (0) δεν ολισθαίνει, η δεύτερη ολισθαίνει κατά μία, η τρίτη κατά δυο και η τέταρτη κατά τρεις θέσεις.
- **Συνδυασμός πολλών bit** (MixColumns). Η διαδικασία αυτή επενεργεί σε κάθε στήλη του πίνακα κατάστασης. Κάθε στήλη του πίνακα πολλαπλασιάζεται με έναν κατάλληλο (πάντα σταθερό και συγκεκριμένο) πίνακα C διαστάσεων 4x4 (όπου κάθε στοιχείο του C είναι 1 Byte). Με αυτόν τον τρόπο, η στήλη μεταβάλλεται συνολικά. Η MixColumns συνάρτηση είναι αυτή η οποία δεν συντελείται στον τελευταίο γύρο του AES. Κατά τα άλλα, ο τελευταίος γύρος είναι ίδιος με τους υπόλοιπους.
- **Πρόσθεση του κλειδιού** (AddRoundKey). Είναι η προσθήκη του κλειδιού στην τρέχουσα κατάσταση. Πρόσθεση XOR του block με το υπο-κλειδί του τρέχοντος γύρου (το οποίο επίσης εκλαμβάνεται ως πίνακας από byte). Είναι το μόνο σημείο της όλης κρυπτογραφικής διαδικασίας στην οποία υπεισέρχεται το κλειδί.

Οι κρυπταλγόριθμοι τμήματος (block ciphers) μπορούν να λειτουργήσουν με διάφορους τρόπους (modes of operation). Μέχρι τώρα έχουμε δει μόνο έναν τρόπο.

Κρυπτογράφηση κάθε τμήματος ξεχωριστά, με εφαρμογή του κλειδιού. Υπάρχουν και άλλοι τρόποι, που γενικά ισχύουν για όλους τους κρυπταλγορίθμους τμήματος και υπάγονται σε δυο βασικές κατηγορίες [24].

- Σε αυτούς που **δεν χρησιμοποιούν ανάδραση**, δηλαδή η κρυπτογράφηση κάθε επόμενου block γίνεται ανεξάρτητα από την επεξεργασία των άλλων block, οπότε όλα τα block μπορούν να κρυπτογραφηθούν παράλληλα χωρίς να υπάρχει σύνδεση μεταξύ τους. Όταν κρυπτογραφούνται δυο block με τα ίδια δεδομένα και με το ίδιο κλειδί θα παράγουν το ίδιο κρυπτοκείμενο με αποτέλεσμα ένας επιτιθέμενος μπορεί να ανακαλύψει μοτίβα στο κρυπτοκείμενο για να βρει παρόμοια κομμάτια στο απλό κείμενο και από αυτά να μπορεί να ξεκινήσει μια κρυπτογραφική επίθεση.
- Σε αυτούς που **χρησιμοποιούν ανάδραση**, δηλαδή κατά την κρυπτογράφηση το κρυπτοκείμενο του προηγούμενου block χρησιμοποιείται και αυτό μαζί με τα δεδομένα του block που κρυπτογραφείται σαν είσοδος, με αποτέλεσμα δύο block με τα ίδια δεδομένα και με το ίδιο κλειδί δεν παράγουν το ίδιο κρυπτογράφημα. Επομένως η κρυπτογράφηση των block πρέπει να γίνει το ένα μετά το άλλο αφού πρέπει να τελειώσει η κρυπτογράφηση του προηγούμενου για να αρχίσει του επόμενου, οπότε δεν μπορεί να γίνει παράλληλη επεξεργασία των block.

Ο κάθε ένας έχει τα δικά του πλεονεκτήματα. Όλοι οι τρόποι (ECB, CTR, CBC, CFB, OFB) περιγράφονται στη συνέχεια, με τους δυο πρώτους να μη χρησιμοποιούν ανάδραση [1] [23]:

- **ECB, ηλεκτρονικό κωδικοβιβλίο** - Electronic CodeBook. Είναι αυτός που έχει περιγραφεί μέχρι τώρα, όπως είπαμε. Το κλειδί κρυπτογραφεί το κάθε block ανεξάρτητα. Δύο ίδια block, για το ίδιο κλειδί κρυπτογράφησης, κρυπτογραφούνται πάντα στο ίδιο block κρυπτοκειμένου. Επομένως, δεν συνίσταται σε εφαρμογές όπου υπάρχουν επαναλαμβανόμενα μοτίβα δεδομένων στο αρχικό μήνυμα. Ένα λάθος στη λήψη επηρεάζει την αποκρυπτογράφηση μόνο του συγκεκριμένου block.
- **CTR, μετρητή ή απαριθμητή** - CounTeR). Η βασική δομική μονάδα είναι ένας μετρητής μήκους n, όπου n το μέγεθος του block. Ο αλγόριθμος τμήματος κρυπτογραφεί κάθε φορά το περιεχόμενο του μετρητή, και η έξοδός του γίνεται XOR με το τμήμα του μηνύματος, για να παραχθεί το κρυπτογραφημένο τμήμα.

- **CBC, αλυσιδωτού τμήματος** - Cipher Block Chaining. Το block του μηνύματος προστίθεται με XOR με το προηγούμενο block του κρυπτοκειμένου, πριν την κρυπτογράφηση. Συνεπώς, δύο όμοια block δεν δίνουν, μετά την κρυπτογράφησή τους με το ίδιο κλειδί, όμοια block κρυπτοκειμένου. Λάθος κατά τη λήψη σε ένα απλό bit του κρυπτοκειμένου θα προκαλέσει λάθος στην αποκρυπτογράφηση δύο διαδοχικών block. Είναι απαραίτητο να υπάρχει ένα block αρχικοποίησης για την κρυπτογράφηση του πρώτου block του μηνύματος (αφού δεν υπάρχει κάποιο κρυπτοκείμενο που να έχει ήδη παραχθεί εκείνη τη στιγμή).
- **CFB, ανάδρασης κρυπταλγορίθμου** - Cipher FeedBack. Τα δεδομένα κρυπτογραφούνται s bits τη φορά. – Υπάρχει ένας καταχωρητής ολίσθησης, μεγέθους όσο το μέγεθος του μπλοκ. – Κάθε χρονική στιγμή, τα περιεχόμενα του καταχωρητή ολίσθησης κρυπτογραφούνται: από το αποτέλεσμα που προκύπτει, τα s αριστερότερα bits γίνονται xor με τα s bits του μηνύματος και προκύπτουν s bits κρυπτοκειμένου. Αυτά για την επόμενη χρονική στιγμή πηγαίνουν στον καταχωρητή ολίσθησης, ο οποίος για να μπορεί να τα «χωρέσει» αποβάλλει τα s αριστερότερα του bits. Μειώνεται η απόδοση (throughput) του συστήματος σε σχέση με το CBC κατά έναν παράγοντα n/s (όπου n το πλήθος bits του block). Λάθος σε ένα bit του κρυπτοκειμένου επηρεάζει το πολύ τις επόμενες [n/s] αποκρυπτογραφήσεις .
- **OFB, ανάδρασης εξόδου –** Output Feedback. Σχεδόν όμοιος με τον CFB, με τη διαφορά ότι στην επόμενη βαθμίδα τροφοδοτείται η έξοδος της συνάρτησης κρυπτογράφησης και όχι το κρυπτοκείμενο. Πλέον τροφοδοτείται ολόκληρη η έξοδος της συνάρτησης (και όχι τα s bits, όπως ίσχυε παλαιότερα, κατ' αναλογία με τον CFB) Μοιάζει πολύ με κρυπταλγόριθμο ροής.

Στους τρεις (CFB, OFB,CTR) από τους πέντε τρόπους, δεν χρειάζεται το κύκλωμα της αποκρυπτογράφησης, πράγμα που είναι σημαντικό πλεονέκτημα ως προς την υλοποίηση. Κάθε τρόπος λειτουργίας προσφέρεται για συγκεκριμένες εφαρμογές. Θεωρούνται, γενικώς, καλύτεροι οι CFB, OFB, CTR, ενώ ο CBC αποτελεί καλή επιλογή για συνάρτηση κατακερματισμού. Όλοι έχουν προτυποποιηθεί από τον οργανισμό τυποποίησης NIST (National Institute of Standards and Technology). Ο ECB πρέπει να αποφεύγεται (μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση μηνύματος που

αποτελείται από ένα μόνο block). Ο τρόπος λειτουργίας μετρητή προσφέρεται για παράλληλη επεξεργασία.

Εκτός από τις γνωστές επιθέσεις, έχουμε και τις επιθέσεις bit-flipping, όπου ο επιτιθέμενος τροποποιεί κάποια συγκεκριμένα bits του κρυπτοκειμένου, και στη συνέχεια το προωθεί στον προορισμό του. Ο παραλήπτης, πχ. ένας εξυπηρετητής επικοινωνίας, αποκρυπτογραφεί το κείμενο χωρίς να καταλάβει τη μεταβολή. Αποτέλεσμα αυτού είναι να μην έχει το 'σωστό' κείμενο. Αν η αλλαγή έχει γίνει, πχ. σε μια IP, τότε το κείμενο δεν θα σταλεί στον αρχικό παραλήπτη, αλλά σε κάποιο άλλο.

3.2 Χαρακτηριστικά, Λειτουργία των Αλγόριθμων Ροής

Οι κρυπταλγόριθμοι ροής κρυπτογραφούν μεμονωμένους χαρακτήρες (συνήθως δυαδικά ψηφία) ενός μηνύματος απλού κειμένου, έναν τη φορά [16]. Ο βασικός στόχος των κρυπταλγόριθμων ροής είναι η αποδοτική παραγωγή μιας φαινομενικά τυχαίας ακολουθίας συμβόλων που καλείται κλειδοροή. Αν η κλειδοροή είναι ανεξάρτητη από το κρυπτοκείμενο και το απλό κείμενο, λέγονται σύγχρονοι. Υπάρχουν και οι ασύγχρονοι κρυπταλγόριθμοι ροής, στους οποίους η κλειδοροή εξαρτάται από το κρυπτοκείμενο καθώς και από την τρέχουσα κατάσταση του συστήματος, και αναφέρονται ως αναδευτήρες [1].

Οι κρυπταλγόριθμοι ροής χρησιμοποιούνται ευρέως σε εφαρμογές με απαιτήσεις για υψηλή ταχύτητα και χαμηλή κατανάλωση ισχύος, γιατί είναι σε γενικές γραμμές ταχύτεροι από τους αντίστοιχους κρυπταλγόριθμους τμήματος και υλοποιούνται αποδοτικά, λόγω των μικρών απαιτήσεων σε υπολογιστική ισχύ και πολυπλοκότητα κυκλωμάτων. Σε πολλές περιπτώσεις η χρήση τους είναι υποχρεωτική, όπως σε συστήματα και εφαρμογές επικοινωνιών, όπου η δυνατότητα μνήμης είναι περιορισμένη ή πρέπει τα λαμβανόμενα σύμβολα να υπόκεινται σε ανεξάρτητη επεξεργασία κατά τη μετάδοση ή την λήψη τους. Επιπλέον επειδή χαρακτηρίζονται από μηδενική ή μικρή διάδοση σφαλμάτων, αποτελούν ιδιαίτερα ελκυστική λύση για επικοινωνιακά κανάλια με σχετικά μεγάλη πιθανότητα σφαλμάτων μετάδοσης [1].

Ο λόγος που χρησιμοποιούμε μια γεννήτρια ψευδοτυχαίας ακολουθίας, η οποία προσομοιάζει το αποτέλεσμα ανεξαρτήτων επαναλήψεων ενός τυχαίου πειράματος που έχει σαν πιθανές εκβάσεις τα σύμβολα της ακολουθίας – κλειδοροής, είναι ότι δεν είναι

δυνατό να κατασκευάσουμε μια γεννήτρια πραγματικά τυχαίων συμβόλων. Οι τυχαίες ακολουθίες έχουν τις παρακάτω ιδιότητες:

- Πλήρης έλλειψη μοτίβων
- Αδυναμία πρόβλεψης συμβόλων
- Έλλειψη απλής περιγραφής

Οι ψευδοτυχαίες ακολουθίες διαθέτουν απλή περιγραφή. Συνεπώς η παραγόμενη κλειδοροή είναι κατάλληλη προς χρήση σε μηχανογραφικές εφαρμογές μόνο αν είναι δυσδιάκριτη ως προ μια τυχαία ακολουθία, δηλαδή είναι υπολογιστικά αδύνατη η εύρεση της αντίστοιχης απλής της περιγραφής. Ο βαθμός δοθείσας κλειδοροής αποτιμάται μέσω της ικανοποίησης ενός μεγάλου αριθμού, πιθανώς αντικρουόμενων, κρυπτογραφικών κριτηρίων [10].

Χαρακτηριστικά παραδείγματα είναι τα ασύρματα δίκτυα (WiFi), κινητές επικοινωνίες (GSM, 3G), πρωτόκολλο Bluetooth, δίκτυα RFID, αλλά και στο Διαδίκτυο (π.χ. αλγόριθμος RC4 στο πρωτόκολλο SSL-Secure Sockets Layer, παλαιότερα γιατί τώρα θεωρείται ανασφαλές, και τώρα έχει αντικατασταθεί από το πρωτόκολλο TLS-Transport Layer Security, χωρίς τον RC4) [25].

Η κρυπτογράφηση γίνεται πάνω σε μία ροή από bits (ή bytes) χρησιμοποιώντας μία γεννήτρια ψευδοτυχαίας ακολουθίας bits (keystream generator). Η παραγόμενη ακολουθία K_i ονομάζεται κλειδοροή όπως είπαμε (keystream) που εξαρτάται από το κλειδί και μια ποσότητα που ονομάζεται διάνυσμα αρχικοποίησης. Τα bits της κλειδοροής προστίθενται (πράξη XOR) με τα bits του μηνύματος για να προκύψει έτσι το κρυπτοκείμενο. Κρυπτογράφηση: $C_i = P_i \oplus K_i$.Αντίστοιχα πραγματοποιείται και η αποκρυπτογράφηση.

Αποκρυπτογράφηση: $P_i = C_i \oplus K_i$. Βλέπουμε ότι η κλειδοροή είναι ανεξάρτητη από το απλό κείμενο και το κρυπτοκείμενο, και είναι αυτοί οι κρυπταλγόριθμοι ροής, που ονομάζονται σύγχρονοι κρυπταλγόριθμοι ροής, και αναφέρονται ως γεννήτριες κλειδοροής ή γεννήτριες ψευδοτυχαίων ακολουθιών. Οι σύγχρονοι κρυπταλγόριθμοι ροής έχουν κάποια βασικά χαρακτηριστικά:

- **Συγχρονισμός**, σε ένα σύγχρονο κρυπταλγόριθμο ροής ο αποστολέας και ο παραλήπτης πρέπει να είναι συνεχώς συγχρονισμένοι, δηλαδή κάθε χρονική στιγμή οι γεννήτριες πρέπει να είναι στην ίδια κατάσταση ώστε να αποκρυπτογραφηθεί σωστά το σύμβολο κρυπτοκειμένου. Σε περίπτωση που χαθεί ο συγχρονισμός λόγω διαγραφής ή εισαγωγής συμβόλων κρυπτοκειμένου κατά τη μετάδοση σαν αποτέλεσμα του θορύβου στο κανάλι επικοινωνίας , τότε

ο συγχρονισμός επανέρχεται με χρήση πρόσθετων τεχνικών επανασυγχρονισμού, όπως η επαναρχικοποίηση ή η εισαγωγή πλεονάζουσας πληροφορίας στα σύμβολα του κρυπτοκειμένου.

- **Διάδοση σφαλμάτων**, η τροποποίηση ενός συμβόλου του κρυπτοκειμένου επηρεάζει μόνο το αντίστοιχο σύμβολο του απλού κειμένου, οπότε οι σύγχρονοι κρυπταλγόριθμοι ροής χαρακτηρίζονται από μηδενική διάδοση σφαλμάτων.

Σαν αποτέλεσμα της πρώτης ιδιότητας, η εισαγωγή ή διαγραφή συμβόλων κρυπτοκειμένου από ενεργούς επιτιθέμενους επιφέρει την απώλεια συγχρονισμού και γίνεται εύκολα αντιληπτή από τον παραλήπτη. Αντίθετα η αλλοίωση συγκεκριμένων συμβόλων του κρυπτοκειμένου, με ταυτόχρονη γνώση του τρόπου που επηρεάζεται το απλό κείμενο δεν γίνεται εύκολα αντιληπτή. Επομένως πρέπει να εφαρμοστούν πρόσθετοι μηχανισμοί για να διασφαλίζεται η ακεραιότητα των δεδομένων.

Παρομοίως οι ασύγχρονοι κρυπταλγόριθμοι ροής έχουν και αυτοί θέματα διάδοσης σφαλμάτων μετά από απώλεια συγχρονισμού και ανάγκη διασφάλισης της ακεραιότητας των δεδομένων με πρόσθετους μηχανισμούς. Επίσης επειδή κάθε σύμβολο του απλού κειμένου συνεισφέρει στον υπολογισμό όλων των μεταγενέστερων συμβόλων του κρυπτοκειμένου, οι εγγενείς στατιστικές ιδιότητες του απλού κειμένου διαχέονται στο μέγιστο βαθμό μέσα στο κρυπτοκείμενο, οπότε δεν είναι ευάλωτο σε στατιστικές κρυπταναλυτικές επιθέσεις.

Ο μηχανικός Gilbert Vernam είχε προτείνει από το 1918 ένα σύστημα όπως οι σημερινοί κρυπταλγόριθμοι ροής, με μόνη κύρια απαίτηση το πολύ μεγάλο μέγεθος κλειδοροής. Όσο μεγάλο μέγεθος όμως και αν θέσουμε εκ των προτέρων για το κλειδί, πάντοτε μπορεί το μήνυμα να έχει μεγαλύτερο μέγεθος. Ως σημειωματάριο μιας χρήσης (one-time pad) αποκαλείται το ιδανικό εκείνο κρυπτοσύστημα, που είναι γενίκευση του αλγορίθμου του Vernam, όπου η κλειδοροή είναι μία τυχαία ακολουθία από bits, μεγέθους όσο και το μήνυμα, μη περιοδική. Επομένως δεν χρησιμοποιείται ποτέ το ίδιο κλειδί εκ νέου, κάθε νέο μήνυμα κρυπτογραφείται με διαφορετικό κλειδί). Το one-time pad είναι απεριόριστα ασφαλές κατά Shannon [26].

Επειδή δεν μπορούμε από έναν υπολογιστή να έχουμε παραγωγή απολύτως τυχαίας ακολουθίας, όπως είπαμε παραπάνω, προσπαθούμε με τη χρήση των κρυπταλγόριθμων ροής να προσομοιάσουμε, κατά το δυνατόν, το σημειωματάριο μιας χρήσης, δηλαδή την εύρεση τεχνικών παραγωγής ακολουθιών πολύ μεγάλης περιόδου, που να εμφανίζουν χαρακτηριστικά τυχαιότητας [26].

Για να πετύχουμε αυτή την 'τυχαία' ακολουθία χρησιμοποιούμε γεννήτριες ψευδοτυχαίων bits τους λεγόμενους καταχωρητές ολίσθησης με ανάδραση (Linear Feedback Shift Registers - LFSR), που παράγουν ακολουθίες bits, τα οποία πληρούν τα κριτήρια τυχαιότητας του Goulomb. Αυτά είναι ιδιότητες που πρέπει να έχουν αυτές για να θεωρούνται τυχαίες, και είναι τα παρακάτω.

- Ισοκατανεμημένο πλήθος 0 και 1 (Balance Property).
- Αν ως διαδρομή (run) ορίζουμε ένα τμήμα της ακολουθίας που αποτελείται μόνο από μηδενικά ή μόνο από άσους (και αμέσως πριν και μετά από αυτά βρίσκονται διαφορετικά bit από αυτά που απαρτίζουν το τμήμα), τότε σε μία περίοδο οι μισές διαδρομές έχουν μήκος 1, το ¼ των διαδρομών έχουν μήκος 2, το 1/8 μήκος 3 κ.ο.κ. Η ισχύς της συνθήκης εξετάζεται όσο ο αριθμός των διαδρομών είναι μεγαλύτερος ή ίσος από 2l, όπου l το μήκος της διαδρομής. (Run Property).
- Η συνάρτηση αυτοσυσχέτησης (συνάρτηση που σχετίζεται με την περίοδο και τους όρους της ακολουθίας) να μπορεί να πάρει μόνο δυο τιμές.

Οι γεννήτριες αυτές, οι LFSR, έχουν καλή μαθηματική περιγραφή και οι ιδιότητες τους αναλύονται εύκολα, ενώ μπορούν να υλοποιηθούν σε υλικό (hardware) εύκολα. Οι γεννήτριες όμως αυτές παράγουν ακολουθίες χαμηλής γραμμικής πολυπλοκότητας. Θα πρέπει να έχουν υψηλή γραμμική πολυπλοκότητα (πρακτικά αυτή είναι ίση με τον ελάχιστό αριθμό αρχικών όρων της ακολουθίας που απαιτούνται για το γραμμικό προσδιορισμό όλων των υπολοίπων όρων της ακολουθίας) για να μην είναι εύκολα προβλέψιμες οι ακολουθίες που παράγουν. Αντίστοιχα έχουμε και τη μη γραμμική πολυπλοκότητα (που είναι ίση με τον ελάχιστο αριθμό των αρχικών όρων της που απαιτούνται για τον μη γραμμικό προσδιορισμό όλων των υπολοίπων όρων της), η οποία επίσης πρέπει να είναι υψηλή για τους ίδιους λόγους [1] [26]. Εφαρμόζοντας μη γραμμικές συναρτήσεις (μη γραμμικά φίλτρα) στις βαθμίδες ενός LFSR επιτυγχάνεται η παραγωγή ακολουθιών υψηλής γραμμικότητας.

Ένας πολύ γνωστός κρυπταλγόριθμος ροής που χρησιμοποιείτο είναι ο RC4, σχεδιασμένος από τον Ron Rivest, ο οποίος χρησιμοποιεί κλειδί μεταβλητού μήκους από 40 έως 256 bits. Δεν χρησιμοποιεί LFSR για την παραγωγή κλειδοροής, αλλά η βασική του δομή είναι ένας πίνακας του οποίου το περιεχόμενο αναδιατάσσεται με συγκεκριμένο τρόπο με βάση το κλειδί. Αποδείχτηκε ότι τα πρώτα bytes της κλειδοροής δεν έχουν χαρακτηριστικά τυχαιότητας με αποτέλεσμα να μπορεί να αποκαλυφτεί τμήμα του κλειδιού. Αποτέλεσμα αυτού είναι να θεωρείται πλέον ανασφαλής.

Γνωστοί αλγόριθμοι ροής είναι οι HC-128, Rabbit για λογισμικό, οι Trivium, Grain v1 για υλοποιήσεις υλικού. Κανένας από αυτούς δεν έχει καθιερωθεί σαν πρότυπο.

3.3 Χαρακτηριστικά, Λειτουργία των Ασύμμετρων Αλγόριθμων

Έχοντας ήδη αναφερθεί στον τρόπο λειτουργίας της ασύμμετρης κρυπτογραφίας θα δούμε τον κρυπταλγόριθμο RSA [1] [27].

Για τη δημιουργία του δημόσιου και του ιδιωτικού κλειδιού ένας χρήστης Α ακολουθεί τα παρακάτω βήματα:

- Επιλέγει δυο ισομήκεις, στη δυαδική τους αναπαράσταση, διαφορετικούς μεγάλους, τυχαίους πρώτους αριθμούς p και q τέτοιους ώστε η διαφορά p-q να είναι επίσης μεγάλος αριθμός.
- Υπολογίζει το γινόμενο n = p*q.
- Υπολογίζει την τιμή της συνάρτησης Euler φ(n) = (p-1)*(q-1).
- Επιλέγει έναν αριθμό e, τέτοιον ώστε να είναι σχετικά πρώτος με το φ(n) και μεγαλύτερος του 1.
- Υπολογίζει τον αριθμό d, τέτοιον ώστε $d*e \equiv 1 \pmod{\varphi(n)}$, ο υπολογισμός του οποίου γίνεται με χρήση του εκτεταμένου αλγόριθμου του Ευκλείδη.
- Το δημόσιο κλειδί είναι το (n,e) και το ιδιωτικό το d.

Για να κρυπτογραφήσει ένα μήνυμα m, ο χρήστης Α και να το στείλει στον χρήστη Β:

- Λαμβάνει το δημόσιο κλειδί (n, e) του Β.
- Μετατρέπει το μήνυμα m σε ένα ακέραιο στο διάστημα {0, 1, …, n-1}, με χρήση πχ του κώδικα ASCII ή οποιασδήποτε άλλης πρωτυποποιημένης διαδικασίας μετατροπής που την γνωρίζει και ο Β, και το χωρίζει σε block το μέγεθος του οποίου εξαρτάται από το n.
- Υπολογίζει την τιμή $c= m^e \bmod n$, για κάθε block, και τα στέλνει ι στο Β.

Ο χρήστης Β για να αποκρυπτογραφήσει αυτό που έλαβε, χρησιμοποιεί το ιδιωτικό του κλειδί d και υπολογίζει την ποσότητα $c^d \bmod n$ για κάθε block που έλαβε και έτσι δημιουργεί το αρχικό μήνυμα.

Τα p, q δεν πρέπει να είναι κοντινοί αριθμοί για να μη μπορεί να παραγοντοποιηθεί ο n, κάνοντας ελέγχους στην περιοχή του $\sqrt{n}$. Το e πρέπει να είναι μεγάλο για να μη μπορεί να υπολογιστεί η e-στη ρίζα του m. Για να αποφευχθεί αυτό το πρόβλημα στην πράξη ο

RSA μετασχηματίζει το μήνυμα προσθέτοντας στο τέλος μερικά bits, η τεχνική αυτή ονομάζεται παραγέμισμα (padding) και υπάρχουν αρκετοί τρόποι υλοποίησης της. Επίσης και ο d πρέπει να είναι μεγάλος αριθμός γιατί μπορεί να αποδειχθεί ότι αν q < p < 2q και $d < n^{1/4} / 3$,τότε ο d μπορεί να υπολογιστεί αποδοτικά από τα γνωστά n,e. Αν ο e είναι σχετικά μικρός, αφού ο n είναι γνωστός και δεν χρησιμοποιείται παραγέμισμα, ο αλγόριθμος είναι ευάλωτος σε κρυπταναλυτικές επιθέσεις. Η συνήθως χρησιμοποιούμενη τιμή του e= 65537, ενώ μικρότερες πρέπει να αποφεύγονται.
Για να παραβιαστεί ο αλγόριθμος θα πρέπει να υπολογιστεί η e-στη ρίζα ενός φυσικού modulo n, όπου n σύνθετος φυσικός αριθμός. Με παραγοντοποίηση του n για εύρεση των πρώτων παραγόντων του, και μετά υπολογισμό του d από ένα επιτιθέμενο θα υπήρχε πρόβλημα. Αυτού του τύπου οι επιθέσεις είναι ωμής βίας και έχουν πετύχει παραγοντοποίηση αριθμών μέχρι 663 bits. Με τις τωρινές δυνατότητες με συνιστώμενη χρήση κλειδιών 2048 bits δεν υπάρχει πρόβλημα. Άλλες επιθέσεις που βασίζονται σε κακή χρήση του RSA είναι η επίθεση κοινού modulo και η επίθεση τυφλής υπογραφής.
Η πρώτη βασίζεται στη χρήση κοινού n, το οποίο πρέπει να αποφεύγεται ,γιατί σε αυτή την περίπτωση υπάρχει τεχνική εύρεσης των p, q. Στη δεύτερη ένας χρήστης υπογράφει ψηφιακά ένα μήνυμα που έχει επιλεγεί με συγκεκριμένο τρόπο από τον επιτιθέμενο. Υπάρχουν και οι γνωστές επιθέσεις παράπλευρου καναλιού, πχ. χρονισμού έναντι των υλοποιήσεων.

Η αξία του RSA βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών, ενώ άλλοι αλγόριθμοι βασίζονται σε αντίστοιχα δύσκολα μαθηματικά προβλήματα. Για να γίνουν αυτοί οι μαθηματικοί υπολογισμοί απαιτείται χρήση μεγάλου αριθμού σύνθετων πράξεων σε μεγάλους αριθμούς, πχ. τα 2048 bits που συνιστώνται για τον RSA. Αποτέλεσμα αυτού είναι οι ασύμμετροι αλγόριθμοι να έχουν μεγάλες απαιτήσεις σε υλικό για να πραγματοποιηθούν και απαιτούν αρκετό χρόνο. Για αυτό χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση των διακινούμενων κλειδιών, που χρησιμοποιούν οι συμμετρικοί αλγόριθμοι για κρυπτογράφηση και αποκρυπτογράφηση μεγάλων κειμένων.

Θα δούμε επίσης έναν αλγόριθμο που χρησιμοποιείται πολύ. Είναι ο αλγόριθμος των Diffie –Hleman (Whitfield Diffie, Martin Hellman), ο οποίος χρησιμοποιείται για την ασφαλή ανταλλαγή του κλειδιού, ενώ δεν μπορεί να κρυπτογραφήσει ένα μήνυμα. Η ασφάλεια του βασίζεται στη δυσκολία του προβλήματος του διακριτού λογάριθμου

(discrete logarithm problem - DLP). Για δοθέντα g, p και g^k(mod p), είναι δύσκολη η εύρεση του k. Ένας ακέραιος αριθμός g ονομάζεται γεννήτορας του mod p, όπου p πρώτος αριθμός, αν όλες οι δυνάμεις g^1(mod p), g^2(mod p), ... ,g^{p-1}(mod p), είναι ανά δυο διαφορετικές μεταξύ τους.

Δυο χρήστες Α και Β που θέλουν να επικοινωνήσουν συμφωνούν δημόσια σε ένα μεγάλο πρώτο αριθμό p και ένα αριθμό g που είναι γεννήτορας (mod p), οι οποίοι αποτελούν το δημόσιο κλειδί.

Ο Α επιλέγει ένα μυστικό αριθμό x, και ο Β επιλέγει ένα μυστικό αριθμό y.

Ο Α στέλνει τον αριθμό x' = g^x(mod p) στον Β.

Ο Β στέλνει τον αριθμό y' = g^y(modp) στον Α.

Ο Α υπολογίζει τον $(y')^x$ (mod p) = g^{xy}(mod p).

Ο Β υπολογίζει τον $(x')^y$ (mod p)= g^{xy}(mod p).

Και οι δυο υπολόγισαν τον ίδιο αριθμό, τον οποίο γνωρίζουν μόνο οι δυο τους, και ο οποίος μπορεί να χρησιμοποιηθεί για κρυπτογράφηση κειμένου, ως συμμετρικό κλειδί. Ο υποκλοπέας θα πρέπει γνωρίζοντας τα g,p και το g^x(mod p) να υπολογίσει το x. Για μεγάλες τιμές του p, που κάνουν ανέφικτη την εξαντλητική αναζήτηση, δεν υπάρχει αποδοτικός αλγόριθμος που να επιλύει το πρόβλημα. Απαραίτητο είναι ο Α και ο Β να πιστοποιούν ο ένας την ταυτότητα του άλλου, για να αποφύγουν την επίθεση man in the middle (αναφερόμαστε παρακάτω). Απόρροια του αλγόριθμου ήταν το πρωτόκολλο των Diffie-Hellman, που παρουσιάστηκε το 1976. Πριν από τη δημιουργία αυτού κάθε κρυπτογραφική τεχνική βασιζόταν σε κάποιο προσυμφωνημένο κλειδί. Το συγκεκριμένο πρωτόκολλο είναι το πρώτο που προτάθηκε ώστε να επιτρέπει σε δυο οντότητες, χωρίς προηγούμενη επικοινωνία, να ανταλλάξουν ένα κοινό κλειδί μέσω ενός μη ασφαλούς διαύλου επικοινωνίας.

Υπάρχει και έκδοση του αλγόριθμου που βασίζεται στη δυσκολία του προβλήματος του διακριτού προβλήματος σε ελλειπτικές καμπύλες ((Elliptic Curve Discrete Logaritmh Problem - ECDLP)) οι οποίες προτάθηκαν το 1985, είναι σε ευρεία χρήση από το 2004 [14].

Κεφάλαιο 4
Μηχανισμοί και Πρωτόκολλα Ασφάλειας

Προκειμένου να αποτρέψουμε την πρόσβαση ανεπιθύμητων σε οποιοδήποτε σύστημα ή δίκτυο και την αποφυγή των συνεπειών αυτής της εισβολής, κλοπή, μεταβολή δεδομένων κλπ. αναπτύχτηκαν υπηρεσίες, μηχανισμοί και πρωτόκολλα ασφαλείας που πετυχαίνουν να διατηρούν τα συστήματα ασφαλή.

4.1 Μηχανισμοί Ασφάλειας και Υπηρεσίες

Οι μηχανισμοί ασφαλείας και οι υπηρεσίες ασφαλείας αναφέρονται, σύμφωνα με το OSI (Open System Interconnection – Ανοικτό Σύστημα Ενδοεπικοινωνίας, οδηγία X.800), ξεχωριστά σε κάθε ένα από τα επτά επίπεδα που υπάρχουν σε αυτό το μοντέλο σύμφωνα με την ITU (International Telecommunication Union). Αναφερόμαστε γενικά για τις υπηρεσίες ασφαλείας που πρέπει να υλοποιούνται για να είναι ασφαλές ένα σύστημα [28].

- **Αυθεντικοποίηση** (Authentication)
  - **Επαλήθευση ταυτότητας οντοτήτων** (Peer entity authentication)
  - **Επαλήθευση προέλευσης δεδομένων** (Data origin authentication)
- **Έλεγχος πρόσβασης (Access control)**, παρεμπόδιση μη εξουσιοδοτημένης χρήσης πόρων
- **Εμπιστευτικότητα δεδομένων** (Data confidentiality), προστασία των δεδομένων από μη εξουσιοδοτημένη αποκάλυψη
  - **Εμπιστευτικότητα σύνδεσης** (Connection confidentiality), προστασία των δεδομένων όλων των χρηστών σε μια σύνδεση
  - **Εμπιστευτικότητα χωρίς σύνδεση** (Connectionless confidentiality), προστασία των δεδομένων του χρήστη σε ένα τμήμα δεδομένων (data block)

- **Εμπιστευτικότητα επιλεγμένου πεδίου** (Selective field confidentiality), η προστασία επιλεγμένων πεδίων στα δεδομένα του χρήστη σε μια σύνδεση ή σε ένα τμήμα δεδομένων
- **Εμπιστευτικότητα ροής κυκλοφορίας** (Traffic flow confidentiality), προστασία από πληροφορίες που προκύπτουν από παρατήρηση της κυκλοφοριακής ροής

❖ **Ακεραιότητα δεδομένων** (Data integrity), η διαβεβαίωση ότι τα δεδομένα που παρελήφθησαν είναι ίδια ακριβώς όπως τα έστειλε ένας εξουσιοδοτημένος χρήστης

- **Ακεραιότητα σύνδεσης με ανάκτηση** (Connection integrity with recovery), φροντίζει για την ακεραιότητα σε όλα τα δεδομένα του χρήστη σε μια σύνδεση και ανιχνεύει αλλαγές, τροποποιήσεις, εισαγωγές, διαγραφές ή επαναλήψεις με προσπάθεια ανάκτησης.
- **Ακεραιότητα σύνδεσης χωρίς ανάκτηση** (Connection integrity without recovery), όπως το προηγούμενο, κάνοντας μόνο ανίχνευση και όχι ανάκτηση
- **Επιλεγμένου πεδίου ακεραιότητα σύνδεσης** (Selective field connection integrity), φροντίζει για την ακεραιότητα των επιλεγμένων πεδίων στα δεδομένα του χρήστη ενός τμήματος δεδομένων που διαβιβάζεται σε μια σύνδεση και καθορίζει το πότε τα επιλεγμένα πεδία έχουν τροποποιηθεί, εισαχθεί, διαγραφεί ή επαναληφθεί.
- **Ακεραιότητα χωρίς σύνδεση** (Connectionless integrity), φροντίζει για την ακεραιότητα ενός τμήματος δεδομένων χωρίς σύνδεση, και μπορεί καθορίσει την ανίχνευση της τροποποίησης των δεδομένων, επίσης μπορεί να ανιχνεύσει μια περιορισμένη επανάληψη δεδομένων
- **Επιλεγμένου πεδίου ακεραιότητα χωρίς σύνδεση** (Selective field connectionless integrity), όπως το προηγούμενο αλλά για επιλεγμένα πεδία, χωρίς ανίχνευση επανάληψης

❖ **Μη αποποίηση** (Non-repudiation), προστατεύει από την άρνηση μίας από τις εμπλεκόμενες οντότητες σε μια επικοινωνία ότι συμμετείχε σε όλη ή σε μέρος της επικοινωνίας.

- **Μη αποποίηση με απόδειξη προέλευσης** (Non-repudiation with proof of origin), Ο παραλήπτης των δεδομένων έχει απόδειξη για την προέλευση των δεδομένων, αυτό θα προστατεύει από οποιαδήποτε απόπειρα από τον αποστολέα να αρνείται ψευδώς την αποστολή των δεδομένων ή των περιεχομένων τους

- **Μη αποποίηση με απόδειξη παράδοσης** (Non-repudiation with proof of delivery), ο αποστολέας των δεδομένων έχει απόδειξη για την παράδοση των δεδομένων, αυτό θα προστατεύει από οποιαδήποτε απόπειρα από τον παραλήπτη να αρνείται ψευδώς την παραλαβή των δεδομένων ή των περιεχομένων τους

Αναφερόμαστε και στους μηχανισμούς ασφαλείας.

- **Ειδικοί μηχανισμοί ασφαλείας** (Specific security mechanisms), που μπορούν να εφαρμοστούν στο αντίστοιχο επίπεδο
  - **Κρυπτογράφηση** (Encipherment), Η κρυπτογράφηση μπορεί να παρέχει εμπιστευτικότητα, είτε στα δεδομένα είτε στη κυκλοφορία των πληροφοριών, και μπορεί να παίξει τον κύριο ρόλο ή να συμπληρώσει έναν αριθμό άλλων μηχανισμών ασφαλείας(συμμετρική και ασύμμετρη όπως έχουμε ήδη αναφέρει)
  - **Μηχανισμοί ψηφιακής υπογραφής** (Digital signature mechanisms), καθορίζει δυο διαδικασίες, υπογραφή μιας μονάδας δεδομένων, και επαλήθευση μιας υπογεγραμμένης μονάδας δεδομένων. Η πρώτη διαδικασία χρησιμοποιεί πληροφορίες που είναι ιδιωτικές (μοναδικές και εμπιστευτικές) του υπογράφοντα. Η δεύτερη διαδικασία χρησιμοποιεί λειτουργίες και πληροφορίες που είναι δημόσια διαθέσιμες, αλλά από αυτές δεν μπορούν προκύψουν οι ιδιωτικές πληροφορίες του υπογράφοντος
  - **Μηχανισμοί ελέγχου πρόσβασης** (Access control mechanisms), μπορούν να βασίζονται σε ένα ή παραπάνω από τα επόμενα.
    - Βάσεις πληροφοριών που διατηρούνται τα δικαιώματα πρόσβασης των οντοτήτων. Προϋποθέτει ότι η αυθεντικοποίηση της οντότητας έχει εξασφαλιστεί.
    - Πληροφορίες αυθεντικοποίησης, όπως κωδικοί εισόδου (passwords), με του οποίους η οντότητα αποδεικνύει ότι έχει εξουσιοδότηση
    - Καθορισμός του επιπέδου πρόσβασης μιας οντότητας ανάλογα με την εξουσιοδότηση που του έχει καθοριστεί
    - Ετικέτες ασφαλείας, οι οποίες όταν συνδέονται με μια οντότητα μπορούν να χρησιμοποιηθούν για τη χορήγηση ή την άρνηση πρόσβασης, συνήθως σύμφωνα με μια πολιτική ασφάλειας
    - Ώρα, διαδρομή και διάρκεια απόπειρας πρόσβασης.

- **Μηχανισμοί ακεραιότητας δεδομένων** (Data integrity mechanisms), έχουμε δύο κατηγορίες, την ακεραιότητα μια απλής μονάδας δεδομένων ή πεδίου και την ακεραιότητα μιας ροής δεδομένων ή πεδίων
- **Μηχανισμοί αυθεντικοποίησης ανταλλαγής** (Authentication exchange mechanism), με χρήση πληροφοριών αυθεντικοποίησης (πχ. passwords), χρήση χαρακτηριστικών και ιδιοτήτων της οντότητας (δικαιώματα), χρήση κρυπτογραφικών τεχνικών, τεχνικές χρονοσήμανσης (time stamping) κλπ Μηχανισμοί συμπλήρωσης κυκλοφορίας (Traffic padding mechanisms), για προστασία ενάντια στην ανάλυση της κυκλοφορίας
- **Μηχανισμοί ελέγχου διαδρομών** (Routing control mechanisms), οι διαδρομές μπορούν να επιλεγούν είτε δυναμικά είτε με προκαθορισμό, ώστε να χρησιμοποιηθούν μόνο φυσικά ασφαλή υποδίκτυα, αναμεταδότες ή σύνδεσμοι
- **Μηχανισμοί αρχών** (Notarization mechanism), ιδιότητες σχετικά με τα δεδομένα που μεταδίδονται μεταξύ δύο ή περισσοτέρων οντοτήτων, όπως η ακεραιότητα, η προέλευση, ο χρόνος και ο προορισμός, μπορούν να εξασφαλιστούν με την χρήση μιας αξιόπιστης αρχής-μηχανισμού. Η εξασφάλιση παρέχεται από τρίτο μέρος, μια αρχή, την οποία εμπιστεύονται οι επικοινωνούντες φορείς

❖ **Διάχυτοι μηχανισμοί ασφαλείας (Pervasive security mechanisms)**, οι οποίοι δεν αφορούν συγκεκριμένες υπηρεσίες

- **Αξιόπιστη λειτουργικότητα** (Trusted functionality), οι αξιόπιστες λειτουργίες μπορούν να χρησιμοποιηθούν για την επέκταση του εύρους ή για την εξασφάλιση της αποτελεσματικότητας άλλων μηχανισμών ασφάλειας. Οποιαδήποτε λειτουργία που παρέχει άμεσα ή παρέχει πρόσβαση σε μηχανισμούς ασφαλείας πρέπει να είναι αξιόπιστη.
- **Ετικέτες ασφαλείας** (Security labels), οι πόροι, συμπεριλαμβανομένων των στοιχείων δεδομένων, μπορεί να έχουν σχετικές ετικέτες ασφαλείας, π.χ. για να υποδείξουν το επίπεδο ευαισθησίας. Συχνά είναι απαραίτητο να διαβιβάζεται η κατάλληλη ετικέτα ασφαλείας με δεδομένα που μεταφέρονται
- **Ανίχνευση συμβάντων** (Event detection), η ανίχνευση συμβάντων σχετικών με την ασφάλεια περιλαμβάνει τον εντοπισμό παραβιάσεων της ασφάλειας, αλλά μπορεί επίσης να περιλαμβάνει ανίχνευση κανονικών συμβάντων, όπως επιτυχή σύνδεση.

- **Ασφάλεια ελέγχου ιχνών** (Security audit trail), προσφέρουν ένα πολύτιμο μηχανισμό ασφαλείας γιατί επιτρέπουν την ανίχνευση και διερεύνηση των παραβιάσεων ασφαλείας επιτρέποντας ένα επακόλουθο έλεγχο ασφαλείας. Ο έλεγχος ασφαλείας είναι μια ανεξάρτητη (από τρίτο) επισκόπηση και εξέταση των εγγραφών και των δραστηριοτήτων του συστήματος, προκειμένου να ελέγχεται η καταλληλότητα των ελέγχων του συστήματος
- **Ανάκτηση ασφαλείας** (Security recovery), η ανάκτηση ασφαλείας ασχολείται με αιτήματα από μηχανισμούς όπως η διαχείριση συμβάντων ή λειτουργίες διαχείρισης, και αναλαμβάνει ενέργειες ανάκτησης ως αποτέλεσμα της εφαρμογής ενός συνόλου κανόνων

4.2 Πρωτόκολλα Ασφάλειας

Το βασικότερο πρωτόκολλο που χρησιμοποιείται για την επικοινωνία των υπολογιστικών συστημάτων είναι το πρωτόκολλο TCP/IP (Transmission Control Protocol/Internet Protocol), το οποίο αποτελείται από επίπεδα, τα οποία δεν αντιστοιχούν ένα προς ένα με το μοντέλο αναφοράς OSI. Σε αυτό η μετάδοση των δεδομένων δεν είναι κρυπτογραφημένη, πχ. το HTTP (Hyper Text Transfer Protocol) στο επίπεδο εφαρμογής . Έτσι αυτό συνδυάζεται με άλλα πρωτόκολλα, συνήθως πρωτόκολλα κρυπτογράφησης, που δρουν κάτω από το επίπεδο εφαρμογής, για να προσφέρουν την απαιτούμενη ασφάλεια. Ένα από αυτά είναι το SSL (Secure Sockets Layer) και έτσι προκύπτει το HTTPS (HTTP Secure). Έχουμε ήδη αναφέρει ότι το SSL, δεν είναι πλέον ασφαλές και έχει αντικατασταθεί σε μεγάλο βαθμό από τον διάδοχο του, το TLS (Transport Layer Security).

Το **Transport Layer Security (TLS)** και το παλαιότερο , το Secure Sockets Layer (SSL), είναι πρωτόκολλα που βασίζονται στην κρυπτογράφηση για να παρέχουν ασφάλεια στις επικοινωνίες σε ένα δίκτυο υπολογιστών. Το TLS είναι ένα πρωτόκολλο που εγκαθιστά μια ασφαλή σύνδεση ανάμεσα σε ένα πελάτη και ένα εξυπηρετητή και εξασφαλίζει την ιδιωτικότητα και την ακεραιότητα της πληροφορίας κατά τη διάρκεια της μετάδοσης. Κρυπτογραφεί τα τμήματα της δικτυακής σύνδεσης στο στρώμα εφαρμογής για το στρώμα μεταφοράς. Χρησιμοποιεί ασύμμετρη κρυπτογράφηση για την ανταλλαγή των κλειδιών, συμμετρική κρυπτογράφηση για εμπιστευτικότητα και κώδικα αυθεντικοποίησης μηνύματος για την ακεραιότητα των μηνυμάτων. Το TLS περιλαμβάνει δυο στρώματα, το TLS Record Protocol (πρωτόκολλο εγγραφής) και το

TLS Handshake Protocol (πρωτόκολλο χειραψίας). Το πρωτόκολλο χειραψίας είναι υπεύθυνο για την αυθεντικοποίηση και την ανταλλαγή κλειδιών αναγκαία για την εγκαθίδρυση ή την επανέναρξη ασφαλών συνόδων. Όταν εγκαθίσταται μια ασφαλής σύνοδος το πρωτόκολλο χειραψίας διαχειρίζεται, την διαπραγμάτευση της ακολουθίας-σετ (suite) κρυπτογραφικών αλγόριθμων, την αυθεντικοποίηση και την ανταλλαγή κλειδιών. Στη διαπραγμάτευση ο πελάτης και ο εξυπηρετητής επικοινωνούν και επιλέγουν την ακολουθία κρυπτογραφικών αλγόριθμων που θα χρησιμοποιηθεί κατά την ανταλλαγή μηνυμάτων. Κατά την αυθεντικοποίηση ο εξυπηρετητής αποδεικνύει την ταυτότητα του στον πελάτη, ο πελάτης μπορεί να χρειαστεί να αποδείξει την ταυτότητα του στον εξυπηρετητή, και χρησιμοποιείται η υποδομή δημόσιου κλειδιού για την αυθεντικοποίηση. Ο πελάτης και ο εξυπηρετητής με τη διαδικασία ανταλλαγής κλειδιών συμφωνούν-δημιουργούν τα κλειδιά συνόδου, που χρησιμοποιούνται ένα για κατακερματισμό, και ένα για κρυπτογράφηση. Αφού ολοκληρωθεί η χειραψία, ο πελάτης και ο εξυπηρετητής ανταλλάσουν τα δεδομένα των εφαρμογών πάνω στο ασφαλές κανάλι που εγκατέστησαν, κρυπτογραφημένα με το κλειδί συνόδου. Το πρωτόκολλο εγγραφής, ασφαλίζει τα δεδομένα των εφαρμογών χρησιμοποιώντας τα κλειδιά που δημιουργήθηκαν κατά τη διαδικασία της χειραψίας επαληθεύοντας την ακεραιότητα και την προέλευση. Η ανταλλαγή κλειδιών και η αυθεντικοποίηση γίνεται με χρήση των αλγορίθμων, RSA, RSA με χρήση DHE (Diffie-Hellman-Exchange), RSA με χρήση ECDH, δηλαδή Diffie-Hellman με χρήση αλγόριθμων ελλειπτικών καμπυλών και άλλους συνδυασμούς. Η κρυπτογράφηση των δεδομένων γίνεται με AES σε λειτουργία GCM και άλλους συνδυασμούς. Χρησιμοποιείται για ασφαλή περιήγηση στο διαδίκτυο, για εφαρμογές ηλεκτρονικού ταχυδρομείου, για κλήσεις μέσω IP (VoIP) [29] [30].

Ένα άλλο πρωτόκολλο ασφάλειας είναι το **IPsec (Internet Protocol Security)**, που απαρτίζεται από πρωτόκολλα, που αναπτύχθηκαν από την IETF (Internet Engineering Task Force), για να υποστηρίξουν την ασφαλή μετάδοση πακέτων στο στρώμα IP του πρωτοκόλλου TCP/IP. Το IPsec προσφέρει έλεγχο πρόσβασης, ακεραιότητα χωρίς σύνδεση, πιστοποίηση αυθεντικότητας προέλευσης δεδομένων, απόρριψη επαναλαμβανόμενων πακέτων (replayed packets), εμπιστευτικότητα (με χρήση κρυπτογράφησης) και περιορισμένη εμπιστευτικότητα ροής (κρύβει τα στατιστικά χαρακτηριστικά του πρότυπου κυκλοφορίας). Έχει δύο τρόπους λειτουργίας. Τη κατάσταση μεταφοράς (Transport mode), στην οποία κρυπτογραφούνται ή αυθεντικοποιούνται μόνο τα δεδομένα (payload) και όχι η επικεφαλίδα του IP πακέτου,

από τον αποστολέα, και την κατάσταση σήραγγας (Tunnel mode), στο οποίο κρυπτογραφούνται και η επικεφαλίδα και τα δεδομένα. Αυτός ο τρόπος χρησιμοποιείται για την δημιουργία VPN. Για να λειτουργήσει το IPsec ο αποστολέας και ο παραλήπτης πρέπει να χρησιμοποιούν προμοιρασμένα κλειδιά. Υποστηρίζονται δυο τρόποι διαχείρισης κλειδιών, η χειροκίνητη διαχείριση και η αυτόματη διαχείριση που βασίζεται στα πρωτόκολλα Oakley/ISAKMP. Οι αλγόριθμοι κρυπτογραφίας που χρησιμοποιούνται για προστασία της ακεραιότητας και αυθεντικοποίηση είναι ο HMAC-SHA1/SH2, για εμπιστευτικότητα ο AES-CBC, και ο AES-GCM για εμπιστευτικότητα και αυθεντικοποίηση [29].

Η παροχή περιορισμών ασφάλειας και ιδιωτικότητας στο IoT εξακολουθεί να είναι μια πρόκληση, λόγω του τεράστιου αριθμού ετερογενών συσκευών, αλλά και στην ανταλλαγή δεδομένων μέσω ανασφαλών συνδέσεων. Επιπλέον η έννοια της ασφάλειας επεκτείνεται και πέραν της συσκευής με συσκευή σύνδεση (από άκρη σε άκρη εμπιστευτικότητα και ακεραιότητα), και στα θέματα του δικτύου (αυθεντικοποίηση συσκευών και πρόσβασης στα δίκτυα). Σαν παράδειγμα αναφέρουμε τη δημιουργία ψεύτικων δικτύων (fake networks-termed botnets) από επιτιθέμενους (hackers) για την υποκλοπή δεδομένων και στοιχείων ιδιωτικότητας των χρηστών [20].
Στο IoT, αρκετές τεχνολογίες έχουν αναπτυχθεί για να προσφέρουν ασφάλεια και ιδιωτικότητα των πληροφοριών, όπως το TLS που αναφέραμε παραπάνω, που βελτιώνει την εμπιστευτικότητα και την ακεραιότητα, η δρομολόγηση πολλαπλών στρωμάτων (onion routing), που κρυπτογραφεί και αναμειγνύει την κυκλοφορία του διαδικτύου από διαφορετικές πηγές, και κρυπτογραφεί τα δεδομένα σε πολλαπλά επίπεδα-στρώματα (layers) χρησιμοποιώντας δημόσια κλειδιά στη διαδρομή μετάδοσης των (δεδομένων). Επίσης με χρήση κρυπτογραφίας μπορούμε να αντιμετωπίσουμε πολλές από τις επιθέσεις σε ένα IoT σύστημα [7], όπως το την υποκλοπή δεδομένων (eavesdropping κρυφάκουσμα) την ανάλυση της κυκλοφορίας των δεδομένων, τον άνθρωπο στη μέση (man in the middle) γιατί δεν θα μπορεί να ‘διαβάσει’ τα δεδομένα που μεταφέρονται. Αποφεύγουμε επίσης και τις επιθέσεις DoS (DoS-Denial of Service, άρνηση εξυπηρέτησης) ασφαλίζοντας με κρυπτογραφικές μεθόδους την ασφάλεια του δικτύου [31].

Τα 6LoWPAN δίκτυα, τα οποία θα δούμε παρακάτω αναλυτικά, επηρεάζονται από επιθέσεις ασφαλείας που μπορεί να προξενήσουν ζημιά στο δίκτυο ή να υποκλέψουν

πληροφορίες από αυτό. Αυτές οι επιθέσεις είναι δυο τύπων. Οι επιθέσεις εκ των έσω (προερχόμενες από κακόβουλους κόμβους του δικτύου, δηλαδή κόμβους που ο επιτιθέμενος με κάποιο τρόπο έχει τροποποιήσει και τους χρησιμοποιεί προς όφελος του), και οι επιθέσεις από έξω (επιθέσεις από συσκευές που δεν έχουν εξουσιοδοτημένη πρόσβαση στο δίκτυο, αλλά καταφέρνουν να διεισδύσουν σε αυτό). Επιπλέον οι επιθέσεις μπορεί να είναι παθητικές, όταν ο κύριος σκοπός του επιτιθέμενου είναι να κατασκοπεύσει το δίκτυο και να πάρει απόρρητες πληροφορίες, ή οι ενεργητικές επιθέσεις, που επιδρούν απ' ευθείας στην απόδοση του δικτύου και έτσι προκαλούν τη δυσλειτουργία του, όπως οι επιθέσεις άρνησης εξυπηρέτησης DoS.

Για την ασφαλή μετάδοση των δεδομένων στο IoT, μπορούμε να χρησιμοποιήσουμε την βασισμένη στο χρόνο (time based) παραγωγή και ανανέωση κλειδιών και για τις μονόδρομες και για τις αμφίδρομες επικοινωνίες δυο συσκευών, η οποία ανανέωση μπορεί να γίνεται και κατά τη διάρκεια της μετάδοσης, επιλέγοντας τα κλειδιά από μια διαμοιρασμένη ακολουθία κλειδιών. Χρησιμοποιούμε τους αλγόριθμους AES και SHA για τη διαφύλαξη της εμπιστευτικότητας και της ακεραιότητας. Η αρχή βασίζεται στη χρήση μιας χρονοσφραγίδας του τοπικού αναμεταδότη (που εισάγεται στο χωρίς κρυπτογράφηση (plain) τμήμα του αποστελλομένου πλαισίου (frame)), για να καθορίσει το κλειδί της κρυπτογράφησης. Μετά αυτό χρησιμοποιείται από το δέκτη για να επιλέξει το κλειδί αποκρυπτογράφησης χωρίς να γίνει κάποια ανταλλαγή κλειδιών ή επιπλέον αποστολή και παραλαβή μηνυμάτων. Η τεχνική αυτή μειώνει δραστικά τις επιθέσεις ασφαλείας και ελαχιστοποιεί-απλοποιεί τις δυνατότητες που πρέπει να έχουν οι συσκευές που χρησιμοποιούνται, πράγμα θεμελιώδες για το IoT. Επίσης εισάγεται και εφαρμόζεται η αρχή της γνωστικής ασφάλειας (cognitive security) στη βασισμένη στο χρόνο λύση ασφαλείας , προσδιορίζοντας τις κύριες παραμέτρους που πρέπει να παρακολουθούνται και να μετριούνται (τα οποία συγκρίνονται με ιστορικά δεδομένα ιδίου τύπου και αναζητούνται, με χρήση αλγορίθμων, αποκλίσεις-αλλαγές) από συντελεστές του δικτύου ώστε να ενδυναμωθεί και να γίνει πιο αυστηρή η ασφάλεια σε ένα ποικίλο και πολύπλοκο περιβάλλον όπως αυτό το IoT [20].

Κεφάλαιο 5
Επικοινωνία και Ασφάλεια στο IoT

Έχοντας αναφερθεί μέχρι τώρα στο IoT, καλό θα είναι να κάνουμε τη διάκριση ανάμεσα σε αυτό, το IoT, και στα CPS (Cyber Physical Systems, Κύβερνο Φυσικά Συστήματα). Τα CPS είναι τα ολοκληρωμένα συστήματα από φυσικά εξαρτήματα, αισθητήρες, εκκινητήρες, δίκτυα επικοινωνίας, και κέντρα ελέγχου. Σε αυτά οι αισθητήρες αναπτύσσονται για να μετρούν και παρακολουθούν φυσικές συσκευές, οι εκκινητήρες για να εξασφαλίζουν την επιθυμητή λειτουργία των φυσικών συσκευών, τα δίκτυα για να στέλνουν τις πληροφορίες από τους αισθητήρες στα κέντρα ελέγχου και να επιστρέφουν σε αυτούς και στους εκκινητήρες ανάδραση-εντολές που προκύπτουν από την ανάλυση-επεξεργασία της πληροφορίας που γίνεται στα κέντρα ελέγχου ώστε το σύστημα να δουλεύει σε επιθυμητά επίπεδα. Ενώ το IoT είναι η δικτυακή υποδομή που ενώνει ένα μεγάλο αριθμό ετερογενών συσκευών και να παρακολουθεί και να ελέγχει αυτές. Δηλαδή ο κύριος σκοπός του IoT είναι να διασυνδέει ποικίλα δίκτυα ώστε να επιτυγχάνεται η συλλογή των δεδομένων, ο διαμοιρασμός των πόρων, η ανάλυση-επεξεργασία και η διαχείριση ανάμεσα σε ετερογενή δίκτυα.

Επομένως το IoT είναι μια οριζόντια αρχιτεκτονική η οποία πρέπει να ενσωματώνει τα επίπεδα επικοινωνίας (communication layers) όλων των εφαρμογών CPS για να επιτευχθεί η διασύνδεση. Η διασύνδεση διαφόρων δικτύων δεν περιορίζεται μόνο στις φυσικές συνδέσεις, αλλά ένα σχέδιο ελέγχου (control plane) που περιλαμβάνει διεπαφές, πρωτόκολλα, μεσισμικό-middleware, κλπ., πρέπει να σχεδιαστεί για να εξασφαλίσει ότι τα δεδομένα διακινούνται αποδοτικά ανάμεσα σε διαφορετικά δίκτυα [32]. Για να επιτευχθούν αυτά έχουν αναπτυχθεί διάφοροι σχεδιασμοί και αρχιτεκτονικές.

5.1 Αρχιτεκτονικές, Πρωτόκολλα και Υπηρεσίες στο IoT

Εδώ θα δούμε υπάρχουσες αρχιτεκτονικές για το IoT, την αρχιτεκτονική τριών επιπέδων-στρωμάτων (Three Layer Architecture) και την προσανατολισμένη σε υπηρεσίες αρχιτεκτονική (SoA Based Architecture) [32].

Η αρχιτεκτονική τριών στρωμάτων τυπικά υποδιαιρείται σε τρία βασικά επίπεδα-στρώματα,

- **Στρώμα αντίληψης** – perception layer , γνωστό και σαν το επίπεδο των αισθητήρων και υλοποιείται σαν το κατώτερο επίπεδο στη αρχιτεκτονική του IoT. Αυτό αλληλεπιδρά με τις φυσικές συσκευές μέσω έξυπνων συσκευών (RFID, sensors, actuators, κλπ. Ο κύριος σκοπός του είναι να συνδέει αντικείμενα στο IoT και να μετρά, συλλέγει και επεξεργάζεται τις βασικές πληροφορίες που σχετίζονται με αυτά τα αντικείμενα μέσω έξυπνων συσκευών μεταδίδοντας τις επεξεργασμένες πληροφορίες στο ανώτερο στρώμα μέσω των διεπαφών του στρώματος.
- **Στρώμα δικτύου** - network layer, γνωστό και σαν στρώμα μετάδοσης υλοποιείται σαν το μεσαίο στρώμα στη IoT αρχιτεκτονική. Χρησιμοποιείται για να λαμβάνει τις επεξεργασμένες πληροφορίες που προέρχονται από το στρώμα αντίληψης και καθορίζει τις διαδρομές για τη μετάδοση των δεδομένων και των πληροφοριών στις IoT συσκευές, hubs (πλήμνη- κέντρο διασυρμάτωσης) και εφαρμογές μέσω ολοκληρωμένων δικτύων. Επίσης στέλνει προς το στρώμα εφαρμογής πληροφορίες. Είναι το σημαντικότερο στρώμα της IoT, γιατί διαφορετικές συσκευές και πολλές τεχνολογίες επικοινωνίας (Bluetooth, WiFi, LTE- Long Term Evolution-4G LTE, 3G/4G κλπ.) ενσωματώνονται σε αυτό το στρώμα. Το στρώμα δικτύου πρέπει να μεταδίδει δεδομένα από και προς διαφορετικά πράγματα ή εφαρμογές μέσω διεπαφών και πυλών (gateways) ανάμεσα σε ετερογενή δίκτυα χρησιμοποιώντας διάφορες τεχνολογίες επικοινωνίας και πρωτόκολλα.
- **Στρώμα εφαρμογής** - application layer, γνωστό και σαν στρώμα επιχείρησης, λαμβάνει δεδομένα από το στρώμα δικτύου και τα χρησιμοποιεί για τη παροχή απαιτούμενων υπηρεσιών ή λειτουργιών. Ένα πλήθος εφαρμογών υπάρχει σε αυτό το επίπεδο πχ, έξυπνες πόλεις, έξυπνες μεταφορές κλπ.

Η αρχιτεκτονική τριών στρωμάτων είναι βασική για το IoT και έχει σχεδιαστεί και πραγματοποιηθεί σε αρκετά συστήματα πχ συστήματα άρδευσης [33]. Οι εφαρμογές και οι λειτουργίες που γίνονται στα στρώματα δικτύου και εφαρμογών είναι πολλές και σύνθετες. Το στρώμα δικτύου δεν πρέπει μόνο να καθορίζει διαδρομές και να μεταδίδει δεδομένα αλλά πρέπει να παρέχει και υπηρεσίες δεδομένων (συγκέντρωση δεδομένων, υπολογισμούς, κλπ.). Το στρώμα εφαρμογής εκτός των υπηρεσιών σε πελάτες και συσκευές πρέπει να παρέχει και υπηρεσίες δεδομένων (εξόρυξη δεδομένων, analytics δεδομένων, κλπ.). Για το λόγο αυτό αναπτύχθηκε η προσανατολισμένη σε υπηρεσίες αρχιτεκτονική που ανάμεσα στο στρώμα δικτύου και στο στρώμα εφαρμογής έχει ένα επιπλέον στρώμα, το στρώμα υπηρεσιών (service layer).

Η τεχνική SoA είναι βασισμένη στο μοντέλο των δομικών στοιχείων-συστατικών (component based model), που είναι σχεδιασμένο για να συνδέει διαφορετικές λειτουργικές μονάδες (τις υπηρεσίες) μιας εφαρμογής μέσω διεπαφών και πρωτοκόλλων. Η SoA επικεντρώνεται στο σχεδιασμό της ροής συναφών υπηρεσιών, επιτρέποντας την επαναχρησιμοποίηση συστατικών λογισμικού και υλικού. Είναι ανεξάρτητη από προμηθευτές προϊόντα και τεχνολογίες. Έτσι χρησιμοποιώντας υπηρεσίες δεδομένων από το στρώμα δικτύου και το στρώμα εφαρμογής της αρχιτεκτονικής τριών στρωμάτων δημιουργείται ένα νέο στρώμα, το στρώμα υπηρεσιών ή διεπαφών ή μεσισμικό (service layer, interface, middleware). Έτσι στην αρχιτεκτονική SoA έχουμε τέσσερα στρώματα,

- **Στρώμα αντίληψης** – perception layer, όπως και στην περίπτωση των τριών στρωμάτων.
- **Στρώμα δικτύου** - network layer, χρησιμοποιείται για να καθορίσει τις διαδρομές και να παρέχει μετάδοση δεδομένων μέσω ολοκληρωμένων ετερογενών δικτύων.
- **Στρώμα υπηρεσιών** – Service layer, που βρίσκεται ανάμεσα στα στρώματα δικτύου και εφαρμογής και παρέχει υπηρεσίες για υποστήριξη του στρώματος εφαρμογής. Αποτελείται από υπηρεσίες ανεύρεσης, σύνθεσης, διαχείρισης, διεπαφών (discovery, composition, management, interfaces. Η υπηρεσία ανεύρεσης χρησιμοποιείται για να βρίσκει επιθυμητά αιτήματα, η υπηρεσία σύνθεσης αλληλεπιδρά με τα συνδεδεμένα αντικείμενα και διαιρεί ή ολοκληρώνει υπηρεσίες ώστε να ικανοποιούνται οι υπηρεσίες αιτημάτων με αποτελεσματικό τρόπο, η υπηρεσία διαχείρισης διαχειρίζεται και καθορίζει τους

μηχανισμούς εμπιστευτικότητας ώστε να ικανοποιεί τις υπηρεσίες αιτημάτων, διεπαφών και να υποστηρίζει τις αλληλεπιδράσεις ανάμεσα σε όλες τις παρεχόμενες υπηρεσίες.

- **Στρώμα εφαρμογής** - application layer, υποστηρίζει τις υπηρεσίες αιτημάτων των χρηστών και μπορεί να υποστηρίξει ένα αριθμό εφαρμογών όπως έξυπνη πόλη, έξυπνη μεταφορά κλπ.

Έχοντας υπ' όψη τις αρχιτεκτονικές που αναφέρθηκαν παραπάνω το IoT μπορεί να υλοποιηθεί-εξελιχθεί χρησιμοποιώντας αρκετές καινοτόμες τεχνολογίες, κάποιες έχουν ήδη αναφερθεί. Παίρνοντας σαν παράδειγμα την SoA του IoT, μπορούμε να δούμε αυτές τις τεχνολογίες ανάλογα το στρώμα στο οποίο βρίσκονται [32].

Στο **στρώμα αντίληψης**, όπου η κύρια λειτουργία του είναι να αναγνωρίζει και να παρακολουθεί αντικείμενα, οι παρακάτω τεχνολογίες μπορούν χρησιμοποιηθούν:

- **RFID**, επιπλέον των ανωτέρω, σε φυσικό επίπεδο, αποτελούνται από ένα μικροτσίπ, μια κεραία, που μαζί αποτελούν την ετικέτα (tag) και ένα αναγνώστη (reader). Κάθε ετικέτα προσαρμόζεται σε ένα αντικείμενο και έτσι του αποδίδει ένα μοναδικό αριθμό αναγνώρισης και με αυτόν μπορεί να ταυτοποιηθεί. Η ετικέτα δεν έχει ενσωματωμένη πηγή ενέργειας. Η τεχνολογία αυτή έχει πλεονεκτήματα, γρήγορη ανίχνευση χωρίς να απαιτείται επαφή, διάρκεια, επαναχρησιμοποίηση, ασφάλεια, μικρό μέγεθος, μικρό κόστος. Οπότε είναι χρήσιμη για αναγνώριση και παρακολούθηση αντικειμένων.
- **WSN**, επιπλέον αναφέρουμε, ότι μπορούν να παρακολουθούν, να καταγράφουν και να μεταδίδουν την κατάσταση των συσκευών μέσω κέντρων ελέγχου ή κόμβων αποδοχής (sink nodes). Τα πλεονεκτήματα τους είναι η επεκτασιμότητα, η δυναμική αναδιαμόρφωση, το μικρό μέγεθος, το μικρό κόστος και η μικρή κατανάλωση ενέργειας. Δηλαδή μας δίνουν τη δυνατότητα να αντιλαμβανόμαστε τις φυσικές παραμέτρους του πραγματικού κόσμου που σχετίζονται με τον περιβάλλοντα χώρο.

Σε αυτό το επίπεδο μπορεί να χρησιμοποιηθεί και το Barcode ή το QRcode με χρήση αναγνώστη υπέρυθρων ακτίνων, για αναγνώριση αντικειμένων. Επίσης υπάρχει και το RFID sensor network (RSN), που είναι μια ολοκλήρωση ενός RFID συστήματος και του WSN.

Στο **στρώμα δικτύου** που καθορίζει τις διαδρομές και παρέχει μεταφορά δεδομένων μέσω ετερογενών δικτύων μπορούν να χρησιμοποιηθούν τα παρακάτω πρωτόκολλα, τα οποία είναι αξιόπιστα και ασφαλή για χρήση στο IoT. [32] [20] :

- **IEEE 802.15.4**: Έχουμε απλώς αναφερθεί σε αυτό, δίνουμε όμως μερικές επί πλέον πληροφορίες γιατί αποτελεί το πρότυπο στις ασύρματες επικοινωνίες για συσκευές μικρής ισχύος, χαμηλού ρυθμού μετάδοσης δεδομένων, ασύρματα δίκτυα κάλυψης μικρών αποστάσεων αισθητήρων (sensors) και εκκινητών (actuators). Αναπτύχτηκε στα πλαίσια της ομάδας προσωπικής περιοχής δικτύου (PAN-Personal Area Network) του IEEE 802.15. Ο τυπικός ρυθμός μετάδοσης είναι 250kb/s με το μέγιστο μέγεθος πακέτου (packet size) τα 127 bytes, το οποίο περιορίζει τα διαθέσιμα bytes από 86 έως 116. Καθορίζει ένα φυσικό στρώμα (physical layer), έχει 16 κανάλια άμεσης ακολουθίας φάσματος διασποράς (direct sequence spread spectrum), και ένα στρώμα ελέγχου μέσων (MAC-Media Access Control). Μπορεί να χρησιμοποιηθεί σε πολυαλματικά δίκτυα, αλλά απαιτεί η συσκευή να είναι συνεχώς ανοικτή. Χρησιμοποιεί μονοκαναλική λειτουργία, η οποία πάσχει από πολυκαναλική εξασθένιση και σκίαση.
- **IEEE 802.15.4e**: Χρησιμοποιεί μια τεχνική που λέγεται συγχρονισμένη στο χρόνο άλμα καναλιού (TSCH-Time Synchronized Channel Hopping), για να αποφύγει τις παρεμβολές, τη σκίαση και τις πολυκαναλικές εξασθενίσεις. Το ανασχεδιασμένο πρωτόκολλο MAC υποστηρίζει κεντρική ή κατανεμημένη διαχείριση χρονοθυρίδων (time slots) ανάμεσα σε γειτονικούς κόμβους του δικτύου. Μια δομή χρόνου-συχνότητας χρησιμοποιείται για να δημιουργεί εικονικούς συνδέσμους (virtual links) ανάμεσα σε γειτονικούς σταθμούς χρησιμοποιώντας ειδικά κανάλια χρονοθυρίδων/ συχνοτοθυρίδων. Το πρότυπο δεν καθορίζει πως το χρονοδιάγραμμα των ζευγαριών χρονοθυρίδων/συχνοτοθυρίδων για ένα συγκεκριμένο εικονικό σύνδεσμο θα πραγματοποιηθεί.
- **6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks**-IPv6 πάνω σε χαμηλής ισχύος ασύρματα προσωπικά δίκτυα)**,** πρωτόκολλο που παρέχει ένα στρώμα προσαρμογής (ώστε να εξασφαλίζει τη διαλειτουργικότητα ανάμεσα στο διαδίκτυο και τα δίκτυα αισθητήρων, και βρίσκεται ανάμεσα στο στρώμα δικτύου και στο στρώμα ζεύξης στο μοντέλο OSI) για να κατακερματίζει και ανασυναρμολογεί τα IPv6 datagrams, λόγω του ότι τα πακέτα του IPv6 είναι

πολύ μεγάλα για το IEEE 802.15.4 πρότυπο ασύρματων επικοινωνιών για 'μικρές' συσκευές. Αναλυτικότερα Το 6LoWPAN επιτρέπει σε ενσωματωμένους κόμβους (embedded nodes, κόμβοι του δικτύου που κάνουν μια συγκεκριμένη δουλεία, συνήθως σε πραγματικό χρόνο, είναι εφοδιασμένοι με μικροεπεξεργαστές και έχουν RAM και ROM, κατ' αναλογία των ενσωματωμένων συστημάτων) να χρησιμοποιούν ένα περιορισμένο υποσύνολο των διευθύνσεων του IPv6. Λεπτομερέστερα το 6LoWPAN είναι ο συνδυασμός του IPv6 και του IEEE 802.15.4, έχοντας σαν σημαντική διαφορά το μέγεθος του πακέτου (packet size)του IPv6. Έτσι η ομάδα εργασίας του για το 6LoWPAN του IETF (Internet Engineering Task Force) πρότεινε να υπάρχει ένα στρώμα προσαρμογής (adaptation layer) που βελτιστοποιεί τα πακέτα του IPv6, με κατακερματισμό και συναρμολόγηση, ώστε να υποστηρίζεται από το επίπεδο σύνδεσης (link layer) του IEEE 802.15.4. Ένα 6LoWPAN δίκτυο αποτελείται από ένα ή περισσότερα LoWPAN δίκτυα συνδεδεμένα στο διαδίκτυο μέσω ενός δρομολογητή στην άκρη του δικτύου (edge router), ο οποίος ελέγχει την εισερχόμενη και εξερχόμενη κίνηση από τα LoWPAN δίκτυα. Οι συσκευές που χρησιμοποιούνται στα 6LoWPAN δίκτυα χαρακτηρίζονται από τη μικρή εμβέλεια των κυμάτων, χαμηλό ρυθμό μετάδοσης δεδομένων, χαμηλή κατανάλωση ισχύος και μικρό κόστος. Σε ένα LoWPAN δίκτυο έχουμε δυο κατηγορίες συσκευών, τις πλήρους λειτουργικότητας συσκευές (FFD-Full Function Devices), και τις περιορισμένης λειτουργικότητας συσκευές (RFD-Reduced Function Devices) που συνδέονται με τον edge router, που είναι υπεύθυνος για τη σύνδεση με το διαδίκτυο. Επιπλέον ένα LoWPAN υποστηρίζει δυο τοπολογίες δικτύου, την τοπολογία αστέρα (star topology, οι κόμβοι επικοινωνούν με ένα συντονιστή, υπεύθυνο για τη διαχείριση των επικοινωνιών στο δίκτυο) και την τοπολογία πλέγματος (mesh topology, οι κόμβοι επικοινωνούν ο ένας με τον άλλο απ' ευθείας). Μέσα στο LoWPAN δίκτυο οι συσκευές δεν χρησιμοποιούν την IPv6 διεύθυνση ή την πλήρη επικεφαλίδα (full header) του UDP (User Datagram Protocol) πρωτοκόλλου, επαφίεται στον edge router να επικοινωνήσει με τον έξω κόσμο. Η ομάδα εργασίας για δρομολόγηση σε χαμηλής ισχύος και με απώλειες δίκτυα (ROLL-Routing over Low power and Lossy Network- LLNS) της IEFT πρότεινε το RPL (routing protocol for low power and lossy networks), επιτρέπει σε ένα αποστολέα ενός πακέτου να καθορίσει, μερικά ή πλήρως, τη διαδρομή που ακολουθεί το πακέτο στο δίκτυο. Επιτρέπει στον κόμβο να

ανακαλύψει όλες τις δυνατές διαδρομές προς τον εξυπηρετητή-host. Το RPL σχεδιάστηκε για στατικά δίκτυα αισθητήρων, υπάρχουν όμως υλοποιήσεις που το τροποποιούν και το προσαρμόζουν για τα περιβάλλοντα των κινητών, το οποίο άνοιξε μια νέα περιοχή για έρευνα και ανάπτυξη.

- **6TiSCH**, που είναι ένα υπόστρωμα προσαρμογής και διαχείρισης, και διαθέτει το πρωτόκολλο 6top. Το IPv6 πρωτόκολλο πάνω σε TSCH λειτουργία του IEEE 802.15.4e παρέχει το μηχανισμό να εισάγουμε ή να ανακαλέσουμε ένα κόμβο από ένα TSCH δίκτυο, περιλαμβάνοντας τον σχεδιασμό των εικονικών καναλιών προς αυτό τον κόμβο, χρησιμοποιώντας τα διαθέσιμα κανάλια θυρίδων /συχνοτήτων, με γειτονικούς κόμβους. Επίσης κάνει τις ρυθμίσεις για να υποστηρίζεται το IETF πρωτόκολλο δρομολόγησης για μικρής κατανάλωσης ισχύος και με απώλειες δίκτυα (LLNs, RPL) πάνω σε 802.15.4e κόμβους.
- **Zigbee**, μια τεχνολογία ασύρματου δικτύου που είναι σχεδιασμένο για μικρού εύρους επικοινωνίες (10-20 μέτρα στην πράξη) με μικρή κατανάλωση ενέργειας, και χαμηλό ρυθμό μετάδοσης (40-250 kbps). Τα πλεονεκτήματα του είναι η μικρή κατανάλωση ενέργειας, το μικρό κόστος, η απλή δομή του, η αξιοπιστία, και η ασφάλεια (η οποία εξασφαλίζεται από συμμετρική κρυπτογράφηση με κλειδί 128 bits). Μπορεί να υποστηρίξει πολλές τοπολογίες δικτύου, όπως αστέρα, δένδρου και πλέγματος, και μπορεί να υποστηρίξει μέχρι 65000 τελικές συσκευές .
- **Z-Wave**, μια μικρού εύρους ασύρματη τεχνολογία δικτύου (30 μέτρα περίπου), με τα πλεονεκτήματα του μικρού κόστους, της μικρής κατανάλωσης ισχύος, χαμηλού ρυθμού μετάδοσης (9,6-100 kbps) και της μεγάλης αξιοπιστίας. Ο βασικός σκοπός αυτού είναι να προσφέρει αξιόπιστη μετάδοση ανάμεσα σε μια μονάδα ελέγχου και των τελικών συσκευών, οι οποίες δεν μπορούν να είναι περισσότερες από 232.
- **CoAP** (Constrained Application Protocol-πρωτόκολλο περιορισμένων εφαρμογών), το οποίο είναι ένα πρωτόκολλο μηνυμάτων που δρα στο στρώμα υπηρεσιών (service layer) επικεντρωμένο στο δίκτυο, οπότε μπορεί να θεωρηθεί ότι δρα στο στρώμα δικτύου, ανάμεσα σε μικρής υπολογιστικής ισχύος, μικρής δυνατότητας αποθήκευσης, και χαμηλής κατανάλωσης συσκευές, οπότε δεν μπορεί να χρησιμοποιηθεί το HTTP λόγω της πολυπλοκότητας του. Για να ξεπεραστεί αυτό το CoAP τροποποιεί ορισμένες λειτουργίες του για να προσαρμοστεί στις απαιτήσεις του IOT. Έτσι επιτρέπει σε αυτές τις συσκευές να

προσφέρουν υπηρεσίες σε άλλες συσκευές, δίνοντας τη δυνατότητα για αποδοτική χρήση των πόρων, η δε επικοινωνία μπορεί να γίνει ανάμεσα σε συσκευές του ιδίου δικτύου ή ανάμεσα σε συσκευές του δικτύου και κόμβων του διαδικτύου ή και ανάμεσα σε συσκευές που είναι σε διαφορετικά δίκτυα και ενώνονται μέσω διαδικτύου, συμμορφούμενο στο REST style, χρησιμοποιώντας το UDP πρωτόκολλο αντί του TCP, έχοντας ένα URI (Uniform Resource Identifier) για κάθε συσκευή (έχουμε αναφερθεί αναλυτικά παραπάνω για αυτό το πρωτόκολλο για LLNs.)

- **MQTT** (Message Queue Telemetry Transport), ένα 'ελαφρύ' πρωτόκολλο μηνυμάτων που 'τρέχει' σε TCP/IP πρωτόκολλο. Ακολουθεί ένα δημοσιεύω/εγγράφω hub-and-spoke παράδειγμα (ένα σύστημα διανομής στο οποίο τα προς διανομή αντικείμενα κατευθύνονται προς και από μια κεντρική θέση), όπου ένας μεσιτικός εξυπηρετητής (broker server) ασύγχρονα προωθεί μηνύματα σε έναν ή περισσότερους ενδιαφερόμενους κόμβους. Συγκεκριμένα θέματα/ενδιαφερόμενοι μοιράζονται πληροφορίες. Όλα τα μηνύματα που κατευθύνονται/δρομολογούνται προς ένα συγκεκριμένο θέμα (πχ. το σπίτι μου/ισόγειο/σαλόνι/θερμοκρασία) από εκδότες θα παραδοθεί σε ένα μεσίτη/διαμεσολαβητή. Συνδρομητές (όσοι συμμετέχουν) σε ένα συγκεκριμένο θέμα δέχονται πληροφορίες που εκδίδονται από ένα διαμεσολαβητή. Παρέχει ένα αγνωστικό δυαδικό ωφέλιμο φορτίο (binary payload). Οι κόμβοι πρέπει να είναι συνδεδεμένοι με τους διαμεσολαβητές.
- **AMQP** (Advanced Message Queuing Protocol), είναι ένα ανοιχτό πρότυπο πρωτόκολλου ουράς μηνυμάτων που χρησιμοποιείται για την παροχή μηνυμάτων, (αναμονή, δρομολόγηση, ασφάλεια και αξιοπιστία κ.λπ.), θεωρούμενο ως πρωτόκολλο μεσισμικού προσανατολισμένο στα μηνύματα, στο στρώμα εφαρμογής. Βασίζεται σε ένα παράδειγμα ουράς αναμονής μηνυμάτων ανάλογα με το είδος του θέματος, όπου προϊόντα γραμμένα για διαφορετικές πλατφόρμες και σε διαφορετικές γλώσσες μπορούν να ανταλλάσουν μηνύματα. Παρότι είναι ένα πρωτοτυποποιημένο πρωτόκολλο, δεν είναι όλες οι εφαρμογές πλήρως συμβατές με το πρότυπο. Το πλήρες AMQP πρότυπο απαρτίζεται από εκδότες , συνδρομητές και διαμεσολαβητές που έχουν εσωτερικές δυνατότητες δρομολόγησης. Η προδιαγραφή του AMQP (έκδοση 1.0) καθορίζει ένα ενσύρματο πρωτόκολλο για τις επικοινωνίες εκδοτών/συνδρομητών με τους διαμεσολαβητές μηνυμάτων. Ο διαμεσολαβητής μπορεί να τροποποιήσει τα

εισερχόμενα μηνύματα και βασιζόμενος σε ένα σύνολο κανόνων ή κριτηρίων, να αποφασίσει σε ποιες ουρές αναμονής τα μηνύματα πρέπει να προωθηθούν για να φτάσουν σε ένα ή περισσότερους συνδρομητές.

- **XMPP** (Extensible Messaging and Presence Protocol), είναι ένα πρωτόκολλο άμεσων μηνυμάτων (instant messaging protocol), ένα πρωτόκολλο για τη ροή στοιχείων XML (Extensible Markup Language) με σκοπό την ανταλλαγή δομημένων πληροφοριών σε σχεδόν πραγματικό χρόνο μεταξύ δυο οποιωνδήποτε τελικών σημείων (end point) δικτύου, και για την ασφαλή μετάδοση της ροής χρησιμοποιεί το πρωτόκολλο TLS. Μπορεί να χρησιμοποιηθεί στο IoT για να υποστηρίξει την επικοινωνία αντικειμένου με αντικείμενο με κείμενα βασισμένα στο XML πρότυπο.
- **DDS** (Data Distribution Service), το οποίο είναι ένα πρωτόκολλο δημοσίευσης-εγγραφής συνδρομής (publish-suscribe) για υποστήριξη υψηλής απόδοσης επικοινωνία συσκευής με συσκευή. Το DDS έχει ένα GDS (Global Data Space), παγκόσμιο χώρο δεδομένων, όπου οι κόμβοι μπορούν να δημοσιεύσουν-εγγράψουν δεδομένα χρησιμοποιώντας θέματα και κλειδιά. Τα αντικείμενα δεδομένων διαχειρίζονται με τη χρήση φυσικής γλώσσας. Υπάρχει επίσης υποστήριξη για συμβόλαια ποιότητας υπηρεσιών (QoS-Quality of Service). Το DDS παρέχει αυτόματο εντοπισμό εκδοτών/συνδρομητών χρησιμοποιώντας ένα πρωτόκολλο που ονομάζεται SDP-Simple Discovery Protocol, απλό πρωτόκολλο εντοπισμού.

Εκτός από τα πρωτόκολλα μεταφοράς, επικοινωνίας και μηνυμάτων και άλλα πρωτόκολλα μπορεί να έχουν σημαντικό ρόλο στο IoT. Όπως πρωτόκολλα για ονοματοδοσία (πχ. Multicast DNS, mDNS) των εφαρμογών του IoT. Επίσης το DNS Service Discovery (DNS-SD), μπορεί να χρησιμοποιηθεί από πελάτες (clients) για να βρίσκει τις επιθυμητές υπηρεσίες μέσω του mDNS. Όλα αυτά τα πρωτόκολλα μπορούν να ενσωματωθούν στο IoT, βελτιωμένα πρωτόκολλα, που προσφέρουν περισσότερη ασφάλεια, αξιοπιστία, και διαλειτουργικότητα, απαιτούνται για βοηθήσουν στη ανάπτυξη του IoT. Ένα ευρύτατα χρησιμοποιούμενο πρωτόκολλο, με πάρα πολλές υλοποιήσεις, το **Bluetooth**, χρησιμοποιείται και αυτό στις εφαρμογές του IoT για επικοινωνία. Η νεότερη έκδοση, Bluetooth Low Energy-BLE, που όπως αναφέρει και η ονομασία του, έχει σημαντικά λιγότερη κατανάλωση και κόστος, προσφέροντας παρόμοιο εύρος επικοινωνίας, αναμένεται να συνεισφέρει στη περαιτέρω χρήση και

ανάπτυξη του IoT. Φυσικά μπορούν να χρησιμοποιηθούν και τα γνωστά δίκτυα κινητής τηλεφωνίας 3G/4G για επικοινωνία στο IoT, όπου οι συσκευές του IoT που συνδέονται σε αυτά τα δίκτυα θα πρέπει να το κάνουν με ασφάλεια, έχοντας 'πάνω τους' αυτήν[34]. Αναφέρουμε επίσης το πλαίσιο αρχιτεκτονικής **GS1 EPDglobal**, που είναι μια συλλογή αλληλοσυνδεόμενων προτύπων για υλικό, λογισμικό, και διεπαφές δεδομένων, που είναι μια πρωτοβουλία της GS1 (GS1 link) για την ανάπτυξη βιομηχανικών προτύπων για το EPC (Electronic Product Code-ηλεκτρονικό κωδικό προϊόντος) για να υποστηρίξει τη χρήση ταυτοποίησης μέσω ραδιοσυχνοτήτων (RFID) στα εμπορικά δίκτυα που είναι πλούσια σε πληροφορίες. Ειδικότερα οι υπηρεσίες που αφορούν πληροφορίες για το EPC (EPCIS-EPC Information Services), είναι ένα πρότυπο του EPCglobal, σχεδιασμένο για να επιτρέψει το διαμοιρασμό των δεδομένων σχετικά με τον EPC, μέσα και ανάμεσα στις επιχειρήσεις. Με αυτόν τον τρόπο τουλάχιστον η κρυπτογράφηση των δεδομένων είναι αναγκαία, όταν μετακινούνται δεδομένα μεταξύ διαφορετικών εταιρειών, αφού χρησιμοποιούνται κοινοί σύνδεσμοι του διαδικτύου.

Στο **στρώμα υπηρεσιών** θα πρέπει να περιλαμβάνονται οι ακόλουθες υπηρεσίες-τεχνολογίες [32]:

- **Διεπαφή** (Interface), θα πρέπει να εξασφαλίζει την ασφαλή και αποδοτική ανταλλαγή της πληροφορίας ανάμεσα στις συσκευές και τις εφαρμογές. Επίσης πρέπει να διαχειρίζεται τις διασυνδεδεμένες συσκευές, περιλαμβάνοντας τη σύνδεση, την αποσύνδεση, την επικοινωνία, και την λειτουργία των συσκευών. Αν και έχουν αναπτυχθεί κάποιες υπηρεσίες-τεχνολογίες διεπαφής (πχ. SIA-SOCRADES INTEGRATION ARCHITECTURE) για το IoT, η χρησιμοποίηση περισσότερο αποτελεσματικών, ασφαλών, και επεκτεινόμενων διεπαφών με λιγότερο κόστος είναι μια πρόκληση για τη μελλοντική έρευνα για την υποστήριξη του IoT.
- **Υπηρεσία διαχείρισης** (Service Management), η οποία πρέπει αποτελεσματικά να ανακαλύπτει τις συσκευές και τις εφαρμογές, και να σχεδιάζει αποτελεσματικές και ασφαλείς υπηρεσίες που να ικανοποιούν τις απαιτήσεις. Αποκρύπτοντας τις λεπτομέρειες της υλοποίησης, αυτές οι υπηρεσίες μπορούν να υλοποιηθούν συμβατά σε ετερογενείς συσκευές και εφαρμογές, η SoA χρησιμοποιείται για να ενσωματώσει αυτές τις υπηρεσίες. Για παράδειγμα η OSGi πλατφόρμα, θεμελιωμένη με μια δυναμική αρχιτεκτονική SoA, είναι μια αποτελεσματική αρθρωτή πλατφόρμα που αναπτύσσει υπηρεσίες.

- **Μεσισμικό** (Middleware), είναι μια προγραμματιστική υπηρεσία ή λογισμικό που παρεμβάλλεται ανάμεσα στις IoT τεχνολογίες και στις εφαρμογές, κρύβοντας τις λεπτομέρειες των διαφορετικών τεχνολογιών, επικεντρωνόμενο στην ανάπτυξη των εφαρμογών, χωρίς να ασχολείται με τη συμβατότητα ανάμεσα στις εφαρμογές και την υποδομή. Έτσι χρησιμοποιώντας middleware, οι συσκευές και οι εφαρμογές με διαφορετικές διεπαφές, μπορούν να ανταλλάξουν πληροφορίες και να μοιραστούν τους υπάρχοντες πόρους. Το μεσισμικό μπορεί να αφορά την ανταλλαγή μηνυμάτων, την επικοινωνία κλπ. Για να ενσωματωθεί το μεσισμικό στο IoT θα πρέπει να ανταποκρίνεται στη διαλειτουργικότητα δηλαδή να συνδράμει στη διασύνδεση ετερογενών συσκευών στην επικοινωνία και στην ανταλλαγή πληροφοριών.
- **Διαχείριση πόρων και διαμοιρασμός** (Resource Management and Sharing), ποικίλα και ετερογενή δίκτυα ενσωματώνονται για την μεταφορά των δεδομένων Για μείωση του κόστους θα πρέπει να έχουμε διαμοιρασμό των πόρων του δικτύου από διάφορες εφαρμογές για να αυξηθεί η χρησιμοποίηση τους. Αυτή τη στιγμή ο διαμοιρασμός γίνεται ως προς το συχνοτικό φάσμα, ενώ θα μπορούσε να γινόταν και ως προς το χρόνο και το χώρο. Στο IoT τα περισσότερα υπάρχοντα σχήματα έχουν αναπτυχθεί για επικοινωνία μηχανής με μηχανή ή συσκευής με συσκευή, τώρα όμως θα πρέπει να εξελιχθεί σε επικοινωνία πράγματος με πράγμα. Επίσης θα πρέπει να έχουμε οικονομία ενέργειας στο επίπεδο της συλλογής δεδομένων (RFID, αισθητήρες). Κάποιες προσπάθειες έχουν γίνει για τη μείωση της κατανάλωσης με εναλλαγή καταστάσεων ύπνωσης και λειτουργίας σε δίκτυο αισθητήρων, ανάλογα με τον κύκλο λειτουργίας αυτών. Επίσης πρωτόκολλα δρομολόγησης που βασίζονται στην εξισορρόπηση κατανάλωσης ενέργειας για να αυξήσουν τη διάρκεια ζωής των δικτύων αισθητήρων. Στο επίπεδο αυτό υπάρχουν πολλά θέματα προς επίλυση και για μελλοντική έρευνα.

5.2 Ασφάλεια, Επιθέσεις και Αντίμετρα στο IoT

Έχοντας αναφερθεί σε θέματα ασφάλειας θα τα δούμε προσαρμοσμένα για το IoT, σε κάθε ένα από τα στρώματα της SoA, τα οποία είναι ίδια με τα της ασφάλειας των τριών στρωμάτων [32]. Στο στρώμα υπηρεσιών τα θέματα ασφάλειας, επειδή βασίζεται σε υπηρεσίες δεδομένων του στρώματος δικτύου και του στρώματος εφαρμογής, είναι ίδια με τα θέματα ασφάλειας αυτών των στρωμάτων.

Στο **στρώμα αντίληψης** οι προκλήσεις είναι η παραποίηση των συλλεγόμενων δεδομένων και η καταστροφή των συσκευών συλλογής δεδομένων.

- **Επιθέσεις κατάληψης κόμβων** (Node Capture Attacks), σε αυτή την κατηγορία επιθέσεων, ο αντίπαλος μπορεί να καταλάβει και να ελέγχει τον κόμβο ή τη συσκευή ή αντικαθιστώντας ολόκληρο τον κόμβο ή συσκευή ή να παραποιήσει το υλικό αυτών. Επίσης μπορεί να αντιγράψει τα χαρακτηριστικά ενός κόμβου, αυτός ο ψεύτικος κόμβος να συνδεθεί στο δίκτυο, και να αποστέλλει παραποιημένα δεδομένα (επίθεση αντιγραφής, replication attack). Η παρακολούθηση των κόμβων και η ανίχνευση των κακόβουλων κόμβων είναι ένα θέμα. Λύση μπορούμε να έχουμε πχ. με χρήση προμοιρασμένων κλειδιών [35].
- **Επιθέσεις έγχυσης κακόβουλου κώδικα** (Malicious code Injection Attacks), ο έλεγχος του κόμβου μπορεί να γίνει και με έγχυση κακόβουλου κώδικα. Η άμυνα κατά αυτών των επιθέσεων μπορεί να γίνει με συστήματα αυθεντικοποίησης, τα οποία θα πρέπει να προσαρμοστούν στο IoT, δηλαδή με χρήση κρυπτογραφίας ενσωματωμένης στο χαμηλό αυτό επίπεδο[36].
- **Επιθέσεις έγχυσης ψευδών δεδομένων** (False Data Injection Attacks), σε αυτή την περίπτωση ο επιτιθέμενος μπορεί να στείλει τα ψευδή δεδομένα στη θέση των πραγματικών με αποτέλεσμα να έχουμε αντίδραση του συστήματος σε αυτά τα ψευδή δεδομένα, με αποτέλεσμα πχ. τη πρόκληση ψευδούς συναγερμού ή την αποφυγή αυτού. Τεχνικές φιλτραρίσματος των ψευδών δεδομένων που να ανιχνεύουν και να απορρίπτουν αυτά πρέπει να σχεδιαστούν και για το IoT. Επίσης με τεχνικές κρυπτογράφησης των πακέτων που αποστέλλονται δεν θα είναι δυνατή η αποστολή των ψευδών δεδομένων.
- **Επιθέσεις επανάληψης** (Replay Attacks), ο επιτιθέμενος μπορεί να χρησιμοποιήσει ένα κακόβουλο κόμβο ή συσκευή για να αποστείλει στο κεντρικό σύστημα συλλογής δεδομένων πληροφορίες με νόμιμα χαρακτηριστικά ταυτότητας, οι οποίες θεωρούνται γνήσιες. Για να μετριαστούν τα αποτελέσματα αυτών των επιθέσεων συστήματα ασφαλούς χρονοσήμανσης πρέπει να αναπτυχθούν.
- **Επιθέσεις κρυπτανάλυσης και επιθέσεις παράπλευρου καναλιού** (Cryptanalysis Attacks and Side Channel Attacks). Έχουμε ήδη αναφερθεί και στους δυο τύπους επίθεσης, στο 2.2.2 της παρούσας. Για να αποφύγουμε αυτά

τα είδη επιθέσεων θα πρέπει οι αλγόριθμοι κρυπτογράφησης θα πρέπει να είναι αποδοτικοί και ασφαλείς, όπως και το σύστημα διαχείρισης κλειδιών.

- **Επιθέσεις παρακολούθησης και παρεμβολής** (Eavesdropping and Interference Attacks). Στο σύνολο του οι συσκευές του IoT επικοινωνούν με ασύρματα δίκτυα οπότε μη εξουσιοδοτημένοι χρήστες μπορούν να παρακολουθήσουν τις επικοινωνίες. Για την αποφυγή της παρακολούθησης χρειάζεται χρήση ασφαλών αλγόριθμων κρυπτογράφησης και συστήματος διαχείρισης κλειδιών. Για την αποφυγή των παρεμβολών απαιτούνται συστήματα φίλτρων που αποκόπτουν τις παρεμβολές.
- **Επιθέσεις στέρησης κατάστασης αναμονής** (Sleep Deprivation Attacks). Για εξοικονόμηση ενέργειας οι συσκευές ή οι κόμβοι, είναι προγραμματισμένα να ακολουθούν ένα πρόγραμμα που τα θέτει σε κατάσταση αναμονής, επειδή στο σύνολο τους αυτές οι συσκευές έχουν περιορισμένα αποθέματα ισχύος. Μια λύση είναι οι συσκευές αυτές να είναι αυτοτροφοδοτούμενες (πχ ηλιακή ενέργεια, όπου είναι δυνατό.) Επίσης ασφαλείς κύκλοι λειτουργίας αυτών των συσκευών θα πρέπει να αναπτυχθούν για το IoT.

Στο **στρώμα δικτύου**, στο σύνολο του οποίου χρησιμοποιούνται ασύρματες επικοινωνίες, θα δούμε τους κινδύνους που σχετίζονται με το ασύρματο δίκτυο [32].

- **Επιθέσεις άρνησης εξυπηρέτησης** (Denial of Service Attacks, DoS), που προκαλούνται από μαζική αποστολή άσχετων δεδομένων στο δίκτυο του IoT εξαντλώντας τους πόρους, καθιστώντας τις υπηρεσίες δικτύου μη διαθέσιμες. Αποτέλεσμα αυτής της συνεχούς αποστολής από πολλούς κόμβους είναι να έχουμε άρνηση εξυπηρέτησης (DoS) λόγω της πληθώρας των δεδομένων (UDP flood, Syn Flood, και άλλες που προκαλούν άρνηση εξυπηρέτησης). Για προστασία θα πρέπει να μελετηθούν οι τρόποι επίθεσης και μετά να αναπτυχθούν συστήματα για μείωση των επιθέσεων όπως το πρωτόκολλο RAEED [37].
- **Επιθέσεις παραπλάνησης** (Spoofing Attacks), όπου ο επιτιθέμενος έχει την έγκυρη διεύθυνση IP μιας εξουσιοδοτημένης συσκευής ή τις πληροφορίες μιας έγκυρης ετικέτας RFID, και αποστέλλει από αυτές, κακόβουλα δεδομένα κάνοντας τα να φαίνονται ως έγκυρα στο IoT σύστημα. Ένα μοντέλο ασφαλούς διαχείρισης, η ταυτοποίηση και η αυθεντικοποίηση, είναι λύσεις για προστασία ενάντια σε αυτές τις επιθέσεις.

- **Επιθέσεις καταβόθρας** (Sinkhole Attacks), στην οποία ο προσβεβλημένος κόμβος ή συσκευή δηλώνει ότι διαθέτει παραπάνω ικανότητες ισχύος (ενέργειας), υπολογιστικής ισχύος και επικοινωνίας από τους γειτονικούς κόμβους ή συσκευές ώστε οι περισσότεροι γειτονικοί κόμβοι ή συσκευές να επιλέξουν αυτόν τον κόμβο ή συσκευή λόγω των δηλωθέντων ιδιοτήτων. Έτσι ο επιτιθέμενος μπορεί να ελέγξει τη διακίνηση δεδομένων και τα δεδομένα. Για να αποτρέψουμε αυτού του είδους τις επιθέσεις μπορούμε να χρησιμοποιήσουμε κρυπτογραφημένα πρωτόκολλα δρομολόγησης, όπως τα RESIST-0 και RESIST-1 [38].
- **Επιθέσεις σκουληκότρυπας** (Wormhole Attacks), όπου δυο προσβεβλημένοι απομακρυσμένοι κόμβοι ή συσκευές θεωρούν ότι είναι γειτονικοί. Επειδή τα άλματα προώθησης μειώνονται, περισσότερα δεδομένα προωθούνται σε αυτούς τους κόμβους ή συσκευές. Οπότε έχουμε το ίδιο αποτέλεσμα με την επίθεση καταβόθρας. Για να αντιμετωπίσουμε αυτή την κατηγορία επίθεσης, μπορούμε να χρησιμοποιήσουμε πρωτόκολλα δρομολόγησης που ενισχύουν την ασφάλεια στην διαδικασία επιλογής της διαδρομής. Άλλος τρόπος είναι να αναπτύξουμε ασφαλές υλικό με χρήση συστημάτων γεωεντοπισμού, ή με κατευθυντικές κεραίες.
- **Επιθέσεις ενδιάμεσου** (Man in the Middle Attacks), όπου μια κακόβουλη συσκευή που ελέγχεται από τον εισβολέα παρεμβάλλεται εικονικά ανάμεσα σε δυο συσκευές που επικοινωνούν στο IoT. Υποκλέπτοντας τις πληροφορίες ταυτοποίησης των δυο κανονικών συσκευών η κακόβουλη συσκευή μπορεί αποθηκεύει ή να προωθεί ή και να αλλάζει τα δεδομένα που ανταλλάσσονται ανάμεσα στις δυο συσκευές, χωρίς αυτές να μπορούν να ανιχνεύσουν την ύπαρξη της, πιστεύοντας ότι επικοινωνούν άμεσα μεταξύ τους. Αποτέλεσμα αυτής είναι η παραβίαση της εμπιστευτικότητας, και της ακεραιότητας των δεδομένων που διακινούνται ανάμεσα στους δυο κόμβους. Δεν είναι απαραίτητη η φυσική παραβίαση των συσκευών, μπορεί να γίνει βασιζόμενη στα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στα δίκτυα του IoT. Η χρήση ασφαλών πρωτόκολλων επικοινωνίας, και συστημάτων διαχείρισης κλειδιών, που να εξασφαλίζουν ότι αυτές οι πληροφορίες δεν θα διαρρεύσουν στον επιτιθέμενο είναι μια αποτελεσματική μέθοδος για την αντιμετώπιση αυτή της επίθεσης. Έτσι μπορούμε να αποφύγουμε και τις επιθέσεις bit-flipping.

- **Επιθέσεις πληροφοριών δρομολόγησης** (Routing Information Attacks), είναι επίθεση κατά των πρωτοκόλλων δρομολόγησης των IoT συστημάτων, όπου οι πληροφορίες δρομολόγησης παραποιούνται από τον επιτιθέμενο ώστε να δημιουργούνται βρόγχοι στη μετάδοση των δεδομένων, με αποτέλεσμα την επιμήκυνση των διαδρομών και την αύξηση των καθυστερήσεων από το ένα άκρο στο άλλο του δικτύου IoT. Για αμυνθούμε ενάντια σε αυτές τις επιθέσεις μπορούμε να χρησιμοποιούμε ασφαλή πρωτόκολλα δρομολόγησης (είναι αυτά που εγγυώνται ότι η υπηρεσία δρομολόγησης λειτουργεί σωστά, παραδίδει πακέτα ανάμεσα στην πηγή και ένα ή πολλαπλούς προορισμούς, χωρίς να αλλοιώνονται, καθυστερούν, ή να χάνονται από ενδιάμεσους κόμβους προώθησης, και αυτό γίνεται με χρήση κρυπτογραφικών μηχανισμών, όπως MACs και ψηφιακών υπογραφών ώστε να εξασφαλίζουν την αυθεντικοποίηση και ακεραιότητα των μηνυμάτων που ανταλλάσσονται ανάμεσα στους κόμβους [39], και έμπιστη διαχείριση ώστε να έχουμε ασφαλείς συνδέσμους ανάμεσα στις συσκευές και οι πληροφορίες ταυτοποίησης και οι διευθύνσεις IP δεν θα διαρρεύσουν στον επιτιθέμενο.
- **Σιβυλλικές επιθέσεις** (Sybil Attacks), σε αυτές μια κακόβουλη συσκευή, που ονομάζεται σιβυλλική συσκευή, εμφανίζει αρκετές έγκυρες ταυτότητες, τις οποίες οικειοποιείται στο IoT σύστημα, οπότε στο σύστημα εμφανίζεται σαν ένας μεγάλος αριθμός από συσκευές, ενώ στην πραγματικότητα είναι μόνο μία. Αποτέλεσμα είναι να μπορεί να στείλει αυτή η συσκευή λανθασμένα δεδομένα, τα οποία αποδέχονται οι κανονικές συσκευές, ενώ οι δρομολογήσεις που γίνονται μέσω της σιβυλλικής συσκευής σαν κόμβοι προώθησης ενώ φαίνονται σαν πολλές διαδρομές στην πραγματικότητα είναι μόνο μια και μάλιστα μέσω της σιβυλλικής συσκευής, στην οποία μπορεί να έχουμε συμφόρηση του δικτύου ή άρνηση εξυπηρέτησης. Η ανάπτυξη ασφαλών μηχανισμών ταυτοποίησης και αυθεντικοποίησης είναι η λύση για τα συστήματα του IOT.
- **Μη εξουσιοδοτημένη πρόσβαση** (Unauthorized Access), ένας μεγάλος αριθμός από RFID συσκευές ενσωματώνονται στο IoT και οι περισσότερες RFID ετικέτες δεν έχουν ικανοποιητικούς μηχανισμούς αυθεντικοποίησης, οπότε οι πληροφορίες που υπάρχουν σε αυτές μπορούν να ανακτηθούν, να τροποποιηθούν ή και να διαγραφούν. Επομένως πρέπει να αναπτυχθούν μηχανισμοί αυθεντικοποίησης, με χρήση αλγορίθμων κρυπτογράφησης που

καταναλώνουν λίγη ισχύ, των συσκευών που βασίζονται στην τεχνολογία RFID για το IoT.

Στο **στρώμα εφαρμογών**, οι επιθέσεις αφορούν το λογισμικό που υλοποιεί τις απαιτήσεις των χρηστών. Οι τρόποι αντιμετώπισης είναι αυτοί που ισχύουν για οποιοδήποτε λογισμικό, πχ. αυθεντικοποίηση, ταυτοποίηση, τείχη ασφαλείας αντιικά προγράμματα, επαγρύπνηση του χρήστη για αποφυγή παραπλάνησης, η οποία επαγρύπνηση μπορεί να προέρχεται από την εφαρμογή ορισμένων πολιτικών ασφάλειας.

Υπάρχουν και άλλες προτάσεις για αρχιτεκτονικές, εκτός από τις δυο που έχουμε ήδη αναφέρει, όπως αυτή των πέντε στρωμάτων, η οποία έχει ένα επιπλέον στρώμα πάνω από το στρώμα εφαρμογών, το επιχειρηματικό στρώμα (Business Layer) [40]. Βασίζονται όμως στις αρχιτεκτονικές που έχουμε αναφέρει.

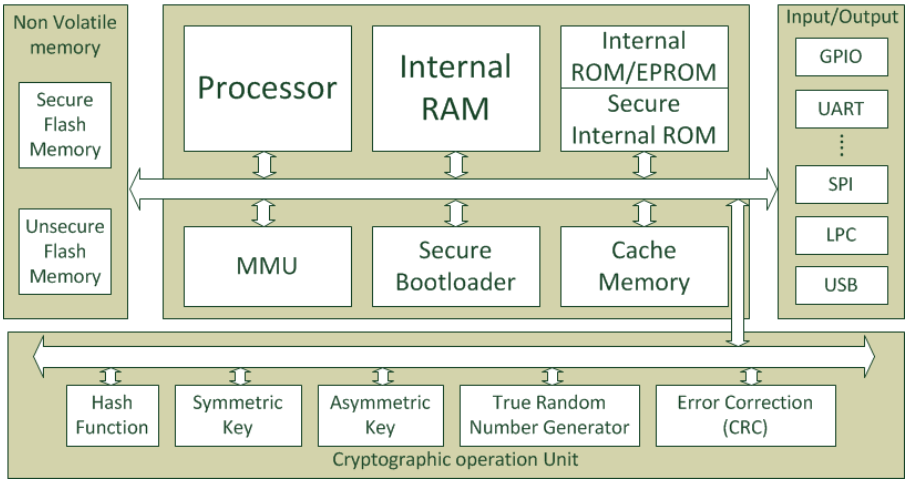
Κεφάλαιο 6
Σχεδιασμοί, Υλοποιήσεις, Υπολογιστικές Πλατφόρμες, Χαρακτηριστικά Απόδοσης

Θα δούμε μερικούς σχεδιασμούς και υλοποιήσεις συστημάτων, που είναι επικεντρωμένα στην ασφάλεια.

6.1 Σχεδιασμός Ασφαλούς Ενσωματωμένου Συστήματος

Λόγω της μεγάλης αύξησης φορητών και κινητών συστημάτων, της αυξανόμενης ενσωμάτωσης της υπολογιστικής λογικής σε ποικίλες συσκευές, και του πλήθους των έξυπνων συσκευών που περιέχουν ενσωματωμένους επεξεργαστές, οι οποίες συλλέγουν επεξεργάζονται και αποστέλλουν πληροφορίες, κάποιες από τις οποίες μπορεί να είναι ευαίσθητες ή και εμπιστευτικές, δημιουργείται η ανάγκη της ύπαρξης ασφάλειας για προστασία αυτών των πληροφοριών που πρέπει να πραγματοποιείται μέσα στα ενσωματωμένα συστήματα. Στο κόσμο της πληροφορικής τεχνολογίας αυτό λύνεται με χρήση κρυπτογραφίας της οποίας οι υλοποιήσεις πρέπει να ενσωματώνονται στα συστήματα και όχι από ανεξάρτητες δομές ώστε να είναι δυσκολότερο να παρακαμφτεί αλλά και να υπάρχει μικρότερη κατανάλωση ενέργειας (πολλές συσκευές έχουν περιορισμένους πόρους ενέργειας). Η ασφάλεια μπορεί να επιτευχθεί μέσα από Ασφαλείς Μονάδες Υλικού, Hardware Security Modules (HMS), που υλοποιούν ένα πλήθος πρωτόκολλων και αλγόριθμων ασφάλειας, και βρίσκονται σε ένα πλήθος από συσκευές περιλαμβανομένων και των ενσωματωμένων συστημάτων (embedded systems), όπως έξυπνες κάρτες, αυτοκίνηση, έξυπνο περιβάλλον κλπ. Θα

δούμε το σχεδιασμό ώστε συμμετρική, ασύμμετρη κρυπτογραφία και συναρτήσεις κατακερματισμού, να χρησιμοποιούνται για να παρέχουν ασφάλεια στους χρήστες αυτών των ενσωματωμένων συστημάτων. Για να χειριστούμε τις απαιτήσεις ασφάλειας αλλά και αυτές των ενσωματωμένων συστημάτων (μικρή υπολογιστική ισχύς επεξεργαστών, μικρή παροχή ενέργειας-μπαταρίες, προσαρμογή σε πολλά περιβάλλοντα, αντοχή έναντι των επιθέσεων και το θέμα του κόστους) θα πρέπει η δομή ασφάλειας να ενσωματωθεί στο σύστημα μαζί με οποιαδήποτε άλλη λειτουργικότητα απαιτείται να προσφέρει αυτό. Επειδή οι ενσωματωμένοι επεξεργαστές δεν έχουν αρκετή ισχύ για να υποστηρίξουν την απαιτούμενη ασφάλεια που χρειάζεται από τα πρωτόκολλα ασφάλειας, το φόρτο των κρυπτογραφικών λειτουργιών πρέπει να το κάνουν ειδικά σχεδιασμένες μονάδες Η κρυπτογραφική μηχανική αυτό ακριβώς πετυχαίνει σχεδιάζοντας κρυπτογραφικές συναρτήσεις με ένα ασφαλή αλλά και αποδοτικό τρόπο ώστε να ταιριάζει τις λειτουργικές και τις μη λειτουργικές απαιτήσεις λαμβάνοντας υπ' όψη το υλικό, την απόδοση του λογισμικού, την αντίσταση στις επιθέσεις (όχι μόνο του στον κρυπταλγόριθμο αλλά και στην υλοποίηση) και το πώς το όλο αποτέλεσμα θα ταιριάξει στο σύστημα. Οι αρχές της κρυπτογραφικής μηχανικής είναι πολύ χρήσιμες όταν προσθέτουν χαρακτηριστικά ασφάλειας και τις σχετιζόμενες δομές υλικού σε ένα ενσωματωμένο σύστημα, όπου οι περιορισμοί είναι αυστηροί και το περιβάλλον λειτουργίας μπορεί να είναι εχθρικό. Βλέπουμε στην Εικόνα 1 ένα γενικό σχεδιασμό ενός ασφαλούς ενσωματωμένου συστήματος.



Εικόνα 1. Αρχιτεκτονική ασφαλούς ενσωματωμένου συστήματος.
Πηγή : Η εργασία που υπάρχει στην αναφορά [24].

Το σύστημα αυτό έχει κλασικά επεξεργαστή, RAM, ROM για την υποστήριξη του λογισμικού. Επιπλέον έχει μια εσωτερική ασφαλή περιοχή μνήμης που προστατεύεται απόλυτα από επιθέσεις υλικού και είναι προστατευμένη από αλλοιώσεις, ώστε η φυσική πρόσβαση από ένα επιτιθέμενο να είναι αδύνατη, Πρόσθετη ασφάλεια επιτυγχάνεται διατηρώντας τα δεδομένα της σε κρυπτογραφημένη μορφή. Το λειτουργικό και το σχετικό λογισμικό μπορούν επίσης να προστατεύονται από ένα φορτωτή εκκίνησης (bootloader), που εκτελείται κατά την εκκίνηση του συστήματος και εγγυάται ότι το ενσωματωμένο λειτουργικό και σχετικό σταθερισμικό (firmware) είναι γνήσια και αναλλοίωτα όταν φορτώνονται κατά την εκκίνηση. Ο ασφαλής bootloader χρησιμοποιεί την ασφαλή εσωτερική μνήμη για να ανακτήσει μυστικές πληροφορίες, όπως το δημόσιο και το ιδιωτικό κλειδί. Μπορεί να περιλαμβάνει και μια μνήμη που δεν χρειάζεται συνεχή παροχή για λειτουργία (Non-Volatile Memory-NVRAM), ανάλογα με τις εφαρμογές, που επίσης έχει ασφαλή και μη ασφαλή περιοχή.

Το σημείο που μας ενδιαφέρει από πλευράς ασφάλειας είναι η μονάδα κρυπτογραφικής επεξεργασίας (Cryptographic operation unit), που κάνει όλες τις κρυπτογραφικές λειτουργίες των κρυπτογραφικών πρωτοκόλλων του ενσωματωμένου συστήματος, και όχι ο κύριος επεξεργαστής που συνήθως έχει μικρές δυνατότητες. Ο σχεδιασμός αυτής της μονάδας πρέπει να είναι με τέτοιο τρόπο ώστε να μην αυξάνει πολύ την κατανάλωση και την επιφάνεια του συστήματος για να είναι ανταγωνιστικό και ασφαλές. Κάθε κρυπτογραφική λειτουργία γίνεται σε συγκεκριμένη μονάδα υλικού, και όλες αυτές οι μονάδες συνδέονται μέσω διεπαφής κοινού διαύλου (common bus interface), στον κύριο δίαυλο του συστήματος και ελέγχεται από τον επεξεργαστή. Όπως κάθε σύστημα, έτσι και αυτά έχουν θέματα ασφάλειας. Οι κρυπτογραφικές μονάδες συμμετρικών και ασύμμετρων αλγόριθμων έχουν σχεδιαστεί ώστε να προσφέρουν βελτιστοποιημένη απόδοση. Μπορεί το σύστημα να προσφέρει καλή προστασία έναντι κρυπταναλυτικών επιθέσεων, αλλά φυσικές επιθέσεις στο υλικό μπορεί να δημιουργήσουν διάφορα προβλήματα. Αυτές οι επιθέσεις στο υλικό μπορούν να κατηγοριοποιηθούν σε τρεις τύπους [24].

- **Επιθέσεις εισβολής** (Invasive Attacks), όπου διακόπτουν τη σωστή λειτουργία του ολοκληρωμένου σε επίπεδο υλικού, έχοντας παρακάμψει το περίβλημα και παρακολουθώντας ή και παραβιάζοντας τις λειτουργίες του κάνοντας το να εκτελεί τροποποιημένο κώδικα ή αλλάζοντας τις τιμές των καταχωρητών. Για να

γίνει αυτό απαιτείται εξειδικευμένος εξοπλισμός και υψηλό επίπεδο εξειδικευμένης γνώσης, πράγμα όχι τόσο εύκολο.

- **Επιθέσεις ημι-εισβολής** (Semi invasive attacks), και εδώ απαιτείται πρόσβαση στην επιφάνεια του ολοκληρωμένου, αλλά όχι δημιουργία επαφών με τις εσωτερικές γραμμές του ολοκληρωμένου. Σκοπός είναι να προκληθεί σφάλμα στη υπολογιστική ροή κατά την κρυπτογραφική λειτουργία και να παρατηρηθεί το κρυπτογραφικό αποτέλεσμα, καθώς το σφάλμα διαδίδεται. Και εδώ απαιτείται μεγάλη εξειδίκευση.
- **Επιθέσεις μη-εισβολής** (Non-invasive attacks), γνωστές και σαν επιθέσεις παράπλευρου καναλιού, στις οποίες έχουμε αναφερθεί παραπάνω.

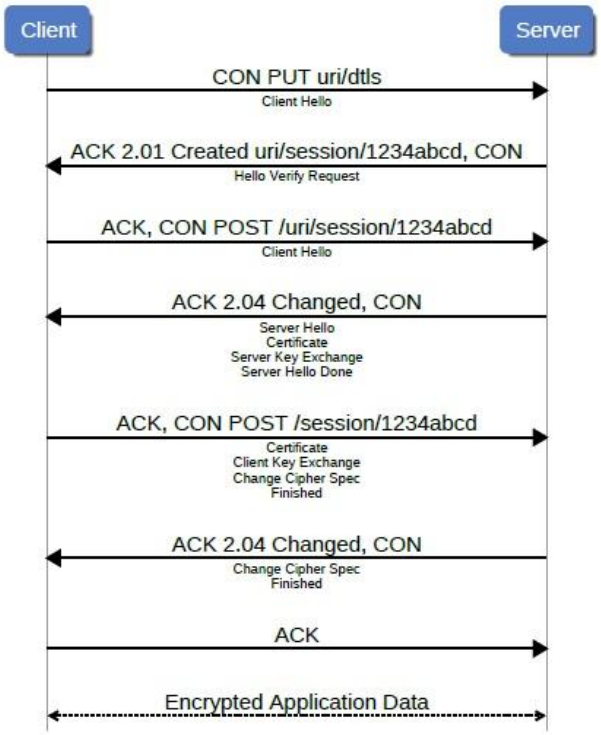
Για να αντιμετωπίσουμε τις επιθέσεις στο υλικό, πράγμα όχι τόσο εύκολο γιατί κάθε αλγόριθμος έχει τη δική του υλοποίηση σε υλικό άρα και τις δικές του ευπάθειες, έχουμε δυο γενικές προσεγγίσεις. Αντίμετρα που αφορούν τον αλγόριθμο, και αντίμετρα που αφορούν το ηλεκτρονικό κύκλωμα. Στα πρώτα, τροποποιείται ο κρυπτογραφικός αλγόριθμος και οι σχετικές αλγεβρικές υπολογιστικές λειτουργίες ώστε όταν υλοποιούνται σε υλικό, οι σχετιζόμενες πληροφορίες που διαρρέουν να μη μπορούν να χρησιμοποιηθούν από τον επιτιθέμενο, και αφορούν κυρίως τις επιθέσεις ημι-εισβολής και μη-εισβολής. Στα δεύτερα, κατά τη φάση της υλοποίησης ή του 'πακεταρίσματος' του ολοκληρωμένου κρυπτογράφησης, προστίθενται ολοκληρωμένα που μπορούν να ανιχνεύσουν ή και να αποτρέψουν μια επίθεση υλικού ή και μια παραβίαση του ολοκληρωμένου, και αφορούν όλα τα είδη επιθέσεων υλικού. Για τις επιθέσεις παράπλευρου καναλιού τα αντίμετρα εξαρτώνται από το είδος της επίθεσης. Λέγοντας περισσότερα από το 5.2 της παρούσας μεταπτυχιακής διατριβής, σκοπός των αντίμετρων είναι να υλοποιήσουν την κρυπτογραφική αρχιτεκτονική με τέτοιο τρόπο ώστε η κατανάλωση ενέργειας, ο χρόνος λειτουργίας και η εκπομπή ηλεκτρομαγνητικής ακτινοβολίας να αφήνουν να διαρρεύσει όσο το δυνατό λιγότερη πληροφορία για το κλειδί ή τα δεδομένα. Αυτό επιτυγχάνεται με δύο τρόπους, είτε μπερδεύοντας-ανακατεύοντας το σήμα που διαρρέει ώστε να μη σχετίζεται με τη κρυφή πληροφορία που υπολογίζεται στην κρυπτογραφική μονάδα, είτε περιορίζοντας τη διαρροή στο σύνολο της, ώστε να είναι πολύ δύσκολο για τον επιτιθέμενο να τη χρησιμοποιήσει για επίθεση. Η πρώτη προσέγγιση σχετίζεται με τα κρυπτογραφικά αντίμετρα που στοχεύουν στην εισαγωγή τυχαιότητας στη υπολογιστική ροή των αλγόριθμων κρυπτογράφησης, παρέχοντας κάλυψη των κρυφών πληροφοριών, είτε Boolean είτε

αριθμητική, η οποία γίνεται με πολλαπλασιασμό ή πρόσθεση τυχαίου αριθμού. Αυτά τα αντίμετρα, που είναι γνωστά σαν τύφλωση του κρυπταναλυτή, είναι πολύ χρήσιμα για την αντιμετώπιση των διαφορικών επιθέσεων καθώς στοχεύουν στην αποσυσχέτιση των κρυφών δεδομένων με την ίδια τη διαρροή ηλεκτρομαγνητικής ακτινοβολίας κλπ. Η δεύτερη προσέγγιση έχει σχέση κυρίως με τον τρόπο υλοποίησης του κυκλώματος που εκτελείται ο κρυπταλγόριθμος. Με χρήση ειδικών κυκλωμάτων γίνεται προσπάθεια να κανονικοποιηθούν τα σήματα που διαρρέουν στο περιβάλλον, ώστε να παραμένουν αναλλοίωτα κατά τη διάρκεια των κρυπτογραφικών λειτουργιών. Φυσικά η προστασία έναντι αυτών των επιθέσεων, αλλά και γενικότερα, δεν δύναται να είναι απόλυτη. Σκοπός είναι η υλοποίηση των κυκλωμάτων να γίνεται με τόσα αντίμετρα ώστε η επίθεση στο σύστημα να είναι πολύ ακριβή σε προσπάθεια ή κόστος, οπότε να μη ενδιαφέρει τους επιτιθέμενους.
Η παραπάνω ενότητα βασίζεται στην εργασία που υπάρχει στην αναφορά [24].

6.2 Υλοποίηση DTLS στο CoAP

Μια άλλη υλοποίηση είναι αυτή του DTLS (η έκδοση του γνωστού TLS, που έχουμε περιγράψει παραπάνω, με χρήση του UDP πρωτόκολλου) πάνω στο CoAP πρωτόκολλο
Εδώ εκμεταλλεύεται η δυνατότητα του CoAP να παρέχει επικοινωνία προσανατολισμένη στις συνδέσεις που προσφέρει το στρώμα μηνυμάτων για να ελαχιστοποιηθεί το μέγεθος του κώδικα και η ποσότητα των μηνυμάτων που ανταλλάσσονται με αποτέλεσμα ένα βελτιστοποιημένο πρωτόκολλο χειραψίας, εφαρμόσιμο σε συσκευές περιορισμένων δυνατοτήτων. Πιο συγκεκριμένα ένα επιβεβαιώσημο (CON) μήνυμα απαιτεί ένα αναγνωριστικό (ACK) μήνυμα σαν απάντηση, επιτρέποντας μια αξιόπιστη μετάδοση. Επί πλέον ο κατακερματισμός μπορεί να γίνει βασιζόμενος στο χαρακτηριστικό της μεταφοράς κατά τμήματα που ορίστηκε από το CoAP για να υποστηρίζει μεταφορά πολλών δεδομένων. Ο συνδυασμός και των δύο μηχανισμών επιτρέπει να εγγυηθούμε την συμβατότητα της λύσης με το πρότυπο, καθιστώντας της ‘ελαφρύτερη. Αναπτύχθηκε με RESTful DTLS σύνδεση σαν ένας πόρος CoAP, ο οποίος δημιουργείται όταν μια νέα ασφαλής σύνοδος ζητείται. Αυτό επιτρέπει από τη μια σημαντική επαναχρησιμοποίηση των λειτουργικοτήτων του CoAP και από την άλλη παρέχει στο CoAP τις δυνατότητες για βελτιστοποιημένη χρήση των πόρων, περιλαμβανομένων αυτών που χρειάζονται για συσχετίσεις ασφάλειας. Για άμβλυνση των επιθέσεων άρνησης εξυπηρέτησης (DoS), χρησιμοποιείται η τεχνική του ακαταστασιακού (stateless) cookie , όπου οι πελάτες εξαναγκάζονται να

επαναμεταδίδουν το Hello του πελάτη (κατά τη χειραψία) με επισυναπτόμενο cookie, ο εξυπηρετητής βασιζόμενος στην επικύρωση του cookie, μπορεί να συνεχίσει την διαδικασία της χειραψίας. Η διαδικασία της χειραψίας εξελίσσεται, όπως φαίνεται στην Εικόνα 2, χρησιμοποιώντας το CoAP, όπου η αξιοπιστία της επικοινωνίας παρέχεται από τα CON και ACK μηνύματα, που περιέχουν τα DTLS μηνύματα της χειραψίας σαν φορτίο.

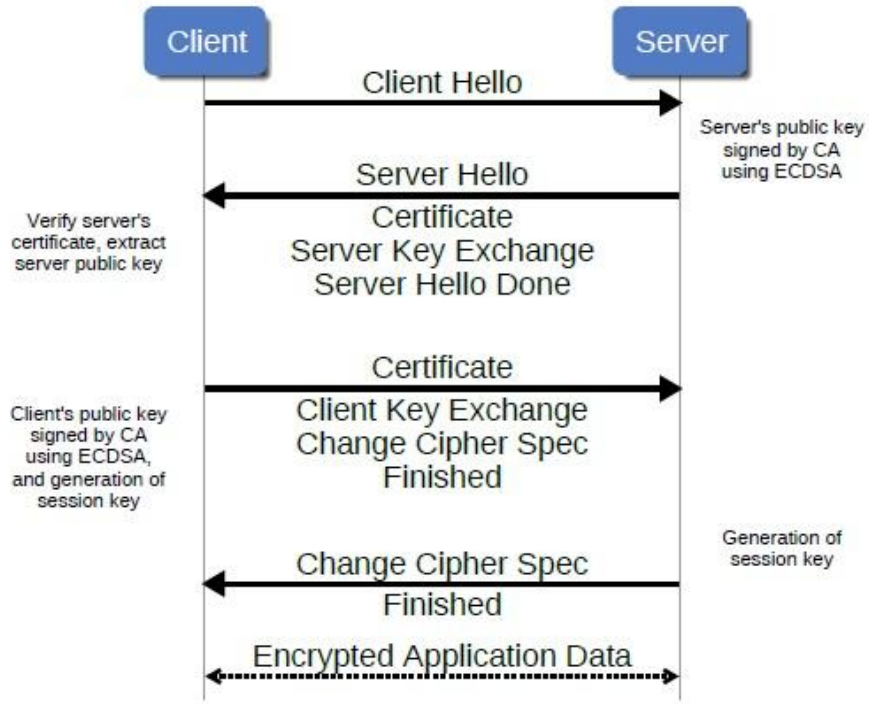


Εικόνα 2. DTLS συμφωνία κλειδιών στο CoAP με Raw Public Key.
Πηγή : Η εργασία που υπάρχει στην αναφορά [41].

Ένα αντικείμενο του IoT δρώντας σαν πελάτης μπορεί να αιτηθεί μια ασφαλή σύνδεση σε ένα αντικείμενο εξυπηρετητή, χρησιμοποιώντας το URI 'coaps://ipv6jost:port/dtls' με τη μέθοδο PUT περιέχοντας το 'Hello' μήνυμα του πελάτη σαν φορτίο. Σαν αποτέλεσμα μια νέα DTLS σύνοδος δημιουργείται στον εξυπηρετητή και μπορεί να ανανεωθεί χρησιμοποιώντας τη μέθοδο POST. Τα 'HelloVerifyRequest' και 'Hello' του πελάτη αντίστοιχα από τον εξυπηρετητή και τον πελάτη που ακολουθούν, μετριάζουν την DoS επίθεση που αναφέραμε παραπάνω. Στην συνέχεια και ανάλογα με τον αλγόριθμο κρυπτογράφησης, ανταλλάσσουν τις αναγκαίες πληροφορίες για να εγκαταστήσουν ένα κοινό μυστικό και να παραχθεί το κλειδί της συνόδου. Ανάλογα με το σετ των κρυπταλγόριθμων, τα μηνύματα σε αυτή τη φάση μπορεί να είναι αρκετά μεγάλα. Η συγκεκριμένη υλοποίηση του DTLS, αφήνει όλες τις εργασίες κατακερματισμού στο CoAP, μέσα από την εγγενή ικανοποιητική κατά τμήματα

μεταφορά. Τελικά, αφού και οι δυο, πελάτης και εξυπηρετητής λαμβάνουν το 'Finished' μήνυμα, η χειραψία έχει ολοκληρωθεί. Καθώς οι πόροι σε ένα αισθητήρα είναι περιορισμένοι, οι συσκευές μπορεί να κλείσουν μια DTLS σύνδεση για να ελευθερώσουν RAM. Αν λάβουμε υπ' όψη ότι η DTLS χειραψία είναι μακράν η πλέον ακριβή (σε πόρους) διαδικασία του DTLS πρωτόκολλου, το συχνό κλείσιμο και επανεγκατάσταση συνδέσεων είναι πολύ αναποτελεσματική. Για ατό αν η διαθέσιμη μνήμη σε ένα αισθητήρα, δεν μπορεί να αποθηκεύσει παραμέτρους για τις δουλειές που σχετίζονται με την ασφάλεια υιοθετείται μια στρατηγική κρυψίματος (caching) για να αποθηκεύει σε μια flash μνήμη του συνόλου των συσχετίσεων ασφάλειας που χρησιμοποιούνται συχνά.

Στο κρυπτογραφικό κομμάτι της διαδικασίας χειραψίας του πρωτόκολλου, χρησιμοποιείται το σετ των κρυπταλγόριθμων TLS ECDH ECDSA WITH AES 128 CCM 8, που περιγράφει την χρήση Diffie-Helman ελλειπτικών καμπυλών (ECDH), για συμφωνία κλειδιών (key agreement), όπου ένα πιστοποιητικό περιέχει το ECDH δημόσιο κλειδί που έχει υπογραφεί από την αρχή πιστοποίησης (CA) με αλγόριθμο ελλειπτικής καμπύλης ψηφιακή υπογραφή (ECDSA- Elliptic Curve Digital Signature Algorithm). Η Εικόνα 3 παρουσιάζει ένα στιγμιότυπο της διαδικασίας χειραψίας του DTLS.



Εικόνα 3. Συμφωνία κλειδιών του DTLS με ενσωματωμένο ECDH.
Πηγή : Η εργασία που υπάρχει στην αναφορά [41].

Η υλοποίηση της παραπάνω πρότασης έγινε σε μια πλατφόρμα MagoNode [42], η οποία αποτελείται από ένα μικροελεγκτή 8 bit πολύ μικρής κατανάλωσης που λειτουργεί στα 16MHz, και ένα ολοκληρωμένο πομποδέκτη μικρής κατανάλωσης ενέργειας. Το σύστημα μπορεί να επικοινωνεί σε μεγάλες αποστάσεις με μικρή κατανάλωση ενέργειας. Διαθέτει 16KB RAM και 128KB ROM, η οποία είναι αρκετή για αποθηκεύσει το τροποποιημένο (στη συγκεκριμένη υλοποίηση) TinyOS, ένα ενσωματωμένο λειτουργικό σύστημα για μικρής κατανάλωσης ασύρματες συσκευές, στο οποίο περιλαμβάνονται τα 6LoWPAN, RPL, UDP, CoAP, και την υλοποίηση του DTLS με χρήση ελλειπτικών καμπύλων. Από άποψη απόδοσης, το να υλοποιείς μια κρυπτογραφική βιβλιοθήκη σε περιορισμένων δυνατοτήτων συσκευές αποτελεί πρόκληση. Οι ασύρματοι αισθητήρες είναι εξοπλισμένοι με απλούς και φτηνούς μικροελεγκτές, με πολύ λίγα KB ROM και 10 ή 16 kb RAM. Κάνοντας βαρείς κρυπτογραφικές λειτουργίες, απαιτείται μεγάλος χρόνος εκτέλεσης, που επιδεινώνει την καθυστέρηση στην επικοινωνία και την κατανάλωση. Είναι κρίσιμο να υλοποιούνται αποτελεσματικά αυτές οι λειτουργίες, βελτιστοποιώντας αυτές στο χαμηλότερο επίπεδο, ώστε να πετύχουμε καλή απόδοση με αποδεκτό επίπεδο ασφάλειας. Περιγράφεται πως γίνεται η βελτιωμένη υλοποίηση των βασικών λειτουργιών, πάνω στις οποίες βασίζονται πολλά πρωτόκολλα ασφάλειας, όπως τα EDCH και ECDSA. Οι μεγάλοι αριθμοί σε συσκευές με 8 bit καταχωρητές υλοποιούνται με πίνακες και όταν γίνονται πολλαπλασιασμοί ή τετραγωνισμοί απαιτείται βελτιστοποιημένη χρήση των καταχωρητών. Αναπτύχθηκαν ρουτίνες σε κώδικα assembly ειδικά για την πλατφόρμα MagoNode, που επιτρέπουν μια εξελιγμένη χρήση των καταχωρητών, μειώνοντας έτσι τον αριθμό των λειτουργιών στη μνήμη. Επίσης αναπτύχθηκε μια ειδική βελτιστοποίηση ελλειπτικών καμπυλών που επιταχύνει τους πολλαπλασιασμούς υπολοίπου (mod) και τετραγωνισμούς, όπως και την αντιστροφή υπολοίπου, με αποτέλεσμα την επιπλέον μείωση του χρόνου για την εκτέλεση αυτών των πράξεων. Αποτέλεσμα αυτών είναι η υλοποίηση μιας βιβλιοθήκης για ECC βασισμένη στον συνδυασμό των TinyECC και Relic βιβλιοθηκών.

Αποτέλεσμα της χρήσης της τροποποιημένης έκδοσης του DTLS, είναι η χρήση της μνήμης κατά 23% λιγότερο από τη χρήση της κλασικής υλοποίησης του DTLS, όπως και μεγάλη αύξηση της ζωής του δικτύου, μέχρι 6,5 φορές, σε σύγκριση με την κλασική υλοποίηση του.

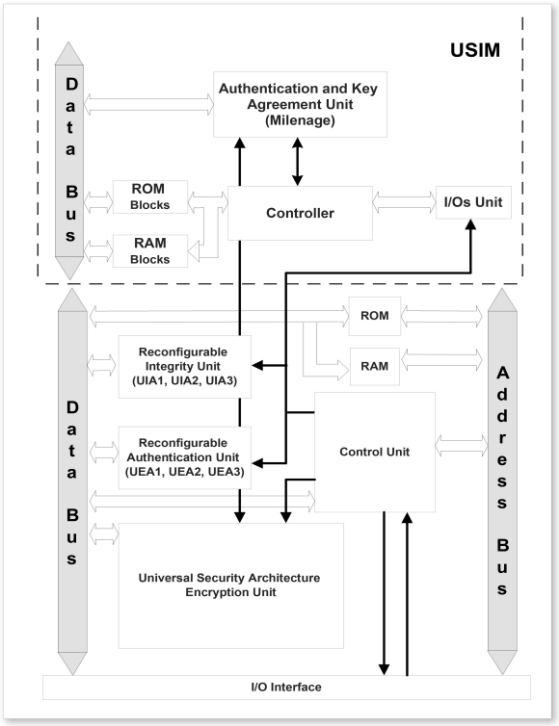
Η παραπάνω ενότητα βασίζεται στην εργασία που υπάρχει στην αναφορά [41].

6.3 Σχεδιασμός , Υλοποίηση Αποδοτικού Κρυπτο-Επεξεργαστή

Το IoT έχει αναπτυχθεί, και θα αναπτυχθεί πολύ περισσότερο και λόγω της εξέλιξης που υπάρχει στο υλικό, με αποτέλεσμα να γίνονται περισσότερα με όλο και μικρότερες συσκευές. Σε αυτό βοήθησε η ανάπτυξη και εξέλιξη των ολοκληρωμένων κυκλωμάτων (integrated circuits). Αναφέρουμε κάποια από αυτά που χρησιμοποιούνται ευρύτατα σε πάρα πολλά συστήματα, όπως το FPGA (Field-programmable gate array), ASIC (Application-specific integrated circuit). Συχνά γίνεται σύγκριση-σύγχυση αυτών με τον ολοκληρωμένο μικροελεγκτή Arduino, της ομώνυμης εταιρείας, που είναι ένα σύνολο από ολοκληρωμένα και ελεγκτές πάνω σε μια μικρή πλακέτα, έχοντας ψηφιακές και αναλογικές εισόδους/εξόδους.

Η αρχιτεκτονική ασφάλειας στα συστήματα LTE/SAE (Long Term Evolution/System Architecture Evolution) στην τεχνολογία LTE, που χρησιμοποιείται για την ασύρματη επικοινωνία και δικτύωση των κινητών συσκευών με υψηλές ταχύτητες, βασίζεται σε τέσσερις κρυπταλγόριθμους προσανατολισμένους στο υλικό (hardware-orienented), τον KASUMI (για εμπιστευτικότητα και ακεραιότητα) που είναι ένας κρυπταλγόριθμος τμήματος, τον SNOW-3G που είναι ένας κρυπταλγόριθμος ροής, το σύνολο των αλγορίθμων MILENAGE (για αυθεντικοποίηση και γεννήτρια κλειδιών), ο οποίος έχει τη δομή του γνωστού AES (Advanced Encryption Standard), και την 4G εξέλιξη του αλγόριθμου του ZUC, που είναι ένας κρυπταλγόριθμος ροής. Πιο συγκεκριμένα οι αλγόριθμοι ασφάλειας ασύρματης διασύνδεσης για 3G LTE, που είναι σε χρήση για την επίτευξη της εμπιστευτικότητας είναι οι UEA1/UEA2 (βασιζόμενοι στον αλγόριθμο KASUMI), και οι UIA1/UIA2 (βασιζόμενοι στον αλγόριθμο SNOW-3G) για την επίτευξη της ακεραιότητας. Οι βασικές διαδικασίες στην ασφάλεια της σύγχρονης κινητής τηλεπικοινωνίας, είναι, όπως ήδη έχουμε πει, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων. Θα δούμε την ανάπτυξη, με το ολοκληρωμένο κύκλωμα FPGA, ενός κρυπτοεπεξεργαστή καθολικής αρχιτεκτονικής ασφάλειας για τα 4G LTE συστήματα επικοινωνίας. Η προτεινόμενη αρχιτεκτονική κρυπτοεπεξεργαστή, για την υλοποίηση

σε υλικό, φαίνεται στην Εικόνα 4. Το προτεινόμενο σύστημα



Εικόνα 4. Η καθολική αρχιτεκτονική ασφάλειας.
Πηγή : Η εργασία που υπάρχει στην αναφορά [43].

ανταπεξέρχεται στις απαιτήσεις απόδοσης των πολυπληθών ενσωματωμένων συστημάτων της αγοράς, και μπορεί να παρέχει την υποδομή του δικτύου, με σχεδιασμό συμπαγούς λύσης που ενσωματώνει πολλά δομικά στοιχεία ασφάλειας του δικτύου, χρησιμοποιώντας λίγη ενέργεια, μικρό χώρο στο ολοκληρωμένο και εισάγοντας μικρή καθυστέρηση. Έχει σχεδιαστεί όπως ένας τυπικός επεξεργαστής περιλαμβάνοντας διαδρομή δεδομένων (data path), μνήμη, διεπαφή εισόδου/εξόδου (I/O interface), και μονάδα ελέγχου. Τέσσερα διαφορετικά σύνολα αλγόριθμων, μαζί με τις μονάδες αυθεντικοποίησης και ακεραιότητας, υποστηρίζονται από τον προτεινόμενο κρυπτοεπεξεργαστή. Οι αλγόριθμοι KASUMI, SNOW-3G, MILENAGE, και ZUC, επιλέχτηκαν για την Καθολικής Αρχιτεκτονικής Ασφάλειας Μονάδα Κρυπτογράφησης, Universal Security Architecture Encryption Unit (USAEU). Η επαναδιαμορφώσιμη μονάδα ακεραιότητας (Reconfigurable Integrity Unit-RIU) αποδίδει ικανοποιητικά στις τρεις μορφές των αλγόριθμων ακεραιότητας του καθολικού συστήματος τηλεπικοινωνιών (Universal Mobile Telecommunications System –UMTS) παρέχοντας όλη τη λειτουργικότητα που απαιτείται για τη τήρηση της ακεραιότητας, επιλέγοντας τον κατάλληλο κρυπταλγόριθμο. Αντίστοιχα συμβαίνει και με τη επαναδιαμορφώσιμη μονάδα αυθεντικοποίησης (Reconfigurable Authentication Unit-RAU) για τους αλγόριθμους τρεις αλγόριθμους αυθεντικοποίησης, παρέχοντας την αναγκαία

λειτουργία ανάλογα με τη λειτουργικότητα του κύριου συστήματος. Η διαφοροποίηση αυτής της υλοποίησης είναι ότι χρησιμοποιεί την βελτιστοποιημένη τεχνική της κοινής δεικτοδότησης των μονάδων αντικατάστασης (SBox), όπως και την επιλογή της κοινής διαδρομής, οι οποίες ενσωματώνονται στην USAEU, που αποτελείται από δυο κύριες μονάδες, την κοινής διαδρομής δεδομένων υπομονάδα (Common Data Path Sub Unit-CDP-SU) και την μονάδα κοινής δεικτοδότησης της μονάδας αντικατάστασης (Common SBox Indexation Module - CSIM). Η CSIM μονάδα υλοποιεί το νέο σχεδιασμός που ενώνει τα επτά SBox των KASUMI, SNOW-3G, MILENAGE(AES) και ZUC αλγόριθμων σε ένα καθολικό – κοινό SBox. Παρατηρείται ότι όλα τα επτά SBox των αλγόριθμων που αναφέρθηκαν παραπάνω, έχουν κοινά υποσύνολα δεκαεξαδικών ή σταθερής ροής από bit, τιμές εξόδου. Αντί να κατασκευαστούν επτά διαφορετικά ατομικά SBox ή μνήμες ROM, με μέγεθος τουλάχιστον το μέγεθος ενός γενικού AES SBox (8 x 8 bits), υλοποιείται μόνο ένα κοινό SBox, που περιέχει τις τιμές όλων των επτά ατομικών SBox. Η CDP-SU υπομονάδα υποστηρίζει τη λειτουργικότητα των τριών κρυπταλγόριθμων (KASUMI, SNOW-3G και ZUC). Αντί να υλοποιούνται σαν ατομικοί πυρήνες, η CDP-SU επιλέγει τα κοινά τμήματα διαύλου ανάλογα με την αίτηση του καθενός. Η μονάδα που εκτελεί αυτές τις λειτουργίες είναι το μπλοκ υλικού κοινού διαύλου δεδομένων (Common Data Path Hardware Block - CDPHB). Η CDP-SU περιέχει τις μονάδες υλικού του πυρήνα των KASUMI, SMOW-3G και ZUC, ενώ ο η λειτουργικότητα του MILENAGE μοντελοποιείται εξωτερικά, στη μονάδα κύριου κρυπτοεπεξεργαστή, επιλέγεται στην CDP-SU για να παρέχει τα κοινά τμήματα εξόδου με τους άλλους κρυπταλγόριθμους. Η CDP-SU περιέχει ένα δίαυλο 64 bit που χρησιμοποιείται για την ανάπτυξη της κοινής διαδρομής δεδομένων, όπως και για να μεταφέρει τα δεδομένα ανάμεσα στους κρυπταλγόριθμους και στον κύριο δίαυλο του συστήματος. Αυτή η προτεινόμενη αρχιτεκτονική συστήματος περιγράφηκε χρησιμοποιώντας τη γλώσσα vhdl, με δομική περιγραφή λογικής. Ο κώδικας συντέθηκε, τοποθετήθηκε και δρομολογήθηκε χρησιμοποιώντας ολοκληρωμένες συσκευές FPGA της XILINGS. Τα αποτελέσματα των μετρήσεων έδειξαν ότι η χρήση του κοινού SBox μείωσε το χώρο πάνω στο ολοκληρωμένο κατά 35 % σε σύγκριση με το κλασικό σύστημα των ατομικών SBox. Επίσης το κοινό Data Path αποδίδει αποτελεσματικά και στους τέσσερις αλγόριθμους και επιφέρει μείωση της καλυπτόμενης επιφάνειας του ολοκληρωμένου κατά 44 % περίπου σε συνδυασμό με την προηγούμενη τεχνική. Παράλληλα αυξήθηκε και η διεκπεραιωτικότητα (throughput) σε σύγκριση με τις υλοποιήσεις των ανεξάρτητων κρυπταλγόριθμων. Αποτέλεσμα αυτών είναι τα μικρότερα και οικονομικότερα

συστήματα, τόσο στην κατασκευή αλλά και στη χρήση διότι μικρότερο μέγεθος ολοκληρωμένου σημαίνει μικρότερη κατανάλωση ενέργειας.
Η παραπάνω ενότητα βασίζεται στην εργασία που υπάρχει στην αναφορά [43].

6.4 Σχεδιασμός Ασφαλούς Αρχιτεκτονικής Κίνησης Πολυμέσων

Πριν προχωρήσουμε στην παρουσίαση της αρχιτεκτονικής θα αναφέρουμε μερικά πράγματα για τη διαχείριση των κλειδιών σε ένα δίκτυο [44]. Έχουν προταθεί πολλά σχήματα τα οποία μπορούν να χωριστούν σε τρεις κλάσεις

- Μη Επεκτάσιμα σχήματα (Non Scalable) και Επεκτάσιμα σχήματα (Scalable). Τα επεκτάσιμα σχήματα μπορούν να χωριστούν σε τρεις ομάδες διαχείρισης κλειδιών: Ιεραρχική (Hierarchical), Κεντρικοποιημένη οριζόντια (Centralized flat), Κατανεμημένη οριζόντια (Distributed)
- Οριζόντια σχήματα (Flat schemes), σχήματα συστάδας (Clusterd Schemes), Δενδροειδή σχήματα (Tree based schemes).
- Κεντρικοποιημένα σχήματα (Centralized schemes), κατανεμημένης υποομάδας σχήμα (Distributed subgroups schemes), κατανεμημένα σχήματα (Distributed schemes)

Επίσης σημαντική είναι η διαδικασία της περιοδικής ανανέωσης των κλειδιών, που πρέπει να γίνεται λαμβάνοντας υπ' όψη αφ' ενός την βελτίωση της ασφάλειας και αφ' ετέρου ότι είναι πολύπλοκο να επιτευχθεί. Τρεις τρόποι ανανέωσης προτείνονται:

- Περιοδική ομαδική ανανέωση κλειδιών(Periodic batch rekeying), ο εξυπηρετητής κλειδιών χειρίζεται τα αιτήματα εισόδου και εξόδου περιοδικά και ομαδικά.
- Περιοδική ομαδική ανανέωση κλειδιών εξόδου (Periodic batch leave rekeying), γίνεται ενημέρωση άμεσα των αιτημάτων εισόδου, για να μειωθεί η καθυστέρηση εισόδου στο IoT, ενώ τα αιτήματα εξόδου επεξεργάζονται ομαδικά.
- Περιοδική ομαδική ανανέωση αιτημάτων εισόδου(Periodic batch join rekeying), χειρίζεται άμεσα κάθε αίτημα εξόδου, για να μειώσει την έκθεση των χρηστών που έχουν φύγει, και περιοδικά και ομαδικά τα αιτήματα εισόδου.

Τα χαρακτηριστικά του IoT επιτρέπουν την ανάπτυξη τεράστιων ποσοτήτων πολυμεσικής κίνησης, συνήθως αυτό πραγματοποιείται με πολλαπλούς αισθητήρες υψηλής νοημοσύνης για επικοινωνία υπολογισμούς και δυνατότητες υπηρεσιών.

Μπορούμε να κατατάξουμε την πολυμεσική κίνηση στο IoT σε τρεις κατηγορίες: επικοινωνίας, υπολογισμών και υπηρεσιών.

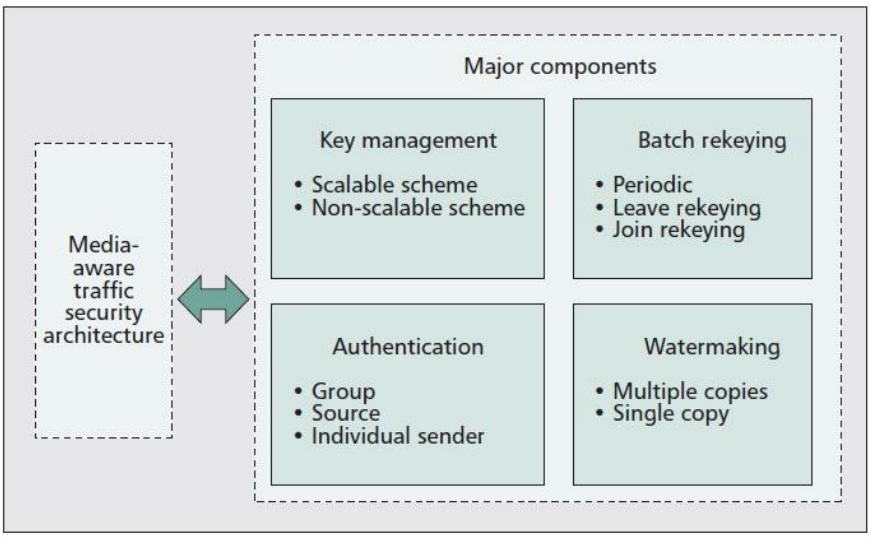
Λέγοντας κυκλοφορία επικοινωνίας εννοούμε την οποτεδήποτε, οπουδήποτε, και με οποιοδήποτε μέσο επικοινωνία στο IoT. Στο γενικό πλαίσιο το βασικό συστατικό είναι ένα σύστημα RFID, που αποτελείται από αρκετούς αναγνώστες και RFID ετικέτες, κάθε ετικέτα χαρακτηρίζεται από ένα μοναδικό αναγνωριστικό και εφαρμόζεται σε διαφορετικά αντικείμενα. Οι αναγνώστες ενεργοποιούν την εκπομπή των ετικετών οι οποίες παράγουν ένα μήνυμα, το οποίο παριστά ένα ερώτημα για την πιθανή παρουσία ετικετών στην περιοχή του αναγνώστη. Τα δίκτυα αισθητήρων είναι τα σημαντικότερα συστατικά του IoT και μπορούν να συνεργαστούν με τα συστήματα RFID για να ολοκληρωθεί η λειτουργία της επικοινωνίας. Τα δίκτυα αισθητήρων αποτελούνται από κόμβους αισθητήρων που επικοινωνούν με πολυαλματικό τρόπο, και αναφέρουν το αποτέλεσμα σε κόμβους αποδέκτες.

Για την κίνηση επικοινωνίας στο IoT το πρωτόκολλο IEEE 802.15.4 δεν περιλαμβάνει προδιαγραφές για τα ανώτερα στρώματα, πράγμα που είναι αναγκαίο για την απρόσκοπτη ολοκλήρωση των κόμβων αισθητήρων στο διαδίκτυο. Ένα θέμα είναι να γίνεται η επικοινωνία υπακούοντας στους περιορισμούς που θέτει το IEEE 802.15.4 (πχ. 127 bytes το μέγεθος του πακέτου στο φυσικό στρώμα και 102 bytes στο MAC στρώμα), και στη ιδιαιτερότητα των αισθητήρων που τίθενται σε κατάσταση ύπνωσης για εξοικονόμηση ενέργειας. Συνοπτικά σκοπός του σχεδιασμού κατάλληλων δικτύων κίνησης πολυμέσων είναι η ενεργειακή απόδοση, η επεκτασιμότητα, η αξιοπιστία και η ευρωστία.

Συνήθως η υπολογιστική κίνηση στο IoT μπορεί να επεξεργαστεί από κινητούς πράκτορες ή αποδέκτες (sink nodes) αυτόνομα. Η σειρά με την οποία ένα κινητός πράκτορας επισκέπτεται τους επιλεγμένους κόμβους, μπορεί να έχει σημαντική επίδραση στην υπολογιστική κίνηση. Η υπολογιστική κίνηση κατηγοριοποιείται, σε στατική, δυναμική και υβριδική. Η στατική κατάσταση του κινητού πράκτορα καθορίζεται από τον κόμβο πηγή πριν αποσταλεί, κάνει χρήση των τρεχουσών συνθηκών όλου του δικτύου και βρίσκει ένα ικανοποιητικό μονοπάτι πριν ο κινητός πράκτορας αποσταλεί. Στη δυναμική, ο πράκτορας αυτόνομα καθορίζει του κόμβους πηγές και αποφασίζει τη δυναμική διαδρομή ή την κατανομή των πόρων, σύμφωνα με τις τρέχουσες συνθήκες του δικτύου. Στη υβριδική το σύνολο των κόμβων που αποτελούν πηγή αποφασίζεται από τους κόμβους αποδέκτες, ενώ η σειρά επίσκεψης των κόμβων που αποτελούν πηγή επεξεργάζεται από τους κινητούς πράκτορες. Η

κίνηση υπηρεσιών περιέχει δυο απόψεις, τη βαθμολογία και τη μορφή. Η βαθμολογία εννοεί το βαθμό ενδιαφέροντος που έχει ένας χρήστης για την κίνηση πολυμέσων, ενώ η μορφή υποδηλώνει τα χαρακτηριστικά του περιεχομένου σε μια συγκεκριμένη συσκευή. Για το σκοπό της αποτελεσματικής λειτουργίας ποικίλων τύπων κίνησης πολυμέσων, τα δεδομένα κατατάσσονται σε τρεις κατηγορίες, τα δεδομένα προτίμησης, τα δεδομένα κατάστασης και τα δεδομένα ικανότητας. Επιπλέον η προσαρμογή της κίνησης πολυμέσων χρησιμοποιεί δυο τεχνικές, την ανακεφαλαίωση-σύνοψη και την διακωδικοποίηση. Η σύνοψη πολυμέσων σημαίνει ότι συνοψίζουμε τις υπηρεσίες πολυμέσων σε μια σύντομη (από πλευράς μεγέθους δεδομένων) υπηρεσία που μπορεί να ειδωθεί σε μια μικρή κλίμακα χρόνου. Η διακωδικοποίηση πολυμέσων σημαίνει ότι μετατρέπουμε το περιεχόμενο από ένα τύπο μέσου σε άλλο ώστε το περιεχόμενο να μπορεί κατάλληλα να επεξεργαστεί από μια συγκεκριμένη συσκευή, ή ικανοποιητικά να μεταδοθεί με συγκεκριμένη κατάσταση επικοινωνίας.

Με σκοπό να πετύχουμε τις απαιτήσεις ασφάλειας των πληροφοριών για πολυμέσα, επικοινωνία, υπολογισμό και υπηρεσία, στο περιβάλλον του IoT, είναι απαραίτητο να σκεφτούμε κάποια κριτήρια που αναφέρονται στη στρατηγική της ασφάλειας της κίνησης και στην απόδοση. Προτείνεται μια νέα Ενήμερη Μέσων Αρχιτεκτονική Ασφαλούς Κίνησης, Media-Aware Traffic Security Architecture-MTSA για να λύσει αυτό το πρόβλημα. Ακολουθεί η σχεδίαση του MTSA στην Εικόνα 5.



Εικόνα 5. Τα κύρια μέρη της Αρχιτεκτονικής MTSA.
Πηγή : Η εργασία που υπάρχει στην αναφορά [44].

Η αρχιτεκτονική MTSA περιλαμβάνει την διαχείριση κλειδιών (με νέα κατηγοριοποίηση που έχει σαν κριτήρια την κίνηση στα πολυμέσα που ασκεί τον έλεγχο και αν είναι το σχήμα επεκτάσιμο ή όχι). Έτσι δημιουργούνται τρεις κλάσεις, έλεγχος υπηρεσιών, έλεγχος χρηστών και έλεγχος ροής, και κάθε κλάση ταξινομείται περαιτέρω σε επεκτάσιμα και μη επεκτάσιμα σχήματα. Την ομαδική ανανέωση κλειδιών, που παρέχει μια καλή εναλλακτική ανάμεσα στην βελτίωση της ασφάλειας και την πολυπλοκότητα των υπολογισμών. Την αυθεντικοποίηση (με έλεγχο πρόσβασης που γίνεται από λίστα, πιστοποιητικά ικανότητας, αμοιβαία αυθεντικοποίηση). Η αυθεντικοποίηση πολυμέσων μπορεί να χωριστεί σε τρία επίπεδα, ομαδική αυθεντικοποίηση, αυθεντικοποίηση πηγής και ατομική αυθεντικοποίηση αυτού που αποστέλλει. Την υδατογράφηση (η οποία περιλαμβάνει ταυτοποίηση προέλευσης του περιεχομένου, ιχνηλάτηση παρανόμως κατανεμηθέντων αντιγράφων, απενεργοποίηση μη εξουσιοδοτημένης πρόσβασης στο περιεχόμενο) η οποία, για να μην έχουμε καθυστερήσεις σε ευαίσθητες πολυμεσικές εφαρμογές, ενεργοποιείται μόνο όταν υπάρχει θέμα με τα δικαιώματα του χρήστη.

Η MTSA παρέχει ένα συστηματικό πλαίσιο για πολυμεσική ασφάλεια πληροφοριών. Η αποκεντρωμένη διαδικασία απόκτησης δεδομένων στο MTSA προσφέρει ευκαιρίες εκμετάλλευσης της κατανεμημένης φύσης του δικτύου. Δίνεται ένα νέο κατανεμημένο παράδειγμα ιδιωτικότητας για το MTSA, στο οποίο η αρχή, το κόστος και η κρυπτογράφηση αποκτώνται με αποκεντρωμένο τρόπο. Τρεις επιδιώξεις έχουμε για το κατανεμημένο σύστημα ιδιωτικότητας. Κάθε αισθητήρας ή κινητός πράκτορας πρέπει να δημιουργήσει το δικό του μερίδιο χωρίς την ανάγκη κεντρικής αρχής. Από την πλευρά του μεγέθους, κάθε μυστικό μερίδιο πρέπει να μην είναι μεγαλύτερο από το αρχικό μυστικό. Από την πλευρά ενός επιτιθέμενου η απόκτηση πολυμεσικών περιεχομένων δεν θα υποβαθμίσει το μέγεθος του μυστικού μεριδίου. Η πρώτη επιδίωξη κάνει αναγκαία τη χρήση μιας κατανεμημένης μεθόδου με παραδοσιακή αρχιτεκτονική υπηρεσιών. Η δεύτερη προάγει την αποδοτική διαδικασία του διαμοιρασμού και εξαιρεί την κατευθείαν κρυπτογράφηση. Καθώς κάθε αισθητήρας στο IoT έχει συσχετισμένη πληροφορία, είναι βασικό ότι αυτή η ομοιότητα μπορεί να χρησιμοποιηθεί για να μειώσει το μέγεθος του μυστικού μεριδίου. Η τρίτη προστατεύει το IoT σύστημα από ένα επιτιθέμενο που μπορεί να έχει πρόσβαση στα στατικά περιεχόμενα πολυμέσων ξαναδημιουργώντας το μυστικό. Συγκεκριμένα τα χαρακτηριστικά του μοντέλου απειλής που χρησιμοποιείται είναι: κάθε χρήστης μπορεί να κρυφακούσει μόνο ένα μικρό υποσύνολο των μονοπατιών επικοινωνίας, άπαξ ένας

κόμβος υποστεί υφαρπαγή απομακρύνεται από το σύστημα, και μια ενεργή επίθεση σε εφαρμογές πολυμέσων εκτελείται σε κανονικούς κόμβους. Η πρώτη παραδοχή απειλής αντανακλά ένα εύλογο επίπεδο ικανότητας του επιτιθέμενου. Για να μειώσει το μέγεθος του μεριδίου ένας επιτιθέμενος πρέπει να είναι φυσικά κατανεμημένος σε όλο το IoT. Η δεύτερη και η Τρίτη απαίτηση απειλής καθιστούν αδύνατη την καταστροφή του περιεχόμενου του εξυπηρετητή κατά τη διάρκεια της διαδικασίας της δημιουργίας του μεριδίου.

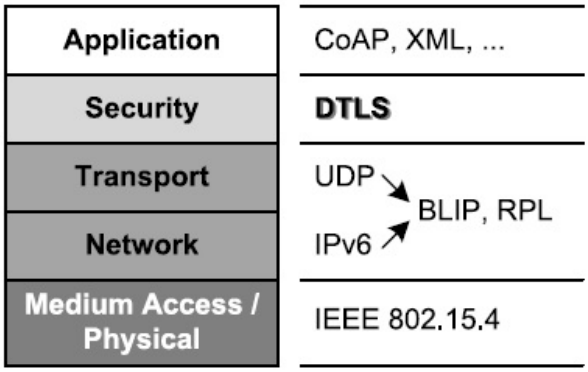
Η προσέγγιση που αναφέρεται είναι διαφορετική από το παραδοσιακό πρόβλημα μυστικού μεριδίου. Κατά το μυστικό μερίδιο, μια έμπιστη κεντρική αρχή, πχ. ένας εξυπηρετητής πολυμέσων, μοιράζει ένα μυστικό σε πολλούς χρήστες. Εδώ απόλυτη εχεμύθεια πετυχαίνεται μέσω της χρήσης από τον εξυπηρετητή συναρτήσεων κατακερματισμού για την παραγωγή των μεριδίων που είναι γνωστά μόνο στον εξυπηρετητή, ούτε οι χρήστες δεν μπορούν να έχουν πρόσβαση στο μερίδιο.
Υπάρχουν διαφορές ανάμεσα στο μυστικό μερίδιο του MTSA και των παραδοσιακών αλγόριθμων μυστικού μεριδίου. Πρώτο, το παραδοσιακό μυστικό μερίδιο έχει σχεδιαστεί να δημιουργεί τα μερίδια από ένα μοναδικό μυστικό. Στο MTSA κάθε αισθητήρας έχει μια συσχετισμένη ανάγνωση των άλλων αναπαριστώντας ένα σύνθετο μυστικό. Δεύτερο, δεδομένης της κεντρικής φύσης του μυστικού μεριδίου, όπου ένας εξυπηρετητής δημιουργεί τα μερίδια, μια σαφής προσαρμογή είναι να έχουμε τους αισθητήρες σε μια ομάδα που ανταλλάσσει τις πληροφορίες σε ένα μοναδικό κόμβο. Τρίτο, αν κάθε αισθητήρας μπορεί να έχει πρόσβαση σε όλους τους εξυπηρετητές, κάθε κόμβος μπορεί υποχρεωτικά να πρέπει να μοιράζει το τυχαίο περιεχόμενο πολυμέσων με ένα εξυπηρετητή, κάνοντας αυτό ευκολότερο για ένα που κρυφακούει να αποκτά τις τιμές, θέτοντας σε κίνδυνο οποιονδήποτε από τους αισθητήρες. Ο αλγόριθμος που προτείνεται θυσιάζει την απεριόριστη ασφάλεια για να παρέχει μια γενική λύση ασφάλειας για πολυμέσα για όλους τους αισθητήρες στο IoT, χρησιμοποιώντας μια κατανεμημένη εκδοχή του οπτικού μυστικού μεριδίου. Συγκεκριμένα, χρησιμοποιείται ένα οπτικό μέτρο μυστικότητας που υποβαθμίζεται αναλογικά με τον αριθμό των μεριδίων που κατέχει ο επιτιθέμενος. Ένας τέτοιος χαλαρός ορισμός της μυστικότητας βασίζεται σε αντιληπτή παραμόρφωση πολυμέσων. Συγκρινόμενο με παραδοσιακές λύσεις οπτικού μυστικού μεριδίου, το προτεινόμενο σχήμα μειώνει την πολυπλοκότητα των πολυμεσικών υπολογισμών και μειώνει το μέγεθος των μεριδίων.
Η παραπάνω ενότητα βασίζεται στην εργασία που υπάρχει στην αναφορά [44].

6.5 Σχεδιασμός Ασφαλούς Αρχιτεκτονικής για το IoT Βασιζόμενη στο DTLS

Πριν προχωρήσουμε στην παρουσίαση της αρχιτεκτονικής θα δούμε σύντομα το πρωτόκολλο DTLS.

Όλα τα μηνύματα που στέλνονται μέσω DTLS έχουν μια επικεφαλίδα 13 byte. Αυτή καθορίζει το περιεχόμενο του μηνύματος, την έκδοση του πρωτόκολλου, όπως και μια ακολουθία αριθμών 64 bit ,και το μήκος της εγγραφής. Τα δυο byte στην κορυφή της ακολουθίας των αριθμών χρησιμοποιούνται να καθορίσουν τη εποχή (epoch) του μηνύματος που αλλάζει όταν νέες παράμετροι κρυπτογράφησης διαπραγματεύονται ανάμεσα στον πελάτη και τον εξυπηρετητή. Η επικεφαλίδα της εγγραφής είτε ακολουθείται από απλό κείμενο, αν δεν έχει ακόμα διαπραγματευτεί ασφάλεια ή από το DTLS block. Αν ένας κρυπταλγόριθμος χρησιμοποιείται, το απλό κείμενο έχει μπροστά του ένα τυχαίο διάνυσμα αρχικοποίησης, που έχει το μέγεθος του block του κρυπταλγόριθμου. Αυτό προστατεύει από επιθέσεις στα σετ των κρυπταλγόριθμων χρησιμοποιώντας την CBC λειτουργία για τους κρυπταλγόριθμους τμήματος του σετ. Το απλό κείμενο ακολουθείται από HMAC, έναν κώδικα αυθεντικοποίησης μηνύματος με συνάρτηση κατακερματισμού, που επιτρέπει στον παραλήπτη να ανιχνεύει αν η DTLS εγγραφή έχει αλλοιωθεί. Τέλος στο μήνυμα προστίθενται χαρακτήρες για να είναι πολλαπλάσιο του μήκους του block του κρυπταλγόριθμου. Σε αντίθεση με το TLS το DTLS δεν επιτρέπει τους κρυπταλγόριθμους ροής γιατί είναι ευαίσθητοι στην απώλεια του μηνύματος και στην αναδιάταξη. Χρησιμοποιεί κρυπταλγόριθμους τμήματος σε CBC λειτουργία. Τα κλειδιά και το σετ των κρυπταλγόριθμων, που αποτελείται από κρυπταλγόριθμο τμήματος και ένα αλγόριθμο κατακερματισμού, διαπραγματεύονται ανάμεσα στον πελάτη και τον εξυπηρετητή κατά τη φάση της χειραψίας που ξεκινά πριν οποιαδήποτε δεδομένα εφαρμογών μεταφερθούν. Υπάρχουν τρεις τύποι χειραψίας. Πρώτα, κατά τη διάρκεια μιας χειραψίας χωρίς αυθεντικοποίηση κανένα μέρος δεν αυθεντικοποιεί το άλλο. Δεύτερο, κατά την διάρκεια της αυθεντικοποιημένης χειραψίας του εξυπηρετητή, μόνο ο εξυπηρετητής αποδεικνύει την ταυτότητα του στον πελάτη. Τρίτο, σε μια πλήρως αυθεντικοποιημένη χειραψία ο πελάτης πρέπει να αυθεντικοποιήσει τον εαυτό του στον εξυπηρετητή επίσης. Υπάρχουν διάφοροι αλγόριθμοι που μπορούν να χρησιμοποιηθούν για αυθεντικοποίηση κατά τη χειραψία του DTLS.

Η αρχιτεκτονική συστήματος ακολουθεί το μοντέλο του IoT. Στο σχεδιασμό αυτό επιλέγεται το πρωτόκολλο DTLS έχοντας πάρει τρεις αποφάσεις σε υψηλό επίπεδο σχεδιασμού. Υλοποίηση βασιζόμενη σε πρότυπα , τα ράδιο πλινθία (radio chip) μπορούν να βασίζονται στο IEEE 802.15.4 για το φυσικό και το MAC στρώμα, το RPL ή το 6LoWPAN προσφέρουν λειτουργικότητα δρομολόγησης, και το CoAP καθορίζει το στρώμα εφαρμογών. Εστίαση στο στρώμα εφαρμογών για από άκρου σε άκρο ασφάλεια , χρησιμοποιώντας το DTLS το οποίο βρίσκεται μεταξύ του στρώματος μεταφοράς και εφαρμογών, δεν απαιτείται από τον πάροχο υποδομής να υποστηρίζει μηχανισμό ασφάλειας, αλλά αφήνεται στις επικοινωνούσες εφαρμογές να αποκαταστήσουν την ασφάλεια. Υποστήριξη για αναξιόπιστα πρωτόκολλα, χρησιμοποιώντας το DTLS σε συνδυασμό με το UDP δεν υποχρεώνει αυτόν που αναπτύσσει εφαρμογές να χρησιμοποιήσει αξιόπιστη μεταφορά, αν απαιτείται αξιόπιστη μηνυματοδοσία (messaging) θα πρέπει να επιλεγεί ένα αξιόπιστο στρώμα.

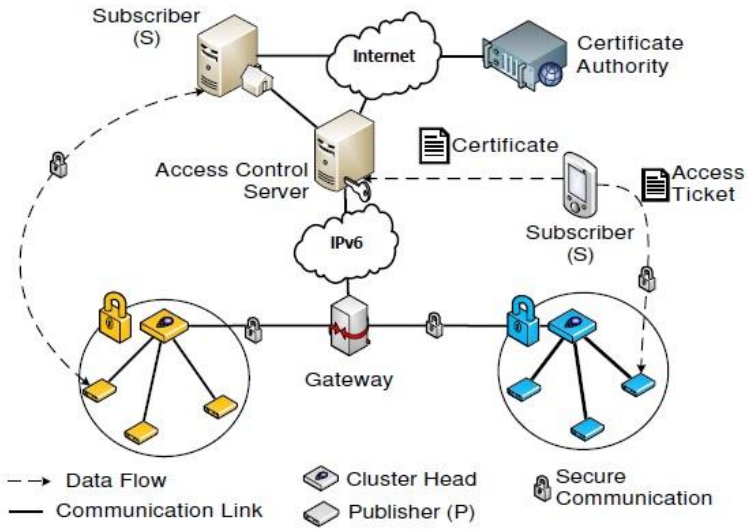


Εικόνα 6. Στοίβα πρωτόκολλων της αρχιτεκτονικής.
Πηγή : Η εργασία που υπάρχει στην αναφορά [45].

Αφού βασίζεται ο σχεδιασμός σε πρότυπα για να υπάρχει διαλειτουργικότητα η αυθεντικοποίηση θα βασίζεται στον RSA, που είναι βασικός στην κρυπτογραφία δημόσιου κλειδιού, και υπάρχει υποστήριξη μέσα από υλικό για αποθήκευση των κλειδιών του RSA στα TPM (Trusted Platform Module, ένα ενσωματωμένο chip που μπορεί να αποθηκεύει τα κλειδιά του RSA, και να τον υλοποιεί), με μόνη επιφύλαξη τα 2048 bits του κλειδιού του. Η αρχιτεκτονική του συστήματος ακολουθεί το μοντέλο του IoT. Θεωρείται ότι στο κοντινό μέλλον το IPv6 θα χρησιμοποιείται στο διαδίκτυο και τμήματα θα τρέχουν σε 6LoWPAN (μετρήσεις της Google δείχνουν ότι τον Δεκέμβριο του 2017 οι χρήστες του διαδικτύου που συνδέονται με IPv6 είναι περίπου το 20%). Το στρώμα μεταφοράς στο 6LoWPAN είναι UDP, που δεν είναι αξιόπιστο, και στο στρώμα δρομολόγησης έχουμε RPL ή Hydro το οποίο και χρησιμοποιείται γιατί είναι ίδιο με το

RPL, ενώ υπάρχει σαν μέρος του TinyOS. Το IEEE 802.15.4 χρησιμοποιείται στο φυσικό και στο στρώμα MAC. Βασιζόμενο σε αυτή τη δομή πρωτόκολλων επιλέγεται το DTLS σαν πρωτόκολλο ασφάλειας. Τοποθετείται στο στρώμα εφαρμογών πάνω από το UDP στρώμα μεταφοράς, το οποίο φαίνεται στην Εικόνα 6.

Παρόμοια με την ασφάλεια στα παραδοσιακά δίκτυα πρέπει να τηρείται η αυθεντικότητα, η ακεραιότητα και η εμπιστευτικότητα. Για να επιτευχθούν αυτές οι βασικές αρχές εισάγεται ένας εξυπηρετητής ελέγχου πρόσβασης (Access Control Sever), και χρησιμοποιούνται αισθητήρες εφοδιασμένοι με TPM στο δίκτυο και η ασφάλεια υλοποιείται με PKC (Public Key Cryptography) και φυσικά συμμετοχή CA (Certified Authority). Αν δεν είναι εφοδιασμένοι με TPM προτείνεται η αυθεντικοποίηση μέσω των προμοιρασμένων κλειδιών του DTLS, τα οποία πρέπει να ανακοινωθούν και στον εξυπηρετητή της CA που τα φανερώνει σε συσκευές με επαρκή εξουσιοδότηση. Η εγκατάσταση της σύνδεσης είναι δυναμική και εξαρτάται από το αν οι αισθητήρες χρησιμοποιούν TPM ή όχι. Το σύστημα υλοποιήθηκε σε ένα DTLS πελάτη (client) που είναι ένας Opal κόμβος αισθητήρα με Atmel SAM3U ελεγκτή και ένα Atmel TPM με 48 kB RAM, και ένα μικροελεγκτή στα 48 MHz , που εκτελεί την χειραψία με ένα OpenSSl 1.0.0.d εξυπηρετητή. Το DTLS χρησιμοποιούσε τον TLS-RSA-with-AES-128-CBC-SHA.AES-128 αλγόριθμο. Τα αποτελέσματα της υλοποίησης έδειξαν ότι το προτεινόμενο σύστημα παρέχει ακεραιότητα, εμπιστευτικότητα και αυθεντικοποίηση μηνύματος με ικανοποιητική κατανάλωση ενέργειας, από άκρου σε άκρο καθυστέρηση και φόρτο μνήμης. Η επισκόπηση αυτού του σχεδιασμού φαίνεται στην Εικόνα 7.

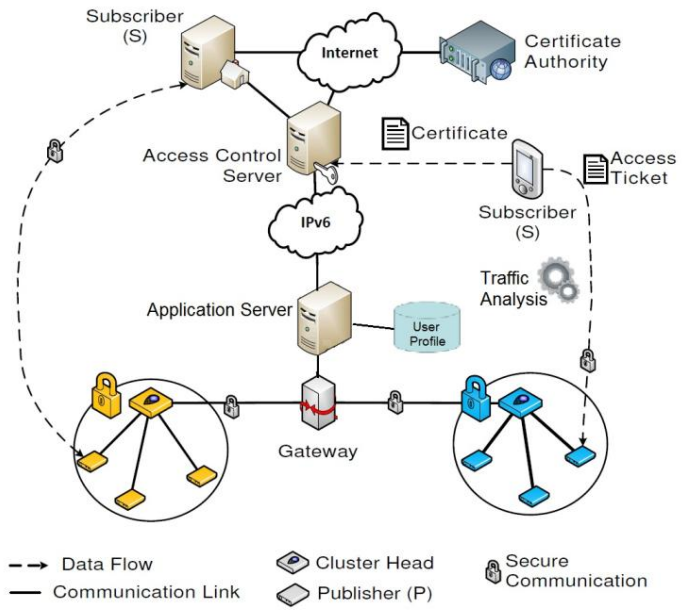


Εικόνα 7. Επισκόπηση προτεινόμενης αρχιτεκτονικής συστήματος.
Πηγή : Η εργασία που υπάρχει στην αναφορά [45].

Η παραπάνω ενότητα βασίζεται στην εργασία που υπάρχει στην αναφορά [45].

6.6 Σχεδιασμός Νέου Συστήματος

Έχοντας αναφερθεί αναλυτικά στα δυο τελευταία συστήματα μπορούμε να προτείνουμε ένα νέο σύστημα που θα συνδυάζει τα δυο παραπάνω. Την αρχιτεκτονική του MTSA, υποενότητα 6.4 της παρούσας διπλωματικής διατριβής, την υλοποιούμε σε ένα εξυπηρετητή εφαρμογών και αυτόν τον ενσωματώνουμε στην προτεινόμενη, στο εδάφιο 6.5 της παρούσας, αρχιτεκτονική συστήματος. Ο σχεδιασμός αυτός φαίνεται στην Εικόνα 8.



Εικόνα 8. Σχέδιο προτεινόμενης αρχιτεκτονικής.
Πηγή : Τροποποίηση συνδυασμού εικόνων των εργασιών στις αναφορές [44] [45].

Η αρχιτεκτονική MTSA χρησιμοποιεί για τον έλεγχο πρόσβασης προκαθορισμένες λίστες με τους υπολογιστές και τις συσκευές που έχουν δικαίωμα σύνδεσης στον εξυπηρετητή. Γι' αυτό και στη προτεινόμενη αρχιτεκτονική διατηρούμε τη διαδικασία εγκατάστασης επικοινωνίας που προβλέπει η αρχιτεκτονική που βασίζεται στο DTLS και η οποία είναι δυναμική. Το κομμάτι που προτείνεται να υιοθετηθεί στη νέα αρχιτεκτονική από την MTSA, είναι αυτό που αφορά στη δημιουργία και χρήση του μυστικού μεριδίου (secret share), καθώς στην MTSA εμπεριέχεται μια κατανεμημένη παραλλαγή κρυπτογράφησης με οπτικά μυστικά μερίδια. Βασίζεται στο γεγονός ότι κάθε αισθητήρας IoT παρέχει πληροφορίες οι οποίες μπορούν να συσχετιστούν με τις πληροφορίες άλλων αισθητήρων στην ομάδα του, και αυτή η ομοιότητα μπορεί να αξιοποιηθεί για τη μείωση του μεγέθους του μυστικού μεριδίου. Επιπλέον, δημιουργείται ένα σύνθετο μυστικό, κάτι που αυξάνει το επίπεδο ασφάλειας και την

ανοχή σε προσπάθειες υποκλοπής δεδομένων. Συνολικά καταλήγουμε στο ότι ο συνδυασμός του οπτικού μυστικού μεριδίου της MTSA αρχιτεκτονικής με την αρχιτεκτονική της υποενότητας 6.5 προσφέρει περισσότερη ασφάλεια, ενώ παράλληλα, όπως αναφέρεται και στο [44] μειώνεται η πολυπλοκότητα των υπολογισμών που σχετίζονται με τις ροές πολυμέσων και μειώνεται και το μέγεθος των μεριδίων.

Κεφάλαιο 7
Επίλογος

Ολοκληρώνοντας την εργασία μπορούμε να συμπεράνουμε ότι η μεγάλη παραγωγή φτηνών συσκευών που μπορούν να συνδέονται στο IoT θα αυξήσει κατά πολύ τους χρήστες του IoT. Εκείνο που προέχει είναι αυτοί που συνδέονται, για οποιοδήποτε λόγο, θα πρέπει να το κάνουν με ασφάλεια. Εύκολα συμπεραίνουμε ότι η ασφάλεια πρέπει να ξεκινά από το χαμηλότερο επίπεδο και αυτό μπορεί να γίνει με ενσωμάτωση των κρυπτογραφικών αλγόριθμων ασφάλειας, με ότι χρειάζεται για να λειτουργήσουν, στα ολοκληρωμένα των συσκευών που κάνουν την αρχική καταγραφή των δεδομένων. Φυσικά και στα παραπάνω επίπεδα πρέπει να υπάρχει ασφάλεια, η οποία πρέπει να υλοποιείται μέσα από τα πρωτόκολλα που χρησιμοποιούνται. Αναφέροντας συνεχώς τις έννοιες της αυθεντικοποίησης και της εμπιστευτικότητας κατανοούμε ακόμα περισσότερο την αξία της ύπαρξης αξιόλογων αλγόριθμων κρυπτογραφίας, γιατί μέσα από της κρυπτογράφηση επιτυγχάνονται. Προφανώς αυτό γίνεται εξελίσσοντας υπάρχοντες αλγόριθμους και δημιουργώντας νέους. Μια υποσχόμενη για το μέλλον εξέλιξη είναι αυτή της Κβαντικής κρυπτογραφίας, που εστιάζεται περισσότερο προς την κβαντική διανομή κλειδιού, η οποία τεχνική βασίζεται στην αρχή της απροσδιοριστίας. Βέβαια κάποιες επιτυχείς επιθέσεις σε κβαντικά συστήματα δεν πρέπει να μειώνουν την αξία του θεωρητικού υπόβαθρου , αλλά πρέπει να οδηγούν προς καλύτερες και πιο αξιόπιστες υλοποιήσεις, όχι μόνο στην συγκεκριμένη περίπτωση αλλά και σε άλλες.

Βιβλιογραφία

[1] M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας, and Β. Χρυσικόπουλος, *Σύγχρονη κρυπτογραφία : Θεωρία και εφαρμογές*. ΑΘΗΝΑ: ΠΑΠΑΣΩΤΗΡΙΟΥ ΕΚΔΟΣΕΙΣ, 2011, pp. 8, 14, 5, 6, 11, 21, 2, 222, 21, 22, 26, 14, 34, 35, 250, 249, 277, 281, 301, 299, 313 ,353.

[2] M. R. Whitman and H. H. Mattord, *Principles of Information Security*. Course Technology, 2007, pp. 42.

[3] "Internet of Things (IoT) τι είναι | Διαδίκτυο των πραγμάτων | SAS." [Online]. Available: https://www.sas.com/el_gr/insights/big-data/internet-of-things.html. [Accessed: 23-Jan-2017].

[4] J. Pescatore, "A SANS Analyst Survey," *SANS Inst. InfoSec Read. Room*, 2014.

[5] ITU Corporation, "Internet of Things Global Standards Initiative," *Internet Things Glob. Stand. Initiat.*, vol. 2060, no. July 2015, p. 1, 2015.

[6] Telecommunication Standardization Sector Of ITU, "ITU-T Recommendation database," *Recommendation ITU-T Y.2060*, 2012. [Online]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060. [Accessed: 27-Jan-2018].

[7] N. Sklavos and I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations," in *", IEEE proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaca, Cyprus, November 21-23*, 2016.

[8] N. Sklavos and P. Souras, "Economic Models and Approaches in Information Security for Computer Networks," International Journal of Network Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January 2006. pp. 14-20, 2006.

[9] R. Shirey, "RFC 4949 - Internet Security Glossary, Version 2," *IEFT*, 2007. [Online]. Available: https://tools.ietf.org/pdf/rfc4949.pdf. [Accessed: 15-Oct-2017].

[10] Β. Κάτος and Γ. Στεφανίδης, *Τεχνικές κρυπτογραφιάς και κρυπτανάλυσης*. Zygos, 2003, pp. 126, 12,13,12.

[11] Κ. Λιμνιώτης, *Κρυπτογραφία Διάλεξη 10, Συναρτήσεις κατακερματισμού*. Σημειώσεις μαθήματος Κρυπτογραφίας Ανοικτού Πανεπιστημίου Κύπρου, 2015, pp. 35, 39, 41.

[12] N. Sklavos, "Cryptographic algorithms on A Chip: Architectures, designs & implementation platforms," in *proceedings of the 6th Design and Technology of Integrated Systems in Nano Era (DTIS'11), Greece, April 6-8*, 2011.

[13] Κ. Λιμνιώτης, *Κρυπτογραφία Διάλεξη 8, Τεχνικές Διανομής Κλειδιού – Αλγόριθμοι Δημοσίου*

Κλειδιού: Αλγόριθμος Diffie-Hellman. Σημειώσεις μαθήματος Κρυπτογραφίας Ανοικτού Πανεπιστημίου Κύπρου, 2015, pp. 3.

[14] Κ. Λιμνιώτης, *Κρυπτογραφία Διάλεξη 11, Ψηφιακές Υπογραφές-Ψηφιακά Πιστοποιητικά*. Σημειώσεις μαθήματος Κρυπτογραφίας Ανοικτού Πανεπιστημίου Κύπρου, 2015, pp. 20, 2, 20-31, 28.

[15] Β. Βασιλείου and Σ. Σιαηλής, *Εισαγωγή στην ασφάλεια δικτύων και πληροφοριών 1*. Σημειώσεις μαθήματος Ασφάλεια Υπολογιστών και Δικτύων στο Ανοικτού Πανεπιστημίου Κύπρου, 2014, pp. 45.

[16] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, vol. 19964964. CRC Press, 1996, pp. 41, 42, 191.

[17] "Machine to machine," *Wikipedia The Free Encyclopedia*. [Online]. Available: https://en.wikipedia.org/wiki/Machine_to_machine. [Accessed: 23-Oct-2017].

[18] "Internet of things," *Wikipedia The Free Encyclopedia*. [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things. [Accessed: 23-Oct-2017].

[19] I. D. Zaharakis, N. Sklavos, and A. Kameas, "Exploiting Ubiquitous Computing , Mobile Computing and the Internet of Things to Promote Science Education," in *IEEE* proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaca, Cyprus, November 21-23, 2016.

[20] F. Hu, *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*. CRC Press, 2016, pp. 463, 464, 465, 471, 274, 465 .

[21] N. Sklavos, I. D. Zaharakis, A. Kameas, and A. Kalapodi, "Security & Trusted Devices in the Context of Internet of Things (IoT)," in *IEEE proceedings of 20th EUROMICRO Conference on Digital System Design, Architectures, Methods, Tools (DSD'17), Vienna, Austria, August 30 – September 1*, 2017.

[22] Κ. Λιμνιώτης, *Κρυπτογραφία Διάλεξη 6, Κρυπταλγόριθμοι τμήματος - Αλγόριθμοι DES και 3DES*. Σημειώσεις μαθήματος Κρυπτογραφίας Ανοικτού Πανεπιστημίου Κύπρου, 2015, pp. 2.

[23] Κ. Λιμνιώτης, *Κρυπτογραφία Διάλεξη 7, Κρυπταλγόριθμοι τμήματος: Αλγόριθμος AES – Τρόποι λειτουργίας*. Σημειώσεις μαθήματος Κρυπτογραφίας Ανοικτού Πανεπιστημίου Κύπρου, 2015, pp. 4, 17.

[24] A. Fournaris, P. Kitsos, and N. Sklavos, "Security and Cryptographic Engineering in Embedded Systems," *ResearchGate*, 2013. [Online]. Available: https://www.researchgate.net/publication/287245321_Security_and_Cryptographic_Engineering_in_Embedded_Systems. [Accessed: 14-Dec-2017].

[25] Κ. Λιμνιώτης, *Διάλεξη 5 Κρυπταλγόριθμοι ροής – Τεχνικές κατασκευής*. Σημειώσεις μαθήματος Κρυπτογραφίας Ανοικτού Πανεπιστημίου Κύπρου, 2015, pp. 26.

[26] Κ. Λιμνιώτης, *Κρυπτογραφία Διάλεξη 4, Κρυπταλγόριθμοι ροής: Βασικά χαρακτηριστικά -*

Τυχαιότητα ακολουθιών, 2015, pp. 5, 7, 9.

[27] Κ. Λιμνιώτης, *Κρυπτογραφία Διάλεξη 9, Αλγόριθμος RSA- Κρυπτοσυστήματα ελλειπτικών καμπυλών*. Σημειώσεις μαθήματος Κρυπτογραφίας Ανοικτού Πανεπιστημίου Κύπρου, 2015, pp. 21.

[28] ITU-T, "Security Architectures for Open Systems Interconnection for CCITT Applications X.800," *ITU*, 1991. [Online]. Available: https://www.itu.int/rec/T-REC-X.800-199103-I/en. [Accessed: 30-Oct-2017].

[29] Β. Βασιλείου and Σ. Σιαηλής, *Πρωτόκολλα ασφάλειας 9*. Σημειώσεις μαθήματος Ασφάλεια Υπολογιστών και Δικτύων στο Ανοικτού Πανεπιστημίου Κύπρου, 2014, pp. 11,12,13,14.

[30] Microsoft Developers' Network (MSDN), "'TLS Handshake Protocol.,'" *MSDN*, 2003. [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa380513(v=vs.85).aspx. [Accessed: 28-Jan-2018].

[31] M. Abdur, S. Habib, M. Ali, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, 2017, pp. 388.

[32] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017. pp. 1125–1142, Oct. 2017, pp. 1126, 1127, 1128, 1129, 1130, 1132

[33] F. Bing, "The research of IOT of agriculture based on three layers architecture," in *Proceedings of 2016 2nd International Conference on Cloud Computing and Internet of Things, CCIOT 2016*, 2017, pp. 162–165.

[34] N. Sklavos, R. Chaves, and F. Regazzoni, "Wireless-SoC-Security: FPGA Based System-On-A-Chip Security Schemes for 4G & 5G," in *11th HiPEAC Conference 2016 (HiPEAC'16), Prague, Czech Republic, January 18-20*, 2016.

[35] M. Vivekananda Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in Wireless Sensor Network: A survey," in *2012 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2012*, 2012, pp. 1–3.

[36] N. Sklavos, "On the Hardware Implementation Cost of Crypto-Processors Architectures," ", ", Information Systems Security, The official journal of $(ISC)^2$, A Taylor & Francis Group Publication, Vol. 19, Issue: 2, pp. 53-60, 2010.

[37] S. Uma Maheswari, N. S. Usha, E. A. Mary Anita, and K. Ramaya Devi, "A novel robust routing protocol RAEED to avoid DoS attacks in WSN," in *2016 International Conference on Information Communication and Embedded Systems, ICICES 2016*, 2016, pp. 1–5.

[38] A. Papadimitriou, F. Le Fessant, A. C. Viana, and C. Sengul, "Cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks," *5th IEEE Work. Secur. Netw. Protoc. NPSEC'09*, pp. 43–48, Oct. 2009, pp. 43.

[39] C. Nita-Rotaru, J. Dong, and R. Curtmola, "Secure Routing in Wireless Mesh Networks," in

van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security, Springer, Boston, MA, 2011.

[40] S. Kraijak and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," in *International Conference on Communication Technology Proceedings, ICCT*, 2016, vol. 2016–Febru, pp. 26–31.

[41] A. Capossele, V. Cervo, G. De Cicco, and C. Petrioli, "Security as a CoAP resource: An optimized DTLS implementation for the IoT," in *IEEE International Conference on Communications*, 2015, vol. 2015–Septe, pp. 549–554.

[42] U. M. Colesanti, A. L. Russo, M. Paoli, C. Petrioli, and A. Vitaletti, "Introducing the MagoNode platform," *11th ACM Conf. Embed. Networked Sens. Syst. SenSys 2013*, vol. 2590, pp. 9–10, 2013.

[43] A. N. Bikos and N. Sklavos, "Architecture Design of an Area Efficient High Speed Crypto Processor for 4G LTE," *IEEE Trans. Dependable Secur. Comput.*, vol. 5971, no. c, pp. 1–1, 2016.

[44] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, May 2011.

[45] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *Proceedings - Conference on Local Computer Networks, LCN*, 2012, pp. 956–963.