ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

Τίτλος Πτυχιακής Εργασίας	Ανασκόπηση Ζητημάτων Ασφάλειας Τεχνολογίας 6TiSCH Review of 6TiSCH Technology Security Issues
Ονοματεπώνυμο Φοιτητή	Κωνσταντίνος Κετσετζίογλου
Πατρώνυμο	Αβραάμ Κετσετζίογλου
Αριθμός Μητρώου	Π19068
Επιβλέπων	Χρήστος Δουληγέρης
Συνεργαζόμενος καθηγητής	Απόστολος Καραλής

Ημερομηνία Παράδοσης 26/03/2024

Copyright ©

Περίληψη

Τις τελευταίες δεκαετίες το διαδίκτυο τον πραγμάτων (Internet of Things) έχει γιγαντωθεί. Όχι μόνο επιτρέπει την ασύρματη επικοινωνία συσκευών μεταξύ τους, αλλά της σύνδεσή τους με διακομιστές (servers) και τη χρήση του δικτύου νέφους (cloud networking). Λόγω αυτής της εκθετικής ανάπτυξης του IoT, έχει προβληθεί η λειτουργία αναπήδησης καναλιού με χρονική αυλάκωση (Time-slotted channel hopping) ή εν συντομία TSCH, όντας αξιόπιστη και ενεργειακά αποδοτική σε δίκτυα, ασύρματα κατά βάση, χαμηλής ισχύος. Η παρούσα πτυχιακή εργασία εστιάζει ,κυρίως, στη βιβλιογραφική ανασκόπηση των ζητημάτων ασφαλείας του ειδικού μοντέλου 6TiSCH και την πιθανή αντιμετώπισή τους. Η εργασία ξεκινάει με μία ανασκόπηση των IEEE802.15.4 και IEEE802.15.4 e standards και του τρόπου λειτουργίας του TSCH, εστιάζοντας στις βασικές αρχές του, τον χρονικό συγχρονισμό, τη μεταπήδηση καναλιού και την κατανομή των θυρίδων. Έπειτα εμβαθύνει στο μοντέλο 6TiSCH, τη σημασία του για την υλοποίηση του IPv6 πάνω στο επίπεδο ελέγχου στο TSCH,τα βασικά ζητήματα ασφαλείας που το διέπουν και πιθανές λύσεις στα ζητήματα αυτά. Βάση των βιβλιογραφικών πηγών, γίνεται μία αξιολόγηση των αποτελεσμάτων των πιθανών τρόπων επίλυσης των ζητημάτων ασφαλείας του 6TiSCH και της εφαρμογής της απόδοσης του συνδυασμού της λειτουργίας TSCH με το μοντέλο 6TiSCH.

Λέξεις κλειδιά : Internet of things, IEEE, TSCH, 6TiSCH, IPv6, ασφάλεια

Πίνακας Περιεχομένων

Εισαγωγή

Βάση των πρόσφατων τεχνολογικών εξελίξεων, η διάδοση και η γιγάντωση του Διαδικτύου των πραγμάτων (Internet of Things – IoT) έχει γίνει ευκολότερη, καθώς έχει αυξηθεί η ανάπτυξη τεχνολογιών ασύρματης επικοινωνίας χαμηλής ισχύος και χαμηλού ρυθμού δεδομένων. Σύμφωνα με τον Kevin Ashton [1] το διαδίκτυο των πραγμάτων αναφέρεται στη διασύνδεση των αναγνωριστικών ραδιοσυχνοτήτων στο διαδίκτυο. Το IoT στοχεύει στη διαχείριση ενός υπέρογκου αριθμού έξυπνων ασύρματων συσκευών, που σχηματίζουν μια υποδομή τριχοειδούς δικτύωσης με σκοπό τη σύνδεσή ενός στο διαδίκτυο.

Σημαντικό ρόλο στην υλοποίηση του IoT έχουν τα δίκτυα WSN που αποτελούνται από αισθητήρες (sensors) και ενεργοποιητές (actuators). Η βασική τεχνολογία που χαίρει απαράμιλλης προσοχής για την επίτευξη της σωστής διαχείρισης των ασυρμάτων αυτών συσκευών είναι το πρωτόκολλο Time Scheduled Channel Hopping (TSCH) , το οποίο αποτελεί το κύριο στοιχείου του IEEE802.15.4 προτύπου. Εφόσον το πρότυπο IEEE802.15.4 σχεδιάστηκε για την επίτευξη της ασύρματης επικοινωνίας χαμηλού ρυθμού και μικρής εμβέλειας και η βιομηχανική διαδικασία ελέγχου απαιτεί έναν σημαντικό αριθμό σημείων αίσθησης (sensing points), έχει αρκετές εφαρμογές στον βιομηχανικό αυτοματισμό.

Βασικός στόχος του IoT είναι η σύγκλιση των επιχειρησιακών τεχνολογιών (operational technologies), που βρίσκονται στα βιομηχανικά δίκτυα και παρέχουν αξιόπιστη, ασφαλή και αιτιοκρατική (ντετερμινιστική) δικτύωση με την τεχνολογία της πληροφορίας (information technology), δηλαδή το διαδίκτυο, το οποίο στηρίζεται στην επιλεκτική ουρά και την απόρριψη πακέτων για την επίτευξη του ελέγχου ροής. Η σύγκλιση των δύο τεχνολογιών αυτών στοχεύει στην αξιοποίηση των επιχειρησιακών τεχνολογιών για την επίλυση των προβλημάτων του διαδικτύου [2]. Για τον λόγο αυτό έχει αναπτυχθεί το πρωτόκολλο 6TiSCH.

Το πρωτόκολλο 6TiSCH (Ipv6 over TSCH) έχει προταθεί και αναδειχθεί ως μία σημαντική τεχνολογία για την επίλυση των προκλήσεων της αξιόπιστης επικοινωνίας, της επεκτασιμότητας και της ενεργειακής απόδοσης [3]. Βασικό του στοιχείο είναι η αξιοποίηση του TSCH για να παρέχει μία αιτιοκρατική και αξιόπιστη επικοινωνία σε περιβάλλοντα, όπου οι απαιτήσεις για την καθυστέρηση και την αξιοπιστία είναι απαράμιλλης σημασίας. Επιπλέον η αφομοίωση τεχνολογιών, όπως η 6LoWPAN (Ipv6 over Low-Power Wireless Personal Area Networks), το πρωτόκολλο RPL για τη δρομολόγηση δικτύων χαμηλής ισχύος και απωλειών και το πρωτόκολλο CoAP μεταφοράς περιορισμένης εφαρμογής, επιτρέπει την ενσωμάτωση συσκευών με χαμηλό ενεργειακό κόστος στο διαδίκτυο που βασίζεται στο Ipv6.

Από τη μία μεριά η υιοθέτηση των παραπάνω τεχνολογιών (TSCH, IEEE802.15.4, 6TiSCH, 6LoWPAN, RPL και CoAP) έχει διευκολύνει τη λειτουργία του IoT, από την άλλη έχει εισάγει πληθώρα προκλήσεων ασφαλείας. Τα χαρακτηριστικά των συσκευών που χρησιμοποιείται η τεχνολογία 6TiSCH, είναι συνήθως χαμηλή ισχύος και έχουν περιορισμό στους πόρους, και η δυναμική ανάπτυξη του IoT τα καθιστούν ευάλωτα σε απειλές ασφαλείας. Εφόσον οι τεχνολογίες χρησιμοποιούνται και αφομοιώνονται στη βιομηχανική διαδικασία και στην υγειονομική περίθαλψη, η ανάγκη για ανθεκτικούς μηχανισμούς ασφαλείας τίθεται άκρως σημαντική για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων.

Η παρούσα πτυχιακή εργασία έχει ως στόχο την ανασκόπηση των ζητημάτων ασφαλείας που ενυπάρχουν στα δίκτυα 6TiSCH. Αρχικά δίνεται μία αναφορά των πρωτοκόλλων IEEE802.15.4 και ενός εξέλιξής του IEEE802.15.4e, στη συνέχεια αναλύεται ο τρόπος λειτουργίας του TSCH και το πώς αναδείχθηκε η ανάγκη ανάπτυξης των δικτύων 6TiSCH. Δίνεται εκτενής αναφορά στη λειτουργία και την αρχιτεκτονική του. Μέσω μίας εις βάθος ανάλυσης των προκλήσεων ασφαλείας και των πιθανών λύσεων, η εργασία προσπαθεί να συνδυάσει πληροφορίες για τα δίκτυα 6TiSCH που βρίσκονται διασκορπισμένα σε ένα ενιαίο κείμενο

1. IEEE Standards

Το ινστιτούτο ηλεκτρολόγων και ηλεκτρονικών μηχανικών (Institute for Electrical and Electronics Engineers – IEEE) ενασχολείται με τα επιστημονικά πεδία της μηχανικής, της επιστήμης υπολογιστών (Computer Science) και της τεχνολογίας πληροφοριών (Information Technology). Κύριο μέλημά του είναι η σύνταξη προτύπων για αρκετά είδη βιομηχανιών. Στη συγκεκριμένη περίπτωση, θα μελετηθούν δύο πρότυπα που οδηγούν στο μοντέλο 6TiSCH. Το IEEE802.15.4 και την εξέλιξή του, το IEEE802.15.4e.

1.1 IEEE802.15.4

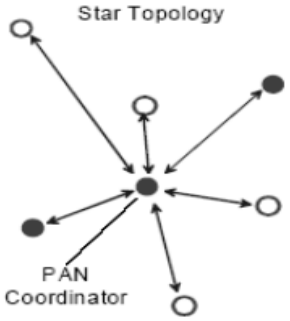
Σύμφωνα με τα [3] και [4], το πρότυπο IEEE802.15.4 δημοσιεύθηκε για πρώτη φορά το 2003 και αποτελεί μέλος της οικογένειας προτύπων IEEE802. Ορίζει το φυσικό επίπεδο (physical layer) και το επίπεδο MAC (MAC layer – Medium Access Control) μίας στοίβας πρωτοκόλλων και θεωρείται το βασικό πρότυπο αναφοράς στα εμπορικά ασύρματα δίκτυα αισθητήρων (Wireless sensor networks – WSNs). Βασικός του στόχος είναι η ενδυνάμωση συσκευών στον τομέα ενός ασύρματης επικοινωνίας σε ένα δίκτυο προσωπικής περιοχής (Personal Area Network – PAN) χαμηλού ρυθμού , χαμηλής ισχύος, όπου γίνεται χρήση μπαταριών διάρκειας έως και 10 έτη, και χαμηλού κόστους.

Αν και το πρότυπο δημιουργήθηκε με στόχο στην απλότητα , εμπεριέχει ένα μεγάλο αριθμό από χαρακτηριστικά ζωτικής σημασίας για μία στιβαρή και αξιόπιστη ασύρματη σύνδεση. Συμπεριλαμβάνει την ταυτοποίηση των ραδιοφώνων του δικτύου μοναδικά, καθώς και τη μέθοδο επικοινωνίας μεταξύ τους. Βέβαια, δεν ασχολείται με την τοπολογία του δικτύου και της διαδικασίας δρομολόγησης. Έχει σχεδιαστεί για επικοινωνίες χαμηλού ρυθμού, δηλαδή ο χρόνος μεταφοράς δεδομένων μεταξύ των συσκευών είναι αμελητέος (κλάσματα του δευτερολέπτου [4]). Συνεπώς, οι συσκευές του δικτύου βρίσκονται κυρίως σε κατάσταση ύπνου (sleep mode), με αποτέλεσμα να υπερτερεί η χαμηλή κατανάλωση ενέργειας. Όσον αφορά την αξιοπιστία του δικτύου, το πρότυπο επιτρέπει στα μηνύματα που μεταφέρονται κατά τη διάρκεια μίας επικοινωνίας των κόμβων να χρησιμοποιήσουν τη λειτουργία της επιβεβαίωσης παραλαβής (ACKnowledgement receipt).

1.1.1 Δίκτυα προσωπικής περιοχής (PAN)

PAN ονομάζονται τα δίκτυα που συνδέουν ηλεκτρονικές συσκευές μέσα σε έναν ατομικό χώρο εργασίας. Βασικό του μέλημα είναι η μεταφορά δεδομένων και η επικοινωνία μεταξύ των συνδεδεμένων συσκευών ,smartphones, υπολογιστές και tablet ή για τη σύνδεση των συσκευών του δικτύου σε ένα άλλο υψηλότερου βαθμού. Για τη δημιουργία ενός PAN απαιτείται ενός συντονιστής PAN που θα επιβλέπει το σύνολο των κόμβων του δικτύου και ενός ή

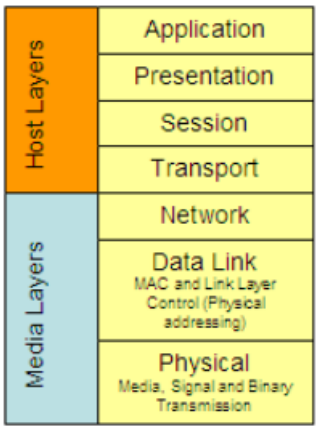
παραπάνω συντονιστών που επιβλέπουν μεμονωμένους κόμβους ή μια ομάδα κόμβων του δικτύου. Ο συντονιστής PAN επιτρέπει την επικοινωνία των κόμβων μεταξύ τους, αν είναι συνδεδεμένοι σε αυτόν. Τα PAN υποστηρίζουν τρεις τοπολογίες δικτύου : τοπολογία πλέγματος (mesh topology) πολλαπλών βημάτων (multi-hop), δένδρου συστάδας (cluster tree) ,αστέρα (star topology) και ενός βήματος (single-hop) (Εικ.1.1).



Εικόνα 1.1: Τοπολογία Αστέρα. Πηγή :An Introduction to IEEE STD 802.15.4 [4]

1.1.2 IEEE802.15.4 και μοντέλο OSI

Όπως όλα τα πρότυπα IEEE , έτσι και το IEEE802.15.4 αναφέρεται και ελέγχει μόνο τα επίπεδα RF, PHYsical και Medium Access Control (MAC) του μοντέλου OSI (Εικ.1.2). Το κανάλι RF παρουσιάζεται ως το φυσικό μέσο (Physical medium) , το PHYsical layer ελέγχει τα χαρακτηριστικά του καναλιού RF και το MAC ελέγχει το PHY. Βέβαια το συγκεκριμένο πρότυπο δεν αναφέρεται ούτε στο επίπεδο δικτύου, αν και βρίσκεται στην οικογένεια των επιπέδων που πραγματεύεται. Κύριος στόχος της εργασίας δεν είναι η πλήρης ανάπτυξη του προτύπου IEEE802.15.4, αλλά χρειάζεται να γίνει αναφορά στα βασικά στοιχεία της αρχιτεκτονικής του προτύπου για την καλύτερη κατανόηση του θέματος.



Εικόνα 1.2 OSI Model
Πηγή :An Introduction to IEEE STD 802.15.4 [4]

Σύμφωνα με τον Adams, το πρότυπο IEEE ορίζει τις παραμέτρους του RF, που περιλαμβάνουν τον τύπο διαμόρφωσης , την κωδικοποίηση, τη διασπορά, το ρυθμό συμβόλου ανά bit και την καναλοποίηση. Το φυσικό επίπεδο (PHYsical layer) ελέγχει όλους του χρόνους μεταφοράς ενός πακέτου μεταξύ των κόμβων, από το χρονισμό σε επίπεδο συμβόλου-bit, τον χρόνο εκπομπής και λήψης του πακέτου, καθώς και τις καθυστερήσεις επιβεβαίωσης. Επίσης, εμπεριέχει

πρωτόκολλα που διαχειρίζονται το κανάλι του ραδιοφώνου και ελέγχουν τη ροή των πακέτων. Χρησιμοποιεί τον αλγόριθμο CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) για την αποφυγή συγκρούσεων μεταξύ των πακέτων που θα οδηγήσουν στην αποτυχία διάδοσης και μεταφοράς του πακέτου δεδομένων.

Για το λόγο αυτό το φυσικό επίπεδο ορίζει 4 πλαίσια: το πλαίσιο δεδομένων, το πλαίσιο επιβεβαίωσης , το πλαίσιο 'φάρος' (beacon) και το πλαίσιο της εντολής MAC. Το πλαίσιο επιβεβαίωσης χρησιμοποιείται από τον κόμβο προορισμό για την επιβεβαίωση της ορθής λήψης του πακέτου στον κόμβο αποστολέα. Το πλαίσιο 'φάρος' χρησιμοποιείται από τους κόμβους για εξοικονόμηση ενέργειας, αλλά και από τον συντονιστή για τη δημιουργία της τοπολογίας του δικτύου. Το πλαίσιο εντολής MAC προσφέρει δυνατότητες αποστολής εντολών χαμηλού επιπέδου μεταξύ κόμβων.

Το επίπεδο MAC του IEEE 802.15.4 έχει καθοριστικό ρόλο στην αποδοτική επικοινωνία εντός των κόμβων του ασύρματου δικτύου. Παρέχει πρόσβαση στα ανώτερα στρώματα του μοντέλου OSI. Μία από τις κύριες λειτουργίες του επιπέδου MAC είναι η δημιουργία των 'φάρων' του δικτύου. Οι ΄φάροι' αποτελούν μέσο ανακάλυψης υπαρχόντων δικτύων από τις συσκευές και μέσο πρόσβασης σε κανάλια κατά τη διάρκεια περιόδων με ή χωρίς ανταγωνισμό. Συνεπώς, είναι απαραίτητοι για τον σωστό συγχρονισμό των δραστηριοτήτων επικοινωνίας εντός του δικτύου.

Επιπλέον, το επίπεδο MAC περιέχει πάνω από 24 πρωτόκολλα που διευκολύνουν τη διαδικασία της μεταφοράς πακέτων δεδομένων, όπως τη διαχείριση του στρώματος ραδιοσυχνοτήτων (RF) και του φυσικού στρώματος (PHY) από οντότητες υψηλότερου επιπέδου. Το επίπεδο MAC εξασφαλίζει την αποτελεσματική και αξιόπιστη ανταλλαγή πληροφοριών μεταξύ των κόμβων εντός του δικτύου, καθώς και την εξοικονόμηση ενέργειας. Εφόσον οι συσκευές σε ένα WSN τροφοδοτούνται κυρίως από μπαταρίες, είναι ιδιαίτερα σημαντικές οι λειτουργίες που παρέχει το επίπεδο αυτό.

Επιπλέον, το στρώμα MAC έχει σχεδιαστεί για να χειρίζεται τη συσχέτιση και την απομόνωση του δικτύου, επιτρέποντας στις συσκευές να εντάσσονται και να αποχωρούν απρόσκοπτα από αυτό ανάλογα με τις ανάγκες που προκύπτουν. Αυτή η ικανότητα είναι σημαντική για τη δυναμική των ασύρματων δικτύων αισθητήρων, όπου οι μεταβαλλόμενες περιβαλλοντικές συνθήκες και οι λειτουργικές απαιτήσεις απαιτούν την είσοδο και την έξοδο συσκευών από το δίκτυο. Συνολικά, το επίπεδο MAC του IEEE 802.15.4 παρέχει ένα ολοκληρωμένο σύνολο χαρακτηριστικών που είναι απαιραίτητο για την αποτελεσματική λειτουργία των ασύρματων δικτύων αισθητήρων.

Από το συγχρονισμό δικτύου και τη μεταφορά δεδομένων έως τη διαχείριση ισχύος και τη χαρτογράφηση συσκευών, το επίπεδο MAC διαδραματίζει κρίσιμο ρόλο στην απρόσκοπτη και αξιόπιστη επικοινωνία των συσκευών σε ένα δίκτυο.

1.1.3 Τεχνικές σύνδεσης

Το πρότυπο IEEE802.15.4 ορίζει 2 μεθόδους (τεχνικές) πρόσβασης καναλιού, τη μέθοδο ενεργοποιημένου 'φάρου' (beacon enabled) και τη μέθοδο μη-ενεργοποιημένου φάρου (non-beacon enabled)[3]. Η πρώτη μέθοδος προσφέρει έναν μηχανισμό διαχείρισης ισχύος βασισμένο σε έναν κύκλο λειτουργίας. Χρησιμοποιεί τη δομή του υπερπλαισίου (Εικ.1.3), που αποτελείται από την ενεργή και την ανενεργή περίοδο, τα όρια της οποίας είναι οι 'φάροι'. Η παράμετρος Beacon Order (σειρά 'φάρων') ορίζει το χρονικό διάστημα μεταξύ δύο 'φάρων' (Beacon Interval).

Οι κόμβοι του υπερπλαισίου αλληλοεπιδρούν με τον συντονιστή τους κατά τη διάρκεια της ενεργής φάσης και μεταβαίνουν σε κατάσταση χαμηλής ισχύος , με στόχο την εξοικονόμηση ενέργειας. Η παράμετρος superframe order (σειρά υπερπλαισίου) ορίζει το μέγεθος ενεργής φάσης (superframe duration). Επιπλέον, το υπερπλαίσιο διαχωρίζεται σε δύο περιοδους, την

περίοδο ελεύθερης διαμάχης (Contention Free Period – CFP) και της περίοδο πρόσβασης διαμάχης (Contention Access Period – CAP).

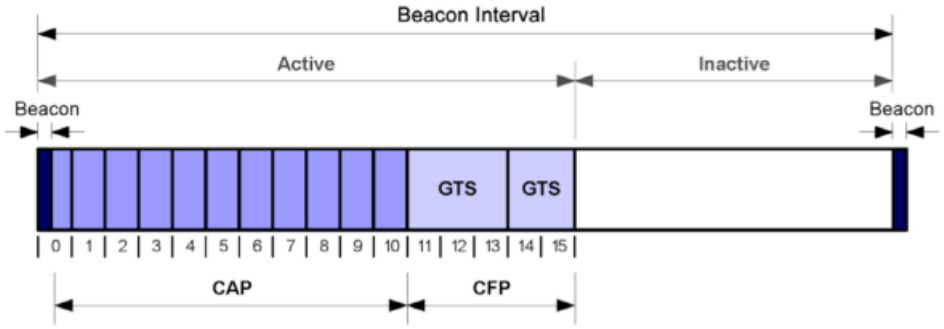


Fig. 1. IEEE 802.15.4 Superframe Structure.

Εικόνα 1.3 : Δομή Υπερπλαισίου στο IEEE802.15.4
Πηγή : IEEE 802.15.4e: A survey [3]

Στην CFP περίοδο χρησιμοποιείται ενας αριθμός προκαθορισμένων χρονοθυρίδων (Guaranteed Time Slots – GTS) για την παροχή επικοινωνίας τύπου διαίρεσης χρόνου πολλαπλής πρόσβασης (Time Division Multiple Access – TDMA). Στην CAP περίοδο χρησιμοποιείται ένας αλγόριθμος CSMA-CA με χρονοθυρίδες για την πρόσβαση στο κανάλι επικοινωνίας.

Αντιθέτως , στη μέθοδο μη-ενεργοποιημένου φάρου δεν υπάρχει υπερπλαίσιο, οι κόμβοι είναι μονίμως ενεργοί, με αποτέλεσμα να υπάρχει τεράστια κατανάλωση ενέργειας και χρησιμοποιείται ένα είδος CSMA-CA αλγορίθμου για πρόσβαση στους διαύλους.

1.1.4 Περιορισμοί του IEEE802.15.4

Έπειτα από τη διαδικασία έρευνας της απόδοσης του προτύπου IEEE802.15.4, έχουν προσδιοριστεί οι εξής ελλείψεις και περιορισμοί [3].

- Απροσδιόριστη καθυστέρηση : Τόσο η μέθοδος Beacon Enabled , όσο και η non-Beacon enabled βασίζονται στον CSMA-CA αλγόριθμο, ο οποίος δεν έχει τη δυνατότητα να θέσει όριο στη μέγιστη καθυστέρηση που βιώνουν τα δεδομένα για να φτάσουν στον τελικό τους προορισμό.
- Επικοινωνία περιορισμένης αξιοπιστίας : Η beacon Enabled μέθοδος παρέχει χαμηλό ποσοστό παράδοσης δεδομένων, εφόσον ο αλγόριθμος CSMA-CA που χρησιμοποιείται είναι ανεπαρκής. Το ίδιο ισχύει και για τη non-Beacon Enabled μέθοδο, όταν υπάρχει μεγάλος αριθμός κόμβων που πρέπει να μεταδοθούν ταυτόχρονα.
- Απουσία προστασίας από παρεμβολές και εξασθένιση : Το IEEE802.15.4 MAC πρωτόκολλο χρησιμοποιεί ένα μόνο κανάλι και δεν έχει εσωτερικούς μηχανισμούς αναπήδησης συχνοτήτων για να απαλύνει τις επιπτώσεις των παρεμβολών και της εξασθένισης πολλαπλών διαδρομών. Ως εκ τούτου το δίκτυο είναι ασταθές και μπορεί να καταρρεύσει.
- Τροφοδοτούμενοι κόμβοι αναμετάδοσης : Οι τοπολογίες πολλαπλών βημάτων (multi-hop topologies) στη beacon enabled μέθοδο απαιτούν πολύπλοκους μηχανισμούς συγχρονισμού και προγραμματισμού των ‘φάρων΄, λειτουργία που δεν υπάρχει στο υπάρχον πρότυπο. Οι ενδιάμεσοι κόμβοι αναμετάδοσης κρατούν το ραδιόφωνο

ανοιχτό, με αποτέλεσμα μεγάλη κατανάλωση ενέργειας.

1.2 IEEE802.15.4e

Λόγω των παραπάνω περιορισμών, το IEEE διαμόρφωσε μία ομάδα εργασίας (work group – WG), η οποία κυκλοφόρησε την εξέλιξη του IEEE802.15.4 , το πρότυπο IEEE802.15.4e. Ο στόχος του συγκεκριμένου work group είναι ο προσδιορισμός ενός πρωτοκόλλου MAC πολλαπλών βημάτων και χαμηλής ενέργειας με σκοπό την αντιμετώπιση των μείζονων ζητημάτων αρκετών εφαρμογών , κυρίως βιομηχανικών. Ως αποτέλεσμα της δουλειάς του IEEE802.15.4e WG ήταν η δημιουργία του προτύπου βελτίωσης IEEE802.15.4e MAC.

Σύμφωνα με το άρθρο [5] το πρότυπο IEEE802.15.4e παρέχει βελτιώσεις μόνο στο υπόστρωμα MAC, δεν ασχολείται καθόλου με το φυσικό επίπεδο και το επίπεδο ασφαλείας. Όπως και με τον προκάτοχό του, έτσι και το πρότυπο IEEE802.15.4e δεν προτείνει κάποια τεχνική επαλήθευσης προς υλοποίηση, παρά μόνο θέτει τον αλγόριθμο κρυπτογράφησης για τα δεδομένα προς μεταφορά. Το βελτιωμένο αυτό πρότυπο επεκτείνει το προγενέστερό του εφαρμόζοντας τρόπους συμπεριφοράς του υποστρώματος MAC και βελτιώσεις σε ορισμένες λειτουργίες.

1.2.1 Βελτιώσεις Λειτουργιών

Βάση των άρθρων [5], [6] και [7] το πρότυπο IEEE802.15.4e φέρει τις παρακάτω βελτιώσεις λειτουργιών.

1. Πολυκαναλική πρόσβαση (Multi-channel access): Σε σχέση με το προγονικό πρότυπο που υποστηρίζει επικοινωνία μέσω ενός καναλιού, το IEEE802.15.4e παρέχει στο δίκτυο πολυκαναλική πρόσβαση, η οποία μετριάζει τη μείωση της απόδοσης του δικτύου λόγω παρεμβολών. Μέσω της αναπήδησης μεταξύ καναλιών (channel hopping) και της προσαρμογής καναλιού (channel adaptation) των μεθόδων TSCH (Time Schedule Channel Hopping) και DSME (Deterministic Synchronous Multichannel Extension) αντίστοιχα παρέχεται στους κόμβους η δυνατότητα να έχουν πρόσβαση και σε άλλα κανάλια.
2. Στοιχεία Πληροφορίας (Information Elements): Αν και τα στοιχεία πληροφορίας προϋπήρχαν και στο πρότυπο IEEE802.15.4, στο εξελιγμένο έχουν περισσότερες λειτουργίες. Είναι ένας επεκτάσιμος μηχανισμός ανταλλαγής πληροφορίας στο υπόστρωμα MAC. Στη μέθοδο TSCH περιέχει πληροφορίες σχετικά με το μέγεθος της χρονοθυρίδας, το ID της και την ακολουθία αναπήδησης καναλιών.
3. Χαμηλή ενέργεια (Low Energy): Το εξελιγμένο πρότυπο IEEE802.15.4e στοχεύει κυρίως σε εφαρμογές που επιτρέπουν το αντιστάθμισμα μεταξύ της καθυστέρησης μεταφοράς (latency) με την ενεργειακή αποδοτικότητα. Επιπλέον, και αρκετά σημαντικό για τη σωστή λειτουργία του διαδικτύου των πραγμάτων , επιτρέπει στους κόμβους του δικτύου να λειτουργούν με αρκετά χαμηλό κύκλο λειτουργίας (duty cycle), ενώ ταυτόχρονα φαίνονται και ενεργοί στα υψηλότερα στρώματα.
4. Πλαίσια πολλαπλών χρήσεων (Multipurpose frames): Το πρότυπο IEEE802.15.4e εφοδιάζει το δίκτυο με ένα ευέλικτο πλαίσιο που έχει τη δυνατότητα να αντιμετωπίσει ένα μεγάλο αριθμό διεργασιών MAC.
5. Βελτιωμένοι ‘φάροι’ (Enhanced Beacons – EBs): Το εξελιγμένο πρότυπο αναθεωρεί τη λειτουργία των ‘φάρων’ στα δίκτυα. Προσφέρει μεγαλύτερη ευελιξία, εφόσον επιτρέπει στη δημιουργία ειδικών πλαισίων για διαφορετικές εφαρμογές, τα οποία εμπεριέχουν σχετικά στοιχεία πληροφορίας. Οι EBs διακρίνονται από τους ΄φάρους’ της προηγούμενης έκδοσης βάση των πληροφοριών πλαισίου που τους δίνει ο συντονιστής

PAN. Περιέχουν πληροφορίες σχετικά με το αν είναι ενεργοποιημένα τα TSCH/DSME, η χαμηλή ενέργεια και σχετικά με τις αντίστοιχες ακολουθίες channel hopping.

6. Μετρήσεις απόδοσης MAC : Το εξελιγμένο πρότυπο της IEEE υποστηρίζει την ανατροφοδότηση των επιδόσεων του δικτύου στα ανώτερά του στρώματα μέσω των μετρήσεων απόδοσης MAC. Παρέχουν πληροφορίες σχετικά με την ποιότητα του καναλιού, όπως η απόδοση σύνδεσης, οι οποίες συνδράμουν το επίπεδο δικτύου στη λήψη αποφάσεων δρομολόγησης, μειώνοντας τη συνολική κατανάλωση ενέργειας και την καθυστέρηση του δικτύου. Οι πληροφορίες που ασχολούνται οι μετρήσεις απόδοσης είναι οι εξής :
    a. Ο αριθμός μεταδιδόμενων πλαισίων που απαιτούν μία ή περισσότερες προσπάθειες πριν από την επιβεβαίωση.
    b. Ο αριθμός μεταδιδόμενων πλαισίων που δεν οδήγησαν σε επιβεβαίωση μετά την περίοδο macMaxFrameRetries.
    c. Ο αριθμός μεταδιδόμενων πλαισίων που αναγνωρίστηκαν σωστά κατά την αρχική μετάδοση του πλαισίου δεδομένων.
    d. Ο αριθμός λαμβανομένων πλαισίων που απορρίφθηκαν λόγω ζητημάτων ασφαλείας.
7. Γρήγορη ένωση (Fast Association – FastA) : Ο μηχανισμός γρήγορης ένωσης του προτύπου IEEE802.15.4e επιτρέπει στον κόμβο να αιτηθεί για ένωση από τον συντονιστή PAN. Στην περίπτωση διαθέσιμων πόρων , ο συντονιστής PAN εκχωρεί μία σύντομη διεύθυνση στον κόμβο και αποστέλλει μία απάντηση σύνδεσης που περιέχει τη διεύθυνση αυτή και μία ένδειξη κατάστασης. Ως εκ τούτου, ο μηχανισμός FastA επιτρέπει στη γρήγορη ένωση των κόμβων στο δίκτυο.

1.2.2 Τρόποι Συμπεριφοράς MAC

Σύμφωνα με τον De Guglielmo κ.α. [3] το πρότυπο IEEE802.15.4e ορίζει πέντε καινούριους τρόπους συμπεριφοράς του Medium Access Control. Στο κεφάλαιο αυτό γίνεται μια σύντομη αναφορά και στους πέντε, ενώ στο επόμενο γίνεται εκτενής ανάλυση της λειτουργίας TSCH, στην οποία στοχεύει και η συγκεκριμένη εργασία.

Α. Χρονοπρογραμματισμένη αναπήδηση καναλιού (Time Scheduled/Slotted Channel Hopping – TSCH): Η συμπεριφορά TSCH απευθύνεται σε τομείς εφαρμογών όπως ο βιομηχανικός αυτοματισμός και ο έλεγχος διεργασιών, παρέχοντας υποστήριξη για πολυπλεγμένες και πολυκαναλικές επικοινωνίες, μέσω της προσέγγισης Πολλαπλής Πρόσβασης με Διαίρεση Χρόνου (Time Division Multiple Access – TDMA). Η προσέγγιση αυτή επιτρέπει στους κόμβους να μοιράζονται το ίδιο κανάλι συχνότητας διαιρώντας το σήμα σε διαφορετικές χρονοθυρίδες και χρησιμοποιείται κυρίως στην ψηφιακή κυψελοειδή τηλεφωνία και την κινητή ραδιοεπικοινωνία [8].

Β. Ντετερμινιστική και παράλληλη επέκταση πολλαπλών καναλιών (Deterministic and Synchronous Multi-Channel Extension – DSME): Στόχος της συμπεριφοράς DSME είναι η υποστήριξη εφαρμογών υψηλών απαιτήσεων για έγκαιρη και αξιόπιστη ενημέρωση στον εμπορικό και βιομηχανικό τομέα. Για την υλοποίηση του στόχου αυτού, συνδυάζεται η πρόσβαση στα μέσα με βάση τον ανταγωνισμό και τον διαμοιρασμό του χρόνο , ενώ παρέχονται και δύο διαφορετικοί τρόποι ποικιλομορφίας καναλιού.

Γ. Ντετερμινιστικό δίκτυο χαμηλής καθυστέρησης (Low Latency Deterministic Network – LLDN): Η συμπεριφορά LLDN έχει διαμορφωθεί για δίκτυα μονοκαναλικά και μονής διαδρομής. Εφαρμόζεται σε εργοστασιακούς προγραμματισμούς , όπου η καθυστέρηση απαιτείται να είναι αρκετά χαμηλή.

Δ. Ασύγχρονη προσαρμογή πολλαπλών καναλιών (Asynchronous multi-channel adaptation – AMCA): Η συγκεκριμένη συμπεριφορά MAC στοχεύει σε τομείς εφαρμογών, που χρήζουν μεγάλης έκτασης, όπως τα δίκτυα παρακολούθησης υποδομών. Η συμπεριφορά AMCA

χρησιμοποιείται μόνο από non-beacon Enabled δίκτυα προσωπικής περιοχής. Κάθε κόμβος, ή αλλιώς συσκευή, επιλέγει το κανάλι με την καλύτερη ποιότητα σύνδεσης, καθορισμένη από το κανάλι ακρόασης, και αρχίζει την ακρόαση στη συγκεκριμένη συχνότητα. Οι συσκευές έχουν τη δυνατότητα να ανταλλάσσουν πληροφορίες μέσω των καναλιών ακρόασης που τους έχουν ανατεθεί, ζητώντας μεταδόσεις ‘φάρου’ (beacon transmissions) ή στέλνοντας ειδικά πακέτα τύπου «Hello».

Ε. Αναγνώριση Ραδιοσυχνότητας Blink (Radio Frequency Identification Blink – BLINK): Η συμπεριφορά BLINK προορίζεται για εφαρμογές όπως η αναγνώριση προσώπου ή/και αντικειμένου, ο εντοπισμός θέσης (GPS) και η παρακολούθηση. Μία συσκευή μπορεί να μεταβιβάσει το αναγνωριστικό της σε άλλες χωρίς να απαιτείται καμία προηγούμενη συσχέτιση ή επαλήθευση. Τα πακέτα BLINK αποστέλλονται συνήθως μέσω του πρωτοκόλλου Aloha.

Το πρότυπο IEEE802.15.4e στοχεύει κυρίως στις τρεις πρώτες συμπεριφορές MAC (TSCH, DSME και LLDN), των οποίων τα βασικά χαρακτηριστικά εμφανίζονται στον Πίνακα I [3].

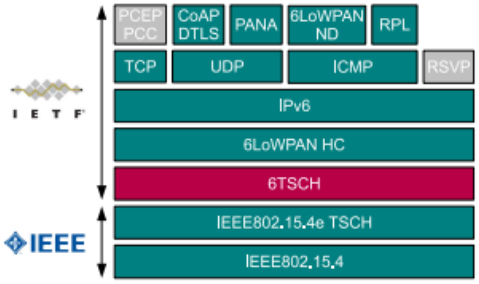
Πίνακας I – Βασικά Χαρακτηριστικά TSCH,DSME και LLDN

	TSCH	DSME	LLDN
‘Φάροι’	Ναι (EBs)	Ναι (EBs)	Ναι
Οργάνωση Χρόνου	Περιοδικό slotframe : Αυθαίρετος αριθμός χρονοθυρίδων και αποκλειστικές/διαμοιρασμένες χρονοθυρίδες	Περιοδικό Υπερπλαίσιο	Περιοδικό Υπερπλαίσιο
Πρόσβαση Καναλιού	TDMA, TSCH-CA	Βάση ανταγωνισμού, βάση χρόνου	Βάση χρόνου, LLDN CSMA-CA
Τοπολογίες	Αστέρα, δέντρου, πλέγματος	Αστέρα, δέντρου, πλέγματος	Μόνος αστέρα
Πολυκαναλικοί Μηχανισμοί	Αναπήδηση καναλιού	Αναπήδηση καναλιού, προσαρμογή καναλιού	Όχι
Μηχανισμός προγραμματισμού χρονοθυρίδας	Δεν αναφέρεται	Κατανεμημένος	Συγκεντρωτικός
Group ACKs	Όχι	Ναι	Ναι
Συγχρονισμός Δικτύου	Συγχρονισμός βάσης πλαισίου	Κατά την υποδοχή του EB	Κατά την υποδοχή του ‘φάρου’

2. Time Scheduled Channel Hopping (TSCH)

Σύμφωνα με το προηγούμενο κεφάλαιο η ομάδα εργασίας IEEE802.15.4e όρισε την τεχνολογία TSCH ως τρόπο συμπεριφοράς τους υποστρώματος MAC. Η συμπεριφορά TSCH είναι μία λύση τελευταίας τεχνολογίας για αξιόπιστη και χαμηλής ισχύος δικτύωση σε δίκτυα χαμηλής ισχύος και απώλειας (Low power and Lossy Networks – LLNs) και στοχεύει , σύμφωνα με τα άρθρα [9] και [10], στην υποστήριξη εφαρμογών αυτοματοποιημένων διαδικασιών, όπως η διαδικασία παραγωγής πετρελαίου ή τροφίμων/ποτών, με ιδιαίτερη έμφαση στην παρακολούθηση συσκευών.

Η τεχνολογία TSCH συνδυάζει τη χρονομετρημένη πρόσβαση (time-slotted access) με τις δυνατότητες πρόσβασης πολλαπλών καναλιών (multi-channel access) και μεταπήδησης καναλιών (channel-hopping). Η πρόσβαση μέσω ενός χρονοδιαγράμματος αυξάνει την απόδοση (throughput) του συστήματος με την αποφυγή συγκρούσεων μεταξύ ανταγωνιστικών κόμβων και παρέχει αιτιοκρατική καθυστέρηση στις εφαρμογές. Η πολυκαναλική πρόσβαση, από την άλλη, προσφέρει τη δυνατότητα σε μεγαλύτερο αριθμό κόμβων να ανταλλάσσουν πλαίσια ταυτόχρονα με τη χρήση διαφορετικής μετατόπισης καναλιού (channel-offset). Η μεταπήδηση καναλιού, επίσης, βελτιώνει την αξιοπιστία της επικοινωνίας, εφόσον περιορίζει τις επιπτώσεις των παρεμβολών και της εξασθένισης πολλαπλών διαδρομών. Συνεπώς, η χρονοπρογραμματισμένη αναπήδηση καναλιού παρέχει αυξημένη χωρητικότητα, υψηλή αξιοπιστία και προβλέψιμη καθυστέρηση στο δίκτυο, ενώ διατηρεί χαμηλό κύκλο λειτουργίας χάρη στη λειτουργία της χρονισμένης πρόσβασης (timed access mode) [10].

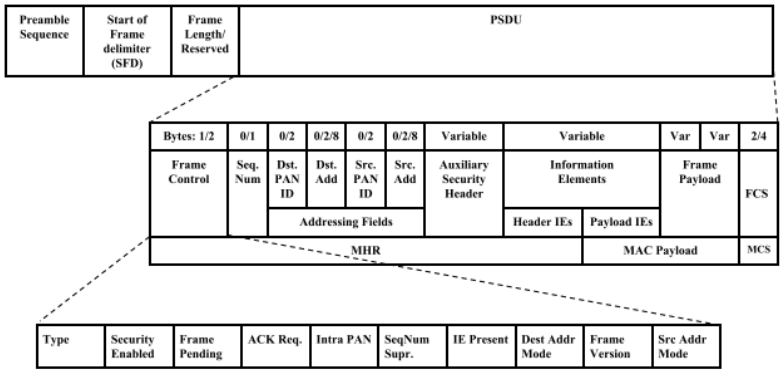


Εικόνα 2.1 : Στοίβα πρωτοκόλλων IPv6-Enabled για LLNs.
Πηγή : IETF 6TSCH: Combining IPv6 Connectivity with Industrial Performance [9]

Η συμπεριφορά TSCH υποστηρίζει όλα τα είδη τοπολογιών δικτύου (αστέρα, δένδρου, μερικού ή πλήρους πλέγματος) και η λειτουργία της παραμένει αμετάβλητη ανεξαρτήτως της επιλεγμένης κατά περίπτωση τοπολογίας του δικτύου. Τονίζεται ότι είναι ιδιαίτερα κατάλληλη για δίκτυα πολλαπλών βημάτων, όπου η μεταπήδηση συχνότητας επιτρέπει την αποτελεσματική χρήση των διαθέσιμων πόρων.

Αρχικά χρειάζεται να γίνει μια μικρή αναφορά στη δομή του πακέτου που αφορά το TSCH και κατ' επέκταση την τεχνολογία 6TiSCH. Βάση του Vilajosana και του IEEE WG έχει σχεδιαστεί το πακέτο για τη διευκόλυνση των λειτουργιών που παρέχει στο TSCH (Εικ2.2). Στο πεδίο ελέγχου

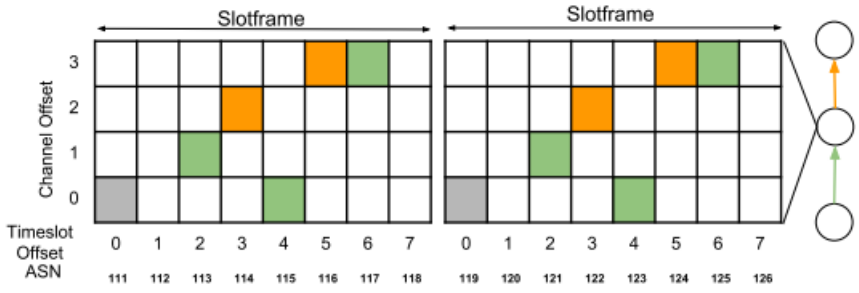
πλαισίου (Frame Control Field – FCF) γίνεται η διαμόρφωση των κύριων χαρακτηριστικών του πλαισίου, όπως η ύπαρξη ασφάλειας, η ύπαρξη στοιχείων πληροφορίας και η έκδοση του πακέτου. Στη συνέχεια υπάρχει το πλαίσιο στοιχείου πληροφορίας (Information element field), στο οποίο αποθηκεύεται πληροφορία σχετική με την επικοινωνία μεταξύ των κόμβων του δικτύου.



Εικόνα 2.2: Επικεφαλίδα MAC ενός πλαισίου IEEE802.15.4 TSCH.
Πηγή : IETF 6TiSCH: A Tutorial [10]

2.1 Περιγραφή λειτουργίας TSCH

Σύμφωνα με τη μελέτη [10], ως βασική δομή το TSCH χρησιμοποιεί το πλαίσιο χρονοθυρίδας, το οποίο ορίζει τον διαχωρισμό του χρόνου σε χρονοθυρίδες, οι οποίες επαναλαμβάνονται με την πάροδο του χρόνου. Κάθε χρονοθυρίδα (timeslot) έχει τη δυνατότητα χρησιμοποίησης ενός συνόλου διαθέσιμων συχνοτήτων, με αποτέλεσμα τη δημιουργία ενός χρονοδιαγράμματος που μοιάζει με πίνακα(Εικ.2.3). Ο πίνακας αυτός αντιπροσωπεύει τις πιθανές επικοινωνίες μεταξύ ενός κόμβου με άλλους γειτονικούς και διαχειρίζεται από μία συνάρτηση χρονοπρογραμματισμού (Scheduling Function).



Εικόνα 2.3 : Παράδειγμα χρονοδιαγράμματος TSCH
Πηγή : IETF 6TiSCH: A Tutorial [10]

Κάθε κελί στον πίνακα προσδιορίζεται από τις συντεταγμένες της μετατόπισης της θέσης (slot-offset) και της μετατόπισης καναλιού (channel offset). Η μετατόπιση της θέσης ενός κελιού υποδεικνύει τη θέση του στον χρόνο σε σχέση με την έναρξη του πλαισίου, ενώ η μετατόπιση καναλιού δείχνει την αντιστοίχιση μίας συχνότητας σε κάθε επανάληψη του πλαισίου χρονοθυρίδας, με αποτέλεσμα η ανταλλαγή πακέτων μεταξύ γειτόνων να πραγματοποιείται εντός ενός κελιού. Ο απόλυτος αριθμός θυρίδας (Absolute Slot Number – ASN) δείχνει τον αριθμό των θυρίδων από την έναρξη λειτουργίας του δικτύου και αυξάνεται κατά μία μονάδα σε

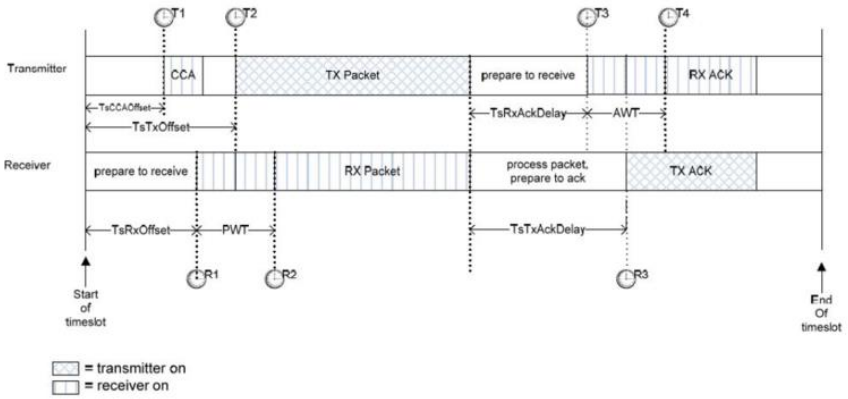
κάθε αλλαγή θυρίδας.

2.1.1 Δομή Πλαισίου

Στη λειτουργία TSCH , κάθε κόμβος λαμβάνει πληροφορίες συγχρονισμού, μεταπήδησης καναλιού, χρονοθυρίδων και πλαισίων θυρίδων από τα πλαίσια Enhanced Beacons (Κεφ.1.2.1), τα οποία αποστέλλονται περιοδικά από άλλους κόμβους του δικτύου με στόχο τη διαφήμισή του. Μόλις ένας κόμβος λάβει έναν έγκυρο Enhanced Beacon , εκείνος με τη σειρά του μπορεί να συγχρονιστεί με το δίκτυο , να αρχικοποιήσει το πλαίσιο χρονοθυρίδας και να ξεκινήσει τη μετάδοση τον δικών του 'φάρων'. Στη συνέχεια τα πλαίσια θυρίδας επαναλαμβάνονται αυτόματα με βάση τον κοινό συγχρονισμό των κόμβων και δεν απαιτείται κάποιος 'φάρος' για την έναρξη της επικοινωνίας.

Κάθε χρονοθυρίδα επιτρέπει σε έναν κόμβο να στείλει ένα πλαίσιο δεδομένων μεγίστου μεγέθους και να λάβει την αντίστοιχη επιβεβαίωση. Εάν δεν ληφθεί καμία επιβεβαίωση εντός ενός προκαθορισμένου χρονικού ορίου, η αναμετάδοση του πλαισίου δεδομένων αναβάλλεται μέχρι την επόμενη χρονοθυρίδα που ανατίθεται στο ζεύγος αποστολέα και προορισμού. Η συγκεκριμένη διαδικασία γίνεται περισσότερο κατανοητή με την εικόνα 2.4.

Σύμφωνα με της πληροφορίες που προσφέρει η εικόνα 2.4 και το άρθρο [10], εντός της χρονοθυρίδας υπάρχουν το πολύ τέσσερα χρονικά όρια που χρησιμοποιούνται από τον κόμβο αποστολέα-πομπού. Το χρονικό όριο διακοπής T1 προγραμματίζεται τη στιγμή που η καθαρή εκτίμηση καναλιού (Clear Channel Assessment – CCA) χρειάζεται να γίνει (TsCCAOffset), αν και είναι προαιρετική. Η διακοπή T2 συμβαίνει τη στιγμή μετάδοσης του πακέτου (TsTxOffset), ώστε το ραδιόφωνο να έχει τη δυνατότητα μετάδοσης. Η χρονική διακοπή T3 είναι προγραμματισμένη, ώστε να ξεκινήσει να ακούει για πλαίσια επιβεβαίωσης σε μία σχετική χρονική μετατόπιση μετά τη λήψη του συμβάντος τέλους του πλαισίου(TsRxAckDelay). Τέλος η χρονοδιακοπή T4 απαιτείται για να περιοριστεί ο χρόνος που ο ασύρματος συνεχίζει να ακούει. Από την πλευρά του δέκτη, η διακοπή R1 καθορίζει τη χρονική στιγμή που ο ασύρματος ενεργοποιείται (TsRxOffset). Η χρονοδιακοπή R2 θέτει τον χρόνο που το ραδιόφωνο διατηρεί την ακρόαση σε περίπτωση που δεν λάβει κάποιο πακέτο. Η τελευταία διακοπή R3 λαμβάνει χώρα μετά τη λήψη του πακέτου, ώστε να μεταδοθεί η επιβεβαίωση λήψης του σε ακριβή χρονικό περιθώριο (TsTxDelay).



Εικόνα 2.4 : Χρονοδιάγραμμα χρονοθυρίδας TSCH
Πηγή : IETF 6TiSCH: A Tutorial [10]

2.1.2 Συγχρονισμός και αναπήδηση καναλιού

Το TSCH έχει ως βασικό του μέλημα τη διαδικασία συγχρονισμού μεταξύ ενός κόμβου και των χρονικών γειτόνων του. Η συγκεκριμένη διαδικασία ονομάζεται επικοινωνία ανά ζεύγη (pairwise communication) και παρέχει δύο είδη συγχρονισμού, τον συγχρονισμό βάση πακέτων (packet-based synchronization) και τον συγχρονισμό βάση επιβεβαιώσεων (acknowledgement-based synchronization).

Κατά την πρώτη περίπτωση, ο κόμβος αποστολέας αποστέλλει τα πακέτα στους δέκτες του κατά τη χρονική στιγμή TsTxOffset, όπως φαίνεται στην Εικόνα 2.3. Μόλις ο κόμβος δέκτης λάβει το απεσταλμένο πακέτο χρονοσημαίνει τη λήψη του πρώτου bit και υπολογίζει τη διαφορά χρόνου μεταξύ χρόνου λήψης και του TsTxOffset, ο οποίος αναφέρεται στον ιδανικό χρόνο λήψης. Με αυτόν τον τρόπο, ο κόμβος αποστολέας σε περίπτωση σφάλματος συγχρονισμού μπορεί να μεγαλώσει ή και να μικρύνει, αναλόγως των περιπτώσεων, τη διάρκεια της χρονοθυρίδας για να το επανορθώσει.

Σχετικά με το δεύτερο είδος συγχρονισμού, ο συγχρονισμός βάση επιβεβαίωσης λειτουργεί κατά βάση όπως και ο συγχρονισμός βάση πακέτων, αλλά τα σφάλματα του συγχρονισμού αποστέλλονται στο πεδίο του πλαισίου επιβεβαίωσης. Ο κόμβος παραλήπτης στέλνει το πλαίσιο επιβεβαίωσης στον αποστολέα και εκείνος με τη σειρά του χρονοσημαίνει τη χρονική στιγμή που λαμβάνει το πλαίσιο. Ο γείτονας βάση χρόνου δείχνει το σφάλμα συγχρονισμού σε ένα στοιχείο πληροφορίας στην επιβεβαίωση που στέλνει πίσω. Όπως και στην προηγούμενη περίπτωση, ο κόμβος ‘παιδί’ αντισταθμίζει το σφάλμα με τη διαχείριση διάρκειας της τρέχουσας χρονοθυρίδας.

Ένας από τους βασικούς λόγους που χρησιμοποιείται η μέθοδος TSCH είναι η υποστήριξη της πολυκαναλικής επικοινωνίας βασισμένη στην εναλλαγή καναλιών. Κάθε επικοινωνία έχει έως και δεκαέξι διαφορετικά κανάλια διαθέσιμα για την επίτευξή της. Βέβαια, λόγω κακής ποιοτικά επικοινωνίας ο αριθμός των διαθέσιμων καναλιών μπορεί να μειωθεί , εφόσον οι συχνότητές τους αποκλειστούν από το δίκτυο. Όπως φαίνεται και στην εικόνα 2.3 τα κανάλια προσδιορίζονται από το ChannelOffset.

Το TSCH ορίζει τη σύνδεση μεταξύ των κόμβων ως μία κατανομή ανά ζεύγη κατευθυνόμενης επικοινωνίας μεταξύ κόμβων σε μία συγκεκριμένη χρονοθυρίδα σε ένα καθορισμένο Channeloffset. Η σύνδεση αυτή αναπαρίσταται από ένα ζεύγος ανάμεσα σε ένα πλαίσιο θυρίδας (SlotOffset) και ένα ChannelOffset ([n, ChannelOffset]). Η συχνότητα f για την επικοινωνία στη χρονοθυρίδα n υπολογίζεται από την Εξίσωση 1, όπου ASN είναι ο απόλυτος αριθμός θυρίδας, το Nchannels το σύνολο των διαθέσιμων καναλιών και F η συνάρτηση που υλοποιείται ως πίνακας αναζήτησης.

$$f = F[(ASN + ChannelOffset)\%Nchannels] \quad (1)$$

Η πολυκαναλική επικοινωνία επιτρέπει την ύπαρξη πολλαπλών ταυτόχρονων επικοινωνιών σε μία χρονοθυρίδα, εφόσον χρησιμοποιείται διαφορετικό ChannelOffset. Βάση της παραπάνω εξίσωσης επιστρέφεται διαφορετική συχνότητα για την ίδια σύνδεση σε διαφορετική χρονοθυρίδα, πράγμα που επισφραγίζει τη χρήση όλων των διαθέσιμων καναλιών για την επικοινωνία εντός της σύνδεσης. Με αυτόν τον τρόπο μειώνονται οι καταστρεπτικές επιπτώσεις στη σύνδεση, λόγω εξωτερικών παρεμβολών.

2.1.3 Αποφυγή Συγκρούσεων

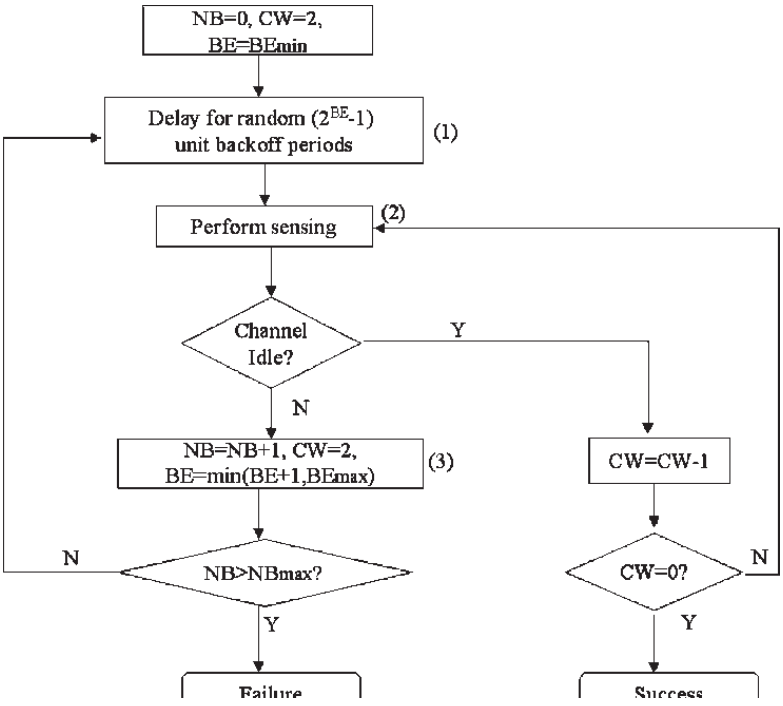
Η πολλαπλή ταυτόχρονη επικοινωνία εντός μία χρονοθυρίδας, αν και μειώνει τα προβλήματα εξωτερικών παρεμβολών στο δίκτυο, μπορεί να προκαλέσει συγκρούσεις και να δημιουργήσει σφάλματα στη μετάδοση των πακέτων κατά τη διαδικασία της επικοινωνίας μεταξύ δύο κόμβων. Για να ελαττωθεί ο αριθμός των συγκρούσεων αυτών, το IEEE802.15.4e WG όρισε τον αλγόριθμο αναμετάδοσης πολλαπλής πρόσβασης αίσθησης φορέα με αποφυγή σύγκρουσης (CSMA/CA), ο οποίος είναι απλοϊκός και αποδίδει αποδοτικά.

Ο αλγόριθμος CSMA/CA λειτουργεί ως εξής [11] :

1. Ανίχνευση φορέα : Πριν από κάθε μετάδοση δεδομένων, μία συσκευή που χρησιμοποιεί τον αλγόριθμο ακούει πρώτα το κανάλι για να δει αν είναι ελεύθερο.
2. Πολλαπλή πρόσβαση : Όταν ένα κανάλι γίνεται ανενεργό, η συσκευή περιμένει έναν τυχαίο τρόπο επαναφοράς (backoff). Έτσι, μειώνεται η πιθανότητα συγκρούσεων μεταξύ συσκευών που επιχειρούν ταυτόχρονη μετάδοση δεδομένων.
3. Αποφυγή συγκρούσεων : Αφού παρέλθει ο χρόνος επαναφοράς, η συσκευή εκτελεί μία αξιολόγηση ελεύθερου καναλιού (Clear Channel Assessment – CCA) για να ελέγξει αν το κανάλι είναι ακόμη ελεύθερο. Στην περίπτωση που είναι κατειλημμένο, η συσκευή αυξάνει τον εκθέτη επαναφοράς (backoff exponent – BE) και επαναλαμβάνει τη διαδικασία. Στην περίπτωση, όμως, που το κανάλι είναι ελεύθερο, η συσκευή συνεχίζει τη μετάδοση δεδομένων στο δίκτυο.
4. Αποστολή: Εάν το CCA είναι επιτυχής, η συσκευή αποστέλλει το πακέτο. Μετά την αποστολή το BE επανέρχεται στην αρχική τιμή.

Ένας ψευδοαλγόριθμος για τον CSMA/CA προκύπτει από το άρθρο [10]:

1. Αρχικοποίηση μεταβλητών αριθμού επαναποστολής (NB = 0) και εκθέτη επαναφοράς (BE = macMinBE).
2. Τυχαίος αριθμός $0 \leq w \leq 2^{BE} - 1$.
3. Η αναμετάδοση του πλαισίου αναβάλλεται για w συνδέσεις με προορισμό τον κόμβο r, ή μέχρι να βρεθεί αποκλειστική σύνδεση με προορισμό τον κόμβο αυτό.
4. Αν η αναμετάδοση γίνει σε κοινόχρηστη σύνδεση και επιτύχει , τότε BE = macMinBE και ο αλγόριθμος τερματίζει.
5. Αν η αναμετάδοση δεν επιτυγχάνεται , τότε NB = NB + 1 kai BE = min(BE + 1, macMinBE).
6. Αν ο αριθμός αναμεταδόσεων έχει υπερβεί την επιτρεπόμενη τιμή (NB > macMaxFrameRetries), το πλαίσιο απορρίπτεται και ο αλγόριθμος επιστρέφει στο βήμα 2.



Εικόνα 2.5 : Ψευδοαλγόριθμος CSMA/CA
Πηγή : Performance Analysis of IEEE 802.15.4[12]

2.2 Απόδοση TSCH

Ο Watteyne κ.α. παρουσιάζουν στο άρθρο τους ένα εμπορικό προϊόν που χρησιμοποιεί το TSCH. το SmartMesh IP. Συνοπτικά το SmartMesh IP συνδυάζει τις τεχνολογίες βιομηχανικής απόδοσης του IEEE802.15.4e με την τεχνολογία 6LoWPAN. Επιπλέον, παρουσιάζεται και ένα μοντέλο που εκτιμά την απόδοση του δικτύου , όπου στη συγκεκριμένη περίπτωση είναι ένα δίκτυο SmartMesh IP. Ορισμένες παράμετροι με τις οποίες ασχολείται το μοντέλο είναι η τοπολογία του δικτύου, οι απαιτήσεις επιπέδου υπηρεσιών, τα διαστήματα αναφοράς, το μέγεθος ωφέλιμου φορτίου, η σταθερότητα της διαδρομής, ο τύπος υλισμικού (hardware), η τάση της τροφοδοσίας και η θερμοκρασία, με στόχο την κατανόηση της απόδοσης του δικτύου.

Τα βασικά κριτήρια για την κατανόηση της απόδοσης του δικτύου είναι η αξιοπιστία (reliability), η διεκπεραιωτική ικανότητα (throughput) και η καθυστέρηση (latency). Το πρώτο κριτήριο αναφέρεται στη μερίδα των πακέτων δεδομένων που φτάνουν στον προορισμό. Το δεύτερο ασχολείται με τον αριθμό των πακέτων δεδομένων που δημιουργούνται από τους κόμβους. Το τρίτο κριτήριο με τη σειρά του παραπέμπει στο χρόνο που απαιτείται μεταξύ της δημιουργίας του πακέτου και της παραλαβής του από τον τελικό του προορισμό. Τονίζεται , επίσης, η αναγκαιότητα ύπαρξης της ικανότητας αντιστάθμισης (trade-off) μεταξύ των τριών παραπάνω κριτηρίων για την άρτια λειτουργία του δικτύου.

Στη συνέχεια, δίδεται ιδιαίτερη έμφαση στα οφέλη των δικτύων που υποστηρίζουν την τεχνολογία TSCH σε εφαρμογές βιομηχανίας και την εκθετικά αυξημένη ζήτηση για την εφαρμογή αυτής της τεχνολογίας και σε άλλους τομείς. Γίνεται αναφορά στο εργαλείο εκτίμησης ισχύος και απόδοσης SmartMesh. Το SmartMesh συνδράμει στον προγραμματισμό της απόδοσης του δικτύου, δημιουργώντας ένα μέσο πρόγραμμα για κάθε άλμα στο δίκτυο και υπολογίζοντας τη μέση ισχύ, καθυστέρηση, κατανάλωση και ρυθμό μετάδοσης με βάση την εισαγωγή του χρήστη.

Επιπλέον, καλύπτει τις απαιτήσεις για διάφορες περιοχές εφαρμογών για δίκτυα χαμηλής ισχύος (LLN), όπως προσδιορίζονται από την Ομάδα Εργασίας Μηχανικής Διαδικτύου (IETF) και επικεντρώνεται σε τρεις τυποποιημένες "έξυπνες" εφαρμογές: έξυπνες πόλεις, έξυπνα κτίρια και έξυπνα εργοστάσια, καθεμία από τις οποίες εξάγει συγκεκριμένες παραμέτρους δικτύου για εισαγωγή σε εργαλεία εκτίμησης επιδόσεων σε πραγματικό κόσμο.

2.3 Σχηματισμός Δικτύου

Στο TSCH, η διαδικασία δημιουργίας δικτύου λαμβάνει χώρα μόλις ο συντονιστής ξεκινάει τη διαφήμιση του δικτύου στέλνοντας έναν Enhanced Beacon (EB). Στην περίπτωση που ένας κόμβος θέλει να ενταχθεί στο δίκτυο, απαιτείται η ενεργοποίηση του ασυρμάτου του και η αναζήτηση πιθανών μηνυμάτων από τους EBs. Μόλις παραλάβει έναν έγκυρο EB, ο κόμβος έχει την ικανότητα μετάδοσης δικών του EBs, ώστε να ανακοινώσει την παρουσία του στο δίκτυο. Βέβαια, τα υπάρχοντα πρωτόκολλα, στη συγκεκριμένη περίπτωση το IEEE802.15.4e, δεν ορίζουν κάποια πολιτική διαφήμισης των EBs, αλλά ούτε και τον ρυθμό με τον οποίο πρέπει να αποστέλλονται. Είναι πολύ σημαντική, συνεπώς, η βελτιστοποίηση της διαδικασίας

σχηματισμού δικτύου, διότι η ένταξη ενός κόμβου καταναλώνει αρκετή ενέργεια, μιας και ο ασύρματος κατά τη διαδικασία αυτή παραμένει ενεργός. Στις μελέτες [13-15] δίδονται τρεις λύσεις για το πρόβλημα αυτό.

1. Τυχαιοκρατικός αλγόριθμος διαφήμισης (Random-based Advertisement Algorithm): Στον αλγόριθμο αυτό, όλοι οι κόμβοι που έχουν ενταχθεί στο δίκτυο ενεργούν ως κόμβοι διαφημιστές και στέλνουν περιοδικά EBs για τη διαφήμιση του δίκτυο. Σε κάθε κόμβο του δικτύου ανατίθεται από τον κεντρικό συντονιστή μία σύνδεση σε ένα πλαίσιο υποδοχής για τη μετάδοση των EBs. Κάθε κόμβος μεταδίδει έναν EB σε μία προγραμματισμένη σύνδεση με πιθανότητα Peb. Η εν λόγω πιθανότητα υπολογίζεται με σκοπό την ελαχιστοποίηση της πιθανότητας σύγκρουσης μεταξύ διαφορετικών EBs. Στη μελέτη [13] διαπιστώθηκε ότι με τη χρήση περισσοτέρων Channel Offsets για τη διαφήμιση, είναι δυνατή η μείωση του χρόνου σύνδεσης και της κατανάλωσης ενέργειας των ήδη συνδεδεμένων κόμβων. Βέβαια, χρειάζεται η πυκνότητα του δικτύου να είναι πολύ υψηλή.
2. Τυχαίο κάθετο/οριζόντιο γέμισμα (Random Vertical/Horizontal Filling- RV,RH): Και στους δύο αλγορίθμους μόλις ένας κόμβος ενταχθεί στο δίκτυο μπορεί να στείλει τους δικούς του EBs και να επιτύχει ταχείς διαδικασίες σύνδεσης. Στους αναφερθέντες αλγορίθμους, πολλαπλά διαδοχικά πλαίσια (slotframes) υποδοχής ομαδοποιούνται με στόχο τον σχηματισμό ενός πλαισίου πολλαπλών υποδοχών (multi-slotframe). Κάθε κόμβος έχει την ικανότητα αποστολής ενός EB μόνο κατά τη διάρκεια του πρώτου χρονικού περιθωρίου ενός μόνο slotframe του multi-slotframe. Και στις δύο περιπτώσεις ο συντονιστής χρησιμοποιεί μόνο το Channel-Offset 0 για να στείλει τον EB στην πρώτη θέση διαφήμισης του πλαισίου πολλαπλών θέσεων/σχισμών του. Όσον αφορά τον αλγόριθμο τυχαίου κάθετου γεμίσματος, οποιοσδήποτε άλλος κόμβος θα πρέπει να μεταδώσει τον EB του στην ίδια θέση διαφήμισης, αλλά χρησιμοποιώντας μια τυχαία επιλεγμένη μετατόπιση καναλιού. Αντιθέτως, στον αλγόριθμο τυχαίου οριζόντιου γεμίσματος οι κόμβοι χρησιμοποιούν το Channel-Offset 0 , αλλά επιλέγεται τυχαία η θέση διαφήμισης στο πλαίσιο πολλαπλών υποδοχών. Στο άρθρο [14] διαπιστώθηκε ότι οι επιδόσεις των αλγορίθμων είναι παρόμοιες και τονίζουν ότι μπορεί να χρησιμοποιηθεί μόνο ένας από τους δύο σε ένα δίκτυο.
3. Αλυσίδα διακριτού χρόνου Markov (Discrete Time Markov Chain – DTMC): Στην προκειμένη περίπτωση μοντελοποιείται η διαδικασία σχηματισμού δικτύου με τη χρήση της DTMC και προκύπτει μία αναλυτική έκφραση του μέσου χρόνου σύνδεσης στο δίκτυο. Από τη διαδικασία αυτή προκύπτει το πρόβλημα βελτιστοποίησης για τον υπολογισμό του βέλτιστου προγράμματος EB που ελαχιστοποιεί τον μέσο χρόνο σύνδεσης, το οποίο επιλύεται με τη χρήση του αλγορίθμου χρονοπρογραμματισμού φάρου βάση μοντέλου (Model-based beacon scheduling – MBS) [15]. Προκύπτει ότι ο MBS υπερτερεί έναντι των προηγούμενων αλγορίθμων, διότι με τη μείωση του μέσου χρόνου σύνδεσης μειώνεται ο χρόνος που ο ασύρματος παραμένει ενεργός και τελικά μειώνεται η συνολική κατανάλωση ενέργειας.

2.4 Κινητικότητα Κόμβων στο δίκτυο

Οι βιομηχανικές εφαρμογές που απαιτούν κινητούς κόμβους δικτύου, όπως αισθητήρες που είναι προσαρτημένοι σε εργαζόμενους ή βιομηχανικά περιουσιακά στοιχεία, απαιτούν μηχανισμούς για τον κατάλληλο χειρισμό της κινητικότητας των κόμβων στο δίκτυο TSCH. Η κινητικότητα των κόμβων μπορεί να επηρεάσει τις επιδόσεις του δικτύου, καθώς οι κόμβοι πρέπει να αναζητούν διαθέσιμα κανάλια και να περιμένουν τα EB να ενταχθούν στο δίκτυο και να γίνουν και πάλι πλήρως λειτουργικά. Το πρόβλημα αυτό επιδεινώνεται περαιτέρω από την έλλειψη ενός τυποποιημένου μηχανισμού χρονοδρομολόγησης φάρου και χρονοθυρίδας, ο οποίος επηρεάζει τον πραγματικό χρόνο συμμετοχής των κόμβων.

Οι συγγραφείς των [3,16] προτείνουν τη μεταπήδηση καναλιού με κινητές χρονοθυρίδες (Mobile Timeslotted Channel Hopping – MTSCH), ένα πλαίσιο με επίγνωση της κινητικότητας που βασίζεται σε παθητικούς φάρους. Αντί για διαφήμιση στο δίκτυο με τη χρήση EB, οι κόμβοι στο

MTSCH χρησιμοποιούν μηνύματα ACK, τα οποία χρησιμοποιούνται για την επιβεβαίωση της λήψης πακέτων σε κανάλια σταθερής συχνότητας. Αυτό επιτρέπει στους κινητούς συνδεδεμένους κόμβους να λαμβάνουν ταχύτερα τα μηνύματα συγχρονισμού (ACK) και να εξοικονομούν ενέργεια. Το ομαδικό ACK χρησιμοποιείται επίσης για να επιτρέψει στους κόμβους να εξοικονομήσουν ενέργεια με την αποστολή μεμονωμένων μηνυμάτων ACK.

Το MTSCH μειώνει σημαντικά τον κύκλο λειτουργίας των κινητών κόμβων σε ποσοστό 7% έως 50% σε σύγκριση με τα τυπικά δίκτυα TSCH. Βελτιώνει επίσης το χρόνο σύνδεσης των κινητών κόμβων κατά 3-50%.

Στη συνέχεια, προτείνεται μια νέα λύση για τη βελτιστοποίηση της δρομολόγησης σε δίκτυα TSCH όπου μπορεί να υπάρχουν κινητοί κόμβοι. Οι συγγραφείς θεωρούν ένα δίκτυο που αποτελείται από στατικούς κόμβους που ονομάζονται κόμβοι άγκυρας και κινητούς κόμβους των οποίων οι θέσεις είναι άγνωστες. Οι συνδέσεις μεταξύ των κόμβων άγκυρας δημιουργούνται με τη χρήση RPL, η οποία επιλέγει συνδέσεις με βάση ορισμένες μετρικές. Όταν εξετάζεται η σύνδεση μεταξύ ενός κινητού κόμβου και ενός κόμβου άγκυρας, λαμβάνεται υπόψη και η πραγματική θέση του κόμβου. Τα αποτελέσματα δείχνουν ότι η συγκεκριμένη λύση παρέχει την καλύτερη αξιοπιστία σύνδεσης από άκρο σε άκρο και μειώνει τις αρνητικές επιπτώσεις των σφαλμάτων θέσης.

2.5 Προγραμματισμός Συνδέσεων

Ένα από τα πιο σημαντικά στοιχεία του TSCH είναι ο προγραμματισμός των συνδέσεων για την κατανομή συνδέσεων στους κόμβους για τη μεταφορά δεδομένων. Αν και οι πολυκαναλικοί μηχανισμοί ανακουφίζουν τα προβλήματα χρονοπρογραμματισμού των συνδέσεων, η εύρεση ενός βέλτιστου χρονοπρογραμματισμού μπορεί να είναι δύσκολη, ιδίως σε μεγάλα δίκτυα με τοπολογίες πολλαπλών σταθμών ή σε δυναμικά δίκτυα με μεταβαλλόμενες τοπολογίες.

Το IEEE 802.15.4e δεν καθορίζει κάποιον τρόπο δημιουργίας ενός κατάλληλου χρονοδιαγράμματος συνδέσεων. Τα περισσότερα από τα υπάρχοντα σχήματα προγραμματισμού πολλαπλών καναλιών δεν είναι κατάλληλα για δίκτυα TSCH λόγω των ακόλουθων περιορισμών: Η μεταπήδηση καναλιού δεν μπορεί να πραγματοποιηθεί σε βάση ανά πακέτο, δεν έχει σχεδιαστεί για κόμβους με περιορισμένους πόρους και δεν είναι αποδοτική βάση της χρήσης του καναλιού.

Πρόσφατα έχουν προταθεί νέοι αλγόριθμοι χρονοπρογραμματισμού σχεδιασμένοι ειδικά για δίκτυα TSCH, οι οποίοι μπορεί να διαχωριστούν σε συγκεντρωτικούς (centralized) και κατανεμημένους (distributed). Στην περίπτωση ενός συγκεντρωτικού αλγορίθμου, ένας συγκεκριμένος κόμβος στο δίκτυο δημιουργεί, διανέμει και ενημερώνει τα σχέδια συνδεσιμότητας με βάση τις πληροφορίες που λαμβάνει από όλους τους κόμβους. Ωστόσο, το πρόγραμμα σύνδεσης πρέπει να υπολογίζεται εκ νέου και να διανέμεται κάθε φορά που αλλάζουν οι συνθήκες λειτουργίας. Αντιθέτως, στην περίπτωση ενός κατανεμημένου αλγορίθμου, υπολογίζονται αυτόνομα τα χρονοδιαγράμματα συνδέσεων για κάθε κόμβο με βάση τις τοπικές μερικές πληροφορίες που ανταλλάσσονται με τους γειτονικούς κόμβους. Παρόλο που το συνολικό σχέδιο που παρέχεται από έναν κατανεμημένο αλγόριθμο δεν είναι συνήθως βέλτιστο, είναι οικονομικά αποδοτικό για κόμβους με περιορισμένη ισχύ λόγω της περιορισμένης επιβάρυνσης.

3. Τεχνολογία 6TiSCH

Η IETF με σκοπό την εξέλιξη της τεχνολογίας TSCH που αναπτύχθηκε στο κεφάλαιο 2 της παρούσας εργασίας, δημιούργησε το 6TiSCH-WG, ώστε να ενσωματωθεί το TSCH στη στοίβα των πρωτοκόλλων του Διαδικτύου των Πραγμάτων. Η διαδικασία επιτεύχθηκε με τον συνδυασμό της υψηλής αξιοπιστίας και της χαμηλής κατανάλωσης ενέργειας της τεχνολογίας TSCH με τη διαλειτουργικότητα που παρέχει το πρωτόκολλο IP. Ο τρόπος λειτουργίας του επιπέδου MAC στο TSCH τοποθετείται κάτω από μια στοίβα πρωτοκόλλων με δυνατότητα IPv6, όπως IPv6 ασύρματου δικτύου προσωπικής περιοχής χαμηλής ισχύος (6LoWPAN), το πρωτόκολλο IPv6 για δίκτυα χαμηλής ισχύος και απωλειών (RPL), ασχολείται με τη δρομολόγηση, και το πρωτόκολλο περιορισμένης εφαρμογής (CoAP). Για το συντονισμό του TSCH με τα πρωτόκολλα ανώτερου επιπέδου, χρησιμοποιείται ένα καινούριο κατασκευασμένο αντικείμενο για τον προγραμματισμό των χρονοθυρίδων TSCH για τα πλαίσια που βρίσκονται σε διαδικασία αποστολής μέσα στο δίκτυο. Η αρχιτεκτονική 6TiSCH και η στοίβα πρωτοκόλλων βρίσκονται σε διαδικασία ανάπτυξης μαζί με τους μηχανισμούς χρονοπρογραμματισμού και δρομολόγησης που βρίσκονται υπό την αιγίδα από την ομάδα εργασίας 6TiSCH.

3.1 Βασικό Προφίλ 6TiSCH

Σύμφωνα με τα άρθρα [10,17] το 6TiSCH-WG όρισε το βασικό προφίλ 6TiSCH στο πρότυπο RFC8180, το οποίο σχεδιάζει το ελάχιστο εύρος ζώνης για τη διαφήμιση του δικτύου και την κίνηση σύνδεσης. Αυτό το προφίλ μπορεί να χρησιμοποιηθεί ως εναλλακτικός τρόπος λειτουργίας σε περίπτωση που ο δυναμικός προγραμματισμός αποτύχει ή δεν επαρκεί, επιτρέποντας σε όλους τους κόμβους να εξαρτώνται από την αμελητέα ρύθμιση για ανάκαμψη. ‘Pledge’ ονομάζεται ο κόμβος που πρόκειται να ενταχθεί μέσα σε ένα δίκτυο 6TiSCH. Όλοι οι κόμβοι που έχουν ενταχθεί εντός του δικτύου στέλνουν ανά τακτά χρονικά διαστήματα EBs. Όταν ο ασύρματος του ‘Pledge’ ενεργοποιείται, εκείνος με τη σειρά του «ακούει» τους EBs και ανακαλύπτει τους κόμβους γύρω του. Το πρότυπο, προτείνει την αναμονή ενός ‘Pledge’ που δεν έχει περατωθεί η διαδικασία ένταξής του και συνεπώς το δίκτυο δεν τον θεωρεί αξιόπιστο.

Η προσέγγιση του βασικού προφίλ 6TiSCH προβλέπει την επιλογή του κόμβου με το μικρότερο Join Metric ως Join Proxy (JP) εν μέσω της ασφαλούς διαδικασίας σύνδεσης. Ο EB περιέχει στοιχεία δεδομένων ωφέλιμου φορτίου που επιτρέπουν στον ‘Pledge’ να γνωρίζει το ελάχιστο χρονοδιάγραμμα και τη διαμόρφωση του στρώματος MAC που πρέπει να χρησιμοποιήσει. Το RFC8180 προδιαγράφει τη χρησιμοποίηση ενός μόνο κοινόχρηστου κελιού για τη δραστηριότητα σύνδεσης (slotted aloha). Με αυτόν τον τρόπο, αφήνει την επιλογή μεγέθους του slotframe ανοιχτή στους υπεύθυνους υλοποίησης, οι οποίοι μπορούν να ανταλλάξουν την κατανάλωση ενέργειας με μικρότερους χρόνους ένταξης.

Σε περίπτωση που χρησιμοποιείται το πρωτόκολλο RPL, απαιτείται η λειτουργία μη αποθήκευσης. Το RFC8180 ταιριάζει την τοπολογία στρώματος σύνδεσης και την τοπολογία διεύθυνσης χρησιμοποιώντας το πεδίο Join Metric, τμήμα του Synchronization IE και μεταδίδεται μέσω του EB. Το Join Metric μπορεί να είναι μια αναπαράσταση της κατάταξης RPL, που εγγυάται ότι ένας 'Pledge' επιλέγει ένα JP κοντά στη ρίζα του δικτύου και περιλαμβάνει μια καλή πιθανότητα να είναι ο RPL προτιμώμενος γονέας του. Η τεχνολογία 6TiSCH υποστηρίζει τη χρήση δυναμικού προγραμματισμού, όπου οι πόροι του στρώματος σύνδεσης προστίθενται/διαγράφονται δυναμικά για τον συντονισμό των προϋποθέσεων επικοινωνίας των εφαρμογών. Ο δυναμικός προγραμματισμός διαχωρίζεται σε δύο εννοιολογικά μέρη: το πρωτόκολλο 6top (6P),το οποίο διαθέτει έναν μηχανισμό συναλλαγής ανά ζεύγη στο επίπεδο ελέγχου λειτουργίας για την προσθήκη ή αφαίρεση κελιών στο πρόγραμμά τους και τη συνάρτηση χρονοπρογραμματισμού (Scheduling Function - SF), η οποία ως βασική της λειτουργία έχει την πρόσθεση ή την αφαίρεση κελιών, καθώς και την ενεργοποίηση των διαπραγματεύσεων 6P [10].

3.1.1 Πρωτόκολλο 6top

Το πρωτόκολλο 6P (6P), όπως χαρακτηρίζεται στο RFC8480, παρέχει έναν μηχανισμό συναλλαγής ανά ζεύγη στο επίπεδο ελέγχου λειτουργίας. Το πρωτόκολλο υποστηρίζει τη συμφωνία για ένα χρονοδιάγραμμα μεταξύ γειτόνων, προσφέροντας τη δυνατότητα κατανεμημένου προγραμματισμού. Η διευθέτηση ανά ζεύγη μπορεί να αντιμετωπιστεί χρησιμοποιώντας ανταλλαγές δύο ή τριών βημάτων. Στη συναλλαγή δύο βημάτων επιτρέπεται στον αιτούντα κόμβο να επιλέξει τα κελιά που θα συμπεριλάβει, θα διαγράψει ή θα μετακινήσει, ενώ με συναλλαγή τριών βημάτων επιτρέπεται στον κόμβο παραλήπτη να επιλέξει κελιά, αφήνοντας για την περίπτωση ενός γονέα να μοιράσει ένα κομμάτι κελιών δίκαια μεταξύ των παιδιών του.

Οι εντολές 6P, εμφανίζονται στον Πίνακα ΙΙ [10,18] μεταφέρονται σε στοιχεία πληροφορίας (IEs) και μεταφέρονται με ένα μόνο άλμα. Μια συναλλαγή 6P επιτυγχάνει όταν εκτελούνται τα δύο ή τρία βήματά της με ακρίβεια και στους δύο γειτονικούς κόμβους. Το 6P χρησιμοποιεί ένα χρονικό όριο για την ακύρωση μιας μεγάλης χρονικά συναλλαγής. Οι παρατυπίες του χρονοδιαγράμματος αναγνωρίζονται με τη χρήση ενός αριθμού διευθέτησης (SeqNum), και η ανίχνευση της απώλειας του μηνύματος όταν δεν λαμβάνεται το τελικό ACK. Μια πιθανή περίσταση παρατυπίας μπορεί να συμβεί όταν ένας κόμβος ξεκινήσει μια συναλλαγή, αλλά μετά την τελική απάντηση, το ACK του στρώματος σύνδεσης χάνεται. Μόλις εντοπιστεί το λανθασμένο ACK, ο δεύτερος κόμβος που παίρνει μέρος στη συναλλαγή εφαρμόζει τον κανόνα που χαρακτηρίζεται από τη συνάρτηση χρονοπρογραμματισμού (SF). Αυτός μπορεί να είναι η έκδοση μιας εντολής CLEAR για την επαναφορά όλων των κελιών μεταξύ των δύο κόμβων που γίνεται η συναλλαγή, ή προσπάθεια επιδιόρθωσης της πιθανής παρατυπίας μέσω μίας δραστηριότητας επαναφοράς. Στη συγκεκριμένη περίπτωση, ο δεύτερος κόμβος μπορεί να εκδώσει την εντολή LIST μετά το χρονικό περιθώριο για να εντοπίσει τις αντιθέσεις του χρονοδιαγράμματος και να τις αποκαταστήσει μέσω των επακόλουθων πράξεων συμπερίληψης, διαγραφής ή μετακίνησης.

Πίνακας ΙΙ – Εντολές του πρωτοκόλλου 6top

Εντολή	Κωδικός	Περιγραφή
ADD/ΠΡΟΣΘΗΚΗ	0	Προσθήκη κελιών μεταξύ δύο γειτόνων.
DELETE/ΔΙΑΓΡΑΦΗ	1	Διαγραφή Κελιών από το χρονοδιάγραμμα
RELOCATE/ΜΕΤΑΚΙΝΗΣΗ	2	Μετακίνηση κελιών στο χρονοδιάγραμμα
COUNT/ΜΕΤΡΗΣΗ	4	Μέτρηση συγκεκριμένων κελιών
LIST/ΛΙΣΤΑ	5	Εμφάνιση συγκεκριμένων κελιών σε μορφή λίστας

SIGNAL	6	Προσωρινή καταχώρηση για εντολές τύπου SF
CLEAR/ΕΚΚΑΘΑΡΙΣΗ	7	Εκκαθάριση όλων των κελιών μεταξύ δύο γειτόνων

Το SeqNum χρησιμοποιείται επιπλέον για τον εντοπισμό διπλότυπων μηνυμάτων και την επαναφορά των κόμβων. Εφόσον, οι κόμβοι εντός του δικτύου αποθηκεύουν το τελευταίο επιτυχές SeqNum που φαίνεται από ένα γειτονικό χρονοδιάγραμμα, οι επαναφορές μπορούν να ανιχνευθούν. Αυτό συμβαίνει όταν ένας κόμβος λαμβάνει SeqNum με τιμή 0 σε ένα αίτημα 6P, ενώ αποθηκεύει ένα SeqNum για τον εν λόγω γείτονα με ξεχωριστή εκτίμηση.

3.1.2 Συνάρτηση Προγραμματισμού

Όπως αναφέρθηκε και στο κεφάλαιο 3.1 το πρωτόκολλο 6top είναι άρρηκτα συνδεδεμένο με μία συνάρτηση χρονοπρογραμματισμού, η οποία ασχολείται με τη διατήρηση των κελιών μεταξύ των κόμβων και την ενεργοποίηση των συναλλαγών του πρωτοκόλλου 6top, οι οποίες αναφέρονται στον Πίνακα ΙΙ. Η βασική συνάρτηση που χρησιμοποιήθηκε από το 6TiSCH-WG είναι η ελάχιστη συνάρτηση χρονοπρογραμματισμού (Minimal Scheduling Function - MSF), η οποία ακολουθεί το βασικό ή αλλιώς ελάχιστο προφίλ 6TiSCH. Σύμφωνα με το άρθρο [19], η MSF ενισχύει το βασικό χρονοδιάγραμμα και η βασική της χρήση είναι να συμπεριλαμβάνει τις συνδέσεις παιδιών-γονέων αναλόγως του φορτίου κυκλοφορίας.

Η MSF ορίζει δύο είδη κελιών, τα αυτόνομα (Autonomous) και τα διαπραγματεύσιμα (Negotiated). Το πρώτο είδος κελιού, προσφέρει την ικανότητα σύνδεσης σε οποιονδήποτε γείτονα χωρίς να απαιτείται σηματοδότηση. Το δεύτερο είδος με τη σειρά του, είναι διαχειρίσιμο από το πρωτόκολλο 6top και δίδεται η δυνατότητα εισαγωγής και αποβολής του από το χρονοδιάγραμμα βάση της κίνησης που υπάρχει στο δίκτυο. Τα αυτόνομα κελιά με τη σειρά τους διαχωρίζονται σε κελιά αυτόνομης μετάδοσης (Autonomous TX) και αυτόνομου δέκτη (Autonomous RX). Τα κελία αυτόνομων δεκτών εγκαθίστανται δια παντός βάσει χρονοδιαγράμματος, ενώ τα κελιά αυτόνομης μετάδοσης εγκαθίστανται κατόπιν ζήτησης. Όταν πρόκειται να μεταδοθεί ένα πλαίσιο ένα προς ένα από ένα σημείο του δικτύου σε ένα άλλο (unicast) χωρίς διαπραγματεύσιμο κελί μετάδοσης, το κελί αυτόνομης μετάδοσης εγκαθίσταται και αφαιρείται αμέσως.

Στη συνέχεια η MSF χρησιμοποιεί μία συνάρτηση κατακερματισμού, τη συμβολική προσέγγιση αθροίσματος (Symbolic Aggregate ApproXimation – SAX), με σκοπό τη διευκόλυνση εύρεσης των συντεταγμένων (slotOffset,channelOffset) από μία διεύθυνση EUI64. Η συγκεκριμένη συνάρτηση κατακερματισμού εγγυάται ομοιογενή μεταφορά των κελιών κατά μήκος των timeslot-offsets και channel-offsets και διευκολύνει στην αποφυγή συγκρούσεων, ενώ παρέχει μια στρατηγική για την αξιόπιστη και ισότιμη διασπορά των κελιών μέσα στο χρονοδιάγραμμα[19]. Οι συγκρούσεις κατακερματισμού μπορούν να οδηγήσουν στον κοινό προγραμματισμό των κελιών αυτόνομης μετάδοσης και αυτόνομων δεκτών στη χρονική ή καναλική τους μετατόπιση. Η MSF παρέχει ορισμένους κανόνες για την αποφυγή αυτών των συγκρούσεων , όπως την προτεραιότητα του κελιού αυτόνομης μετάδοσης με τα περισσότερα πακέτα προς αποστολή και την προτεραιότητα του αυτόνομου κελιού δέκτη στην περίπτωση που τα αυτόνομα κελιά μετάδοσης δεν έχουν κάποιο πακέτο προς αποστολή.

Σύμφωνα με τα αποτελέσματα από το άρθρο [10], Η συνάρτηση MSF κατανέμει κελιά προς διαπραγμάτευση στους κόμβους ανάλογα με το ρυθμό με τον οποίο ανταλλάσσουν πακέτα εφαρμογών με τον επιλεγμένο γονέα τους. Παρακολουθεί τη χρήση του κελιού αυξάνοντας τα numCellElapsed και numCellUsed κάθε φορά που το κελί χρησιμοποιείται για την αποστολή ή τη λήψη ενός πλαισίου από τον συγκεκριμένο γείτονα. Η MSF υπολογίζει τη χρήση του κελιού κάθε 16 slotframes. Εάν είναι πάνω από 75%, στέλνει ένα αίτημα 6P ADD για να προσθέσει ένα αποκλειστικό κελί στον συγκεκριμένο γείτονα. Όταν πέσει κάτω από 25%, αποστέλλεται ένα αίτημα 6P DELETE(ΔΙΑΓΡΑΦΗ) για την αφαίρεση ενός συγκεκριμένου κελιού.

Το σύστημα λειτουργεί με την παραδοχή ότι ο λόγος παράδοσης πακέτων (PDR) είναι 100% για

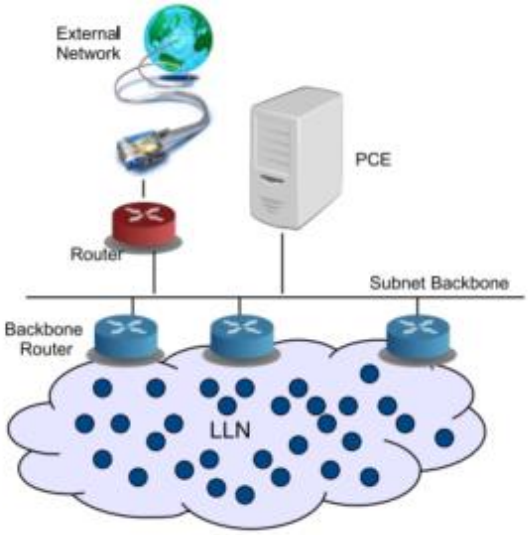
κάθε κελί. Εάν ένας κόμβος πρέπει να παραδώσει δύο πακέτα σε κάθε slotframe στον επιλεγμένο γονέα του, θα έχει μόνο ένα κελί στο πρόγραμμά του. Μετά από 16 slotframes, η χρήση του κελιού παραμένει στο 100%. Στη συνέχεια, η συνάρτηση MSF ζητά από το πρωτόκολλο 6top να συμπεριλάβει ένα επιπλέον κελί μετάδοσης, με αποτέλεσμα τη μείωση της χρήσης του κελιού στο 67%. Όταν η ανάγκη κίνησης του κόμβου μειώνεται σε 1 πλαίσιο ανά 3 slotframes, η χρήση κελιού μειώνεται στο 12,5%. Η συνάρτηση, στη συνέχεια, στέλνει ένα αίτημα 6P DELETE(ΔΙΑΓΡΑΦΗ) για να αφαιρέσει ένα μόνο κελί μετάδοσης, με αποτέλεσμα η χρήση των κελιών να αυξάνεται στο 18,75%.

Η αντικατάσταση ενός κελιού μετάδοσης με ένα κελί δέκτη επιτρέπει στη MSF να προσαρμοστεί στην εισερχόμενη κίνηση. Σε κάθε κελί λήψης, η μεταβλητή numCellElapsed αυξάνεται. Εάν ληφθεί έγκυρο πλαίσιο με τον σωστό κυκλικό έλεγχο πλεονασμού (CRC), η μεταβλητή numCellUsed αυξάνεται. Η ίδια προσέγγιση μπορεί να χρησιμοποιηθεί για την προσθήκη ή αφαίρεση κελιών δέκτες για την προσαρμογή της κίνησης προς τα κάτω (downstream).

Η MSF εντοπίζει συγκρούσεις στο χρονοδιάγραμμα των διαπραγματεύσιμων κελιών που εκχωρούνται από την MSF και μετακινεί τα συγκρουόμενα διαχειρίσιμα κελιά σε διαφορετικές θέσεις στο χρονοδιάγραμμα. Επιπλέον, υπολογίζει τον λόγο παράδοσης πακέτων (Packet Deliver Ratio - PDR) για κάθε κελί προς τον πρωτεύοντα γονέα της κάθε λεπτό και στη συνέχεια τον συγκρίνει με τον PDR όλων των άλλων κυψελών προς τον ίδιο πρωτεύοντα γονέα. Εάν η διαφορά υπερβαίνει το 50%, το MSF θεωρεί ότι η κυψέλη συγκρούεται και ξεκινά ένα αίτημα 6P RELOCATE(ΜΕΤΑΚΙΝΗΣΗ).

3.2 Αρχιτεκτονική δικτύου 6TiSCH

Σύμφωνα με τις μελέτες [3,9] ένα δίκτυο 6TiSCH περιλαμβάνει στο κατώτερο πεδίο ένα δίκτυο χαμηλής ισχύος με απώλειες (LLNs) , το οποίο εμπεριέχει έναν αρκετά μεγάλο αριθμό κόμβων, οι οποίοι με τη σειρά τους κάνουν χρήση της λειτουργίας TSCH στο επίπεδο MAC. Όλοι οι κόμβοι του LLN ανήκουν στο ίδιο υποδίκτυο IPv6. Το LLN συνδέεται με τον κορμό υψηλής ταχύτητας του τοπικού δικτύου μέσω συγχρονισμένων δρομολογητών κορμού (backbone routers – BRRs). Ο κορμός, επιπλέον λειτουργεί ως υποδομή για τις διαδικασίες διασύνδεσης και συγχρονισμού των κόμβων του LLN. Στην αρχιτεκτονική του δικτύου υπάρχει ένας δρομολογητής που λειτουργεί ως πύλη (Gateway), με μέλημά του τη σύνδεση του κορμού με το διαδίκτυο, όπως φαίνεται και στην εικόνα 3.1.



Εικόνα 3.1 Αρχιτεκτονική δικτύου 6TiSCH
Πηγή : IETF 6TSCH: Combining IPv6 Connectivity with Industrial Performance [9]

Ένα σημαντικό τμήμα της αρχιτεκτονικής των δικτύων 6TiSCH είναι η οντότητα υπολογισμού διαδρομής (Path Computation Entity – PCE). Η PCE ως κύρια λειτουργία έχει τον υπολογισμό των διαδρομών εντός του LLN, στην περίπτωση που το δίκτυο έχει χρονοπρογραμματιστεί με τη χρήση συγκεντρωτικού αλγορίθμου (Κεφάλαιο 2.5).

Η δομή της αρχιτεκτονικής ορίζει τον τρόπο μεταβίβασης και επισήμανσης των δεδομένων σε μία προγραμματισμένη διαδρομή IPv6 διαμέσου του δικτύου, διασφαλίζοντας τη συμμόρφωση με τα προκαθορισμένα όρια για καθυστέρηση και jitter.

3.3 Δρομολόγηση δικτύων 6TiSCH

Το πρωτόκολλο που χρησιμοποιείται για τη δρομολόγηση ενός δικτύου τεχνολογίας 6TiSCH είναι το πρωτόκολλο δρομολόγησης για δίκτυα χαμηλής ισχύος και απωλειών (Routing Protocol for Low Power and Lossy Networks - RPL). Το RPL χρησιμοποιεί έναν δρομολογητή, που βρίσκεται συνήθως στα περιθώρια του δικτύου και είναι συνδεδεμένος και με άλλα εξωτερικά δίκτυα, που λειτουργεί ως ρίζα του δικτύου και επιτρέπει τη δρομολόγηση πολλαπλών βημάτων (multi-hop routing). Το RPL δίνει τη δυνατότητα επικοινωνίας στο σύνολο των κόμβων του δικτύου μεταξύ τους με την αποστολή μηνυμάτων τόσο προς τα πάνω (upwards communication) όσο και προς τα κάτω (downwards communication), όπου και στις δύο περιπτώσεις λειτουργεί διαφορετικά.

Το πρωτόκολλο RPL ενσωματώνει χαρακτηριστικά για δυναμική επιλογή διαδρομής, αναγνώριση βρόχων και αποκατάσταση διαδρομής για την αντιμετώπιση της απώλειας πακέτων. Οργανώνει τους δρομολογητές του δικτύου κατά μήκος ενός κατευθυνόμενου άκυκλου γραφήματος προσανατολισμένο σε έναν προορισμό (Destination Oriented Directed Acyclic Graph – DODAG), ο οποίος προορισμός κατά κύριο λόγο είναι η ρίζα του δικτύου. Έχει σχεδιαστεί για πολλές εφαρμογές και μπορεί να λειτουργεί σε πολλές περιπτώσεις μέσα στο ίδιο φυσικό δίκτυο, με την προϋπόθεση ότι κάθε εφαρμογή έχει τις δικές της μοναδικές παραμέτρους διαμόρφωσης. Οι κόμβοι σε μια περίπτωση μπορούν να λειτουργούν πολυάριθμα DODAG, καθένα από τα οποία συνδέεται με μια ξεχωριστή ρίζα, ενισχύοντας την ανοχή σε σφάλματα και την ευελιξία.

Το RPL μπορεί να λειτουργήσει είτε με τον τρόπο αποθήκευσης ή με τον τρόπο μη αποθήκευσης. Στην πρώτη περίπτωση, οι κόμβοι του δικτύου αποθηκεύουν τους πίνακες δρομολόγησης, ενώ στη δεύτερη περίπτωση δεν υπάρχει διατήρηση των πινάκων δρομολόγησης τοπικά. Στη δρομολόγηση χωρίς αποθήκευση, η ρίζα του DODAG διαθέτει μια ολοκληρωμένη τοπολογία του δικτύου που επιβλέπει και δρομολογεί βάση της ρίζας. Η κυκλοφορία κατευθύνεται αρχικά στη ρίζα, όπου υπολογίζονται οι διαδρομές προς αυτή. Στη συνέχεια, τα αποτελέσματα της προς τα πάνω δρομολόγησης μεταδίδονται προς τα κάτω και προωθούνται με βάση την επικεφαλίδα δρομολόγησης πηγής.

Το RPL για την επίτευξη των διαδικασιών που ασχολείται χρησιμοποιεί τέσσερα είδη μηνυμάτων πάνω στο DODAG:

1. Αίτηση πληροφοριών DODAG (DODAG Information Solicitation – DIS): Με τα μηνύματα

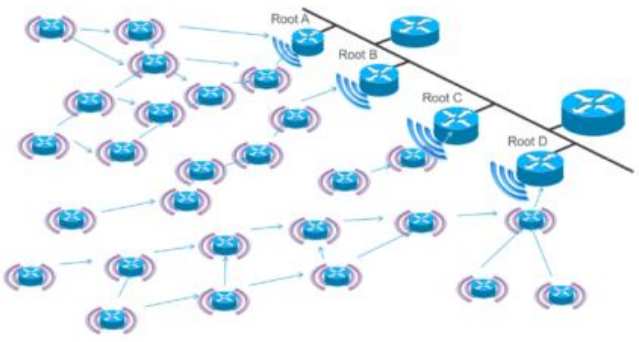
DIS, οι κόμβοι του δικτύου αιτούνται πληροφορίες για τη δρομολόγηση από το σύνολο των γειτόνων τους.
2. Αντικείμενο πληροφορίας DODAG (DODAG Information Object – DIO): Με τα μηνύματα DIO, οι κόμβοι σχηματίζουν το DODAG από τη ρίζα του δικτύου και το διαφημίζουν στο σύνολο των γειτόνων τους.
3. Αντικείμενο διαφήμισης προορισμού (Destination Advertisement Object – DAO): Με τα μηνύματα DAO οι κόμβοι έχουν τη δυνατότητα να έχουν πρόσβαση σε όλο το DODAG.
4. Αναγνώριση αντικειμένου διαφήμισης προορισμού (Destination Advertisement Object Acknowledgement – DAO-ACK): Τα μηνύματα DAO-ACK αποτελούν μηνύματα επιβεβαίωσης των DAO, που στοχεύουν στην εξασφάλιση της αξιοπιστίας μίας διαδρομής είτε εγγράφεται στο DODAG είτε αφαιρείται από αυτό.

Σύμφωνα με τη μελέτη [10] προκύπτει η λειτουργία των τεσσάρων παραπάνω μηνυμάτων. Γενικά, Τα μηνύματα DIS και DIO χρησιμοποιούνται στο RPL για τον σχηματισμό της τοπολογίας του δικτύου και την προς τα πάνω δρομολόγηση. Τα DAO και DAO-ACK μηνύματα με τη σειρά τους συμπληρώνουν το DODAG με διαδρομές που ασχολούνται με την προς τα κάτω δρομολόγηση.

Το πρωτόκολλο RPL είναι ένα πρωτόκολλο διανύσματος απόστασης (DV) που διαχειρίζεται αποτελεσματικά τη βελτιστοποίηση της διαδρομής και το κόστος ελέγχου. Βελτιστοποιεί τις διαδρομές ξεκινώντας από τη ρίζα του RPL DODAG χρησιμοποιώντας μηνύματα ελέγχου. Οι διαδρομές μεταξύ των συσκευών επεκτείνονται μέσω ενός κοινού γονέα, βελτιστοποιώντας τη χρήση προεπιλεγμένων διαδρομών και μειώνοντας τα έξοδα που σχετίζονται με τα μηνύματα ελέγχου και τις πληροφορίες κατάστασης δρομολόγησης. Η συχνότητα των μηνυμάτων ελέγχου μπορεί να είναι ελάχιστη, αλλά ενδέχεται να υπάρχουν καθυστερήσεις στην επισκευή κατεστραμμένων διαδρομών. Οι πληροφορίες πακέτων RPL στα πακέτα δεδομένων βοηθούν στον εντοπισμό και την εξάλειψη των ξεπερασμένων διαδρομών και των βρόχων. Οι χαλασμένες διαδρομές μπορούν να παραμείνουν χωρίς να διαταράσσεται η λειτουργία του δικτύου και δεν δαπανάται ενέργεια για την επιδιόρθωσή τους.

3.3.1 Διαδικασία δρομολόγησης

Κατά την εκκίνηση της δρομολόγηση με RPL αποστέλλονται μηνύματα DIOs πολλαπλής διανομής βάση του αλγορίθμου Trickle [20], ανά χρονική περίοδο, από τον κόμβο ρίζα του δικτύου με στόχο τη διαφήμιση του ιδίου και του DODAG του και θα περιμένει έως ότου και άλλοι κόμβοι συμπεριληφθούν στο DODAG του. Εάν ένας κόμβος ενδιαφέρεται να ενταχθεί στο δίκτυο DODAG που διαφημίζει η ρίζα, χρειάζεται να αποστείλει DIS πολλαπλής διανομής προκειμένου να ζητήσει μηνύματα DIO από τους γείτονες, χωρίς να περιμένει παθητικά μέχρι ένα μήνυμα τύπου DIO περάσει από αυτόν. Μόλις ο κόμβος εκλάβει ένα μήνυμα τύπου DIO, έχει τη δυνατότητα ένταξής του μέσα στο DODAG προχωρά στη διαδικασία επιλογής γονέα, όπως του ορίζει η αντικειμενική συνάρτηση που χρησιμοποιείται στη συγκεκριμένη περίπτωση.



Εικόνα 3.2 : Παράδειγμα τοπολογίας DODAG.
Πηγή : IETF 6TiSCH: A Tutorial[10]

Για τη διαδικασία της δρομολόγησης η IETF έχει ορίσει δύο αντικειμενικές συναρτήσεις, την OF0 και την MRHOF. Η OF0 είναι μία αρκετά απλοποιημένη αντικειμενική συνάρτηση, η οποία έχει την ικανότητα εξυπηρέτησης ενσύρματων δικτύων, όπου αξιοποιείται ο αριθμός μεταπηδήσεων, και την ικανότητα προσαρμογής και σε άλλες μετρικές. Η αντικειμενική συνάρτηση MRHOF χρησιμοποιεί τη μετρική ποιότητας σύνδεσης (Expected Transmission Count – ETX) , με στόχο να αποφανθεί αρχικά τον προτιμώμενο γονέα και γενικά την καλύτερη δυνατή διαδρομή προς τη ρίζα. Οι δύο αντικειμενικές συναρτήσεις λειτουργούν ξεχωριστά, αναλόγως των μετρήσεων που χρησιμοποιούνται και των περιορισμών που έχουν τεθεί.

Στη συνέχεια, ο κόμβος θα διαφημίσει τον γονέα του στο DODAG αποστέλλοντας ένα μήνυμα τύπου DAO απευθείας στη ρίζα, η οποία θα αποθηκεύσει στον πίνακα δρομολόγησής της τη νέα σχέση γονέα-παιδιού που παράχθηκε. Μόλις γίνει η αποθήκευση της νέας σχέσης στη ρίζα, εκείνη στέλνει με τη σειρά της ένα μήνυμα DAO-ACK, ώστε να ενημερώσει τον κόμβο ότι αναγνωρίζει το μήνυμα DAO που έστειλε νωρίτερα στη διαδικασία. Έτσι, ο καινούριος κόμβος του DODAG γνωρίζει ότι είναι πλέον προσβάσιμος από τη στιγμή που λαμβάνει το μήνυμα επιβεβαίωσης από τη ρίζα. Ο καινούριος κόμβος του DODAG βρίσκεται σε θέση να μπορεί να διαφημίσει το DODAG του στέλνοντας με τη σειρά του DIOs πολλαπλής διανομής, τα οποία εμπεριέχουν την απόστασή του από τη ρίζα του DODAG (rank).

Τέλος, ως αποτέλεσμα ακρόασης του DIO που στέλνει ο καινούριος κόμβος του DODAG, οι υπόλοιποι κόμβοι θα ενημερώσουν τον πίνακα γειτνίασής τους και θα έχουν τη δυνατότητα επιλογής ενός γονέα βάση των νέων πληροφοριών. Με αυτόν τον τρόπο, οι συμμετέχοντες κόμβοι συμβάλλουν στην ανάπτυξη μιας τοπολογίας δικτύου πολλαπλών διαδρομών. Για τη διατήρηση της αποτελεσματικής τοπολογίας, οι κόμβοι κάνουν ελέγχους ποιότητας σύνδεσης με τους γείτονές τους και ενημερώνουν τους γονείς τους για τυχόν αλλαγές καθ' όλη τη διάρκεια λειτουργίας του δικτύου.

4. Ζητήματα ασφαλείας 6TiSCH

Τα δίκτυα 6TiSCH, όπως έχει ήδη αναφερθεί στα προηγούμενα κεφάλαια, χρησιμοποιούνται κατά κύριο λόγο σε βιομηχανικές διαδικασίες. Εκεί χρησιμοποιούνται περιορισμένοι κόμβοι , όσον αφορά τους πόρους που μπορούν να διαθέτουν, ενέργεια , μνήμη κ.ο.κ.. Αποτελεσματικό για τη διαδικασία της σωστής κατανομής των πόρων είναι το πρωτόκολλο RPL (Κεφ. 3.3). Στη βιομηχανική , και όχι μόνο διαδικασία, είναι απαραίτητο οι περιορισμένοι κόμβοι να βρίσκονται σε ένα δίκτυο ασφαλές, το οποίο μπορεί να αποτρέψει επιθέσεις προς αυτό, ώστε να μην υπάρχει χαμένο φορτίο και χρήση μεγάλου όγκου ενέργειας. Τα είδη των επιθέσεων που μπορούν να δεχτούν τα δίκτυα 6TiSCH είναι δύο, επιθέσεις στο πρωτόκολλο 6top κατά τη διαδικασία της συναλλαγής πληροφοριών και επιθέσεις στο RPL, δηλαδή στην τοπολογία του δικτύου.

Στην ενότητα θα αναφερθεί αρχικά το ελάχιστο προφίλ ασφαλείας του 6TiSCH (Minimal 6TiSCH security Profile) (Κεφ, 4.1), οι βασικοί μηχανισμοί ασφαλείας (κεφάλαιο 4.3) και τεχνικές αυτοθεραπείας του RPL (κεφάλαιο 4.2). Στη συνέχεια θα ανασκοπηθούν οι επιθέσεις στο RPL και οι υπάρχοντες τρόποι μετριασμού τους (Κεφ 4.4). Τέλος θα ανασκοπηθούν τα δύο είδη επιθέσεων στο πρωτόκολλο 6top, ο διασκορπισμός κυκλοφορίας (traffic dispersion) και οι επιθέσεις υπερφόρτωσης (overloading attacks), καθώς και τρόπος ή τρόπου μετριασμού τους (Κεφ 4.5).

4.1 Ελάχιστο Προφίλ ασφαλείας 6TiSCH

Στα άρθρα [10] και [21] οι συγγραφείς έχουν αναπτύξει τον βασικό τρόπο ασφαλείας για τα δίκτυα 6TiSCH, τον οποίο τον παρέχει το ίδιο το 6TiSCH. Η ελάχιστη ασφάλεια των δικτύων 6TiSCH βασίζεται στο Πρωτόκολλο περιορισμένης σύνδεσης (Constrained Join Protocol – CoJP), και λαμβάνουν μέρος οι τρεις παρακάτω οντότητες. Ο συντονιστής εγγραφής (Join Registrar/Coordinator – JRC), ο ‘pledge’ που θέλει να ενταχθεί μέσα στο δίκτυο και ο διαμεσολαβητής σύνδεσης (Join Proxy – JP), που μεταφέρει πληροφορίες από τον ‘Pledge στο JRC και αντιστρόφως. Βασική αρχή του πρωτοκόλλου CoJP είναι η ύπαρξη ενός προ-διαμοιρασμένο κλειδί κρυπτογράφησης (Pre-Shared Key – PSK) μεταξύ του JRC και του ‘Pledge’.

Τα δίκτυα 6TiSCH ως παράγωγο από το πρωτόκολλο IEEE802.15.4 κληρονομεί τις υπηρεσίες ασφαλείας στο επίπεδο ζεύξης (link-layer) για την προστασία των πλαισίων δεδομένων, όπως η εξασφάλιση της ακρίβειας και της πληρότητας των δεδομένων και την παροχή της επιλογής για την ασφάλεια των πληροφοριών μέσω κρυπτογράφησης.

Κατά τη διάρκεια της διαδικασίας ένταξης του 'Pledge' σε ένα δίκτυο 6TiSCH, τα μηνύματα CoJP που μοιράζονται μεταξύ του pledge και του JRC δεν είναι δυνατό να διασφαλιστούν από το επίπεδο ζεύξης. Για αυτό τον λόγο χρησιμοποιούν το PSK που ως τον βασικό τρόπο διασφάλισης των ανταλλαγών CoJP.

Οι επικοινωνίες που μεταδίδονται εντός του δικτύου ασφαλίζονται κατά κύριο λόγο με τη χρήση κρυπτογράφησης και μέτρων για τη διασφάλιση της ακεραιότητας των δεδομένων. Η αυθεντικοποίηση του πλαισίου δεδομένων παρέχεται σε υψηλό επίπεδο στο εσωτερικό του δικτύου, αλλά δεν υπάρχει εγγύηση αυστηρής αυθεντικοποίησης της πηγής. Αυτή η ευπάθεια επιτρέπει επιθέσεις μέσω παθητικής υποκλοπής, αλλοίωσης μηνυμάτων, έγχυσης και πλαστοπροσωπίας ταυτότητας με χειραγώγηση των πληροφοριών διεύθυνσης. Κατά συνέπεια, οι συναλλαγές 6P είναι ευάλωτες σε απειλές ασφαλείας που εκμεταλλεύονται το κλειδί του δικτύου που συνήθως μοιράζεται για τη διασφάλιση των πλαισίων δεδομένων.

4.2 Τεχνικές αποκατάστασης RPL

Οι συγγραφείς του άρθρου [22] σκιαγραφούν τους δύο διαφορετικούς μηχανισμούς αποκατάστασης του RPL, τον καθολικό (global) και αρκετούς τοπικούς (local). Ο καθολικός μηχανισμός τίθεται σε λειτουργία τη στιγμή που ο κόμβος ρίζας του DODAG, ο οποίος είναι ο μοναδικός με τη δικαιοδοσία να ξεκινήσει μία συνολική επιδιόρθωση, εντοπίσει σημαντικά σφάλματα στην τοπολογία του δικτύου. Στη συνέχεια, παράγεται ένα καινούριο DODAG και οι υπάρχοντες κόμβοι, οι οποίοι προϋπήρχαν στο εγκαταλειμμένο DODAG , προσπαθούν να ενταχθούν στο νέο.

Ο βασικός τρόπος τοπικής επιδιόρθωσης των κατηφορικών διαδρομών στο τοπικό δίκτυο αφορά την επαναφορά των χρονοδιακοπτών DIO trickle και την ανταλλαγή ενημερωμένων μηνυμάτων DIO. Επίσης, γίνεται προσπάθεια διακοπής της σύνδεσης των κόμβων με τον υπάρχον προτιμώμενο γονέα του sub-DODAG, ώστε να επιλεγεί με τη σειρά του ένας νέος κόμβος-γονέας. Ένας εναλλακτικός τρόπος τοπικής επιδιόρθωσης λαμβάνει χώρα, όταν ένας κόμβος δεν έχει πια δυνατότητα σύνδεσης με τον γονέα του και δεν μπορεί να λάβει μηνύματα DIO για μεγάλο χρονικό διάστημα. Στην περίπτωση αυτή, ο κόμβος που δε λαμβάνει τα μηνύματα DIO επιλέγει έναν διαφορετικό προτιμώμενο γονέα από τους διαθέσιμούς για αυτόν, αν υπάρχει, αλλιώς επιστρέφουμε στον βασικό τρόπο τοπικής επιδιόρθωσης.

Το πρωτόκολλο RPL παρέχει δύο βασικούς μηχανισμούς αποκατάστασης, την ανάκτηση βρόχου ασυνέπειας DAG (DAG Inconsistency Loop Recovery) και ανάκτηση βρόχου ασυνέπειας DAO (DAO Inconsistency Loop Recovery). Στον πρώτο μηχανισμό εντοπίζονται οι ασυνέπειες στο DAG, όταν η κατεύθυνση ενός πακέτου αντικρούεται με τη σχέση βαθμίδας μεταξύ του αποστολέα και του κόμβου λήψης, κατά την κάθοδο στην τοπολογία του DODAG η βαθμίδα (Rank) αυξάνεται (Rank(γονέα) < Rank(παιδιού). Ο κόμβος παραλήπτης μεταδίδει το πακέτο με ενεργοποιημένη τη σημαία Rank-Error "R". Εάν η σημαία δεν είναι ενεργοποιημένη, ο παραλήπτης την ενεργοποιεί και μεταδίδει το πακέτο. Όταν η σημαία είναι ενεργοποιημένη, ο παραλήπτης απορρίπτει το πακέτο, μηδενίζει τον χρονοδιακόπτη DIO trickle και ξεκινά μια τοπική λειτουργία επισκευής. Ο δεύτερος μηχανισμός αποκατάστασης διορθώνει ασυνέπειες δικτύου όταν ένας κόμβος λαμβάνει ένα πακέτο από έναν κόμβο-γονέα που προορίζεται για τους κόμβους-παιδιά του. Όταν μια διαδρομή καθίσταται μη διαθέσιμη, το πακέτο αποστέλλεται πίσω με μια σημαία Forwarding-Error ενημερωμένη σε "F" και μια σημαία Down αμετάβλητη, που συμβολίζεται με "O". Εάν ληφθούν διαδρομές με ένδειξη "F", διαγράφονται και αποστέλλονται ξανά.

4.3 Βασικοί μηχανισμοί ασφαλείας RPL

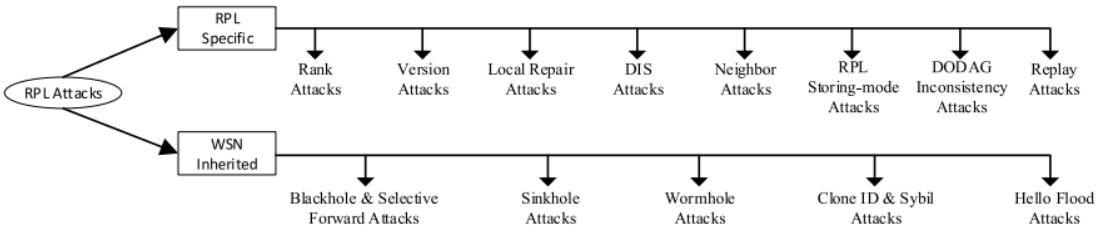
Σύμφωνα με τους συγγραφείς του άρθρου [22] το πρωτόκολλο RPL προσφέρει διάφορα μέτρα ασφαλείας, συμπεριλαμβανομένων μηχανισμών ασφαλείας επιπέδου σύνδεσης για ασφαλή μετάδοση μηνυμάτων. Το πρωτόκολλο διαθέτει τρεις διαφορετικούς τρόπους λειτουργίας. Μη ασφαλής λειτουργίας (Unsecured Mode), προεγκατεστημένη λειτουργίας (Preinstalled mode) και πιστοποιημένη λειτουργία (Authenticated mode).

Στην πρώτη λειτουργία, η οποία είναι και προεπιλεγμένη από το RPL, επιτρέπει στα μηνύματα ελέγχου RPL (DIS,DIO,DAO,DAO-ACK) να μην προστατεύονται. Στη δεύτερη, γίνεται χρήση προεγκατεστημένων κλειδιών στους κόμβους του DODAG για τη διαχείριση και τη δημιουργία ασφαλών αντιγράφων των μηνυμάτων, τα οποία έχουν κρυπτογραφηθεί, του DODAG. Στην τρίτη και τελευταία λειτουργία το RPL απαιτεί από τους κόμβους του DODAG, που έχουν δυνατότητα δρομολόγησης, να αποκτήσουν πρόσθετα κλειδιά, τα οποία έχουν κρυπτογραφηθεί, από μία αρχή αυθεντικοποίησης. Το RPL διαθέτει επίσης ένα προαιρετικό χαρακτηριστικό που ονομάζεται Έλεγχοι συνέπειας, το οποίο χρησιμοποιεί έναν μη επαναλαμβανόμενο αριθμό και αποθηκευμένες πληροφορίες κατάστασης για τον εντοπισμό επιθέσεων επανάληψης.

4.4 Επιθέσεις στο RPL

Τα δίκτυα 6TiSCH είναι άρρηκτα συνδεδεμένα με την επέκταση της έννοιας των δικτύων ασύρματων αισθητήρων (Wireless Sensor Networks – WSNs). Αναμένεται, δηλαδή ότι θα κληρονομήσει και τα προϋπάρχοντα ζητήματα ασφαλείας των δικτύων αυτών. Δίνεται η δυνατότητα, λοιπόν, διαίρεσης των επιθέσεων στο RPL , όπως έχουν κάνει και οι συγγραφείς του άρθρου [22] σε επιθέσεις εξειδικευμένες στο RPL και σε επιθέσεις που έχουν κληρονομηθεί από το WSN, όπως φαίνεται και στην εικόνα 4.1. Είναι σημαντικό να τονιστεί ότι επιθέσεις στο RPL μπορούν να γίνουν μόνο από το εσωτερικό της τοπολογίας και όχι από κάποιον εξωτερικό παράγοντα.

Στο πρώτο είδος επιθέσεων συμπεριλαμβάνονται οι επιθέσεις βαθμίδας (Rank Attacks), επιθέσεις έκδοσης (Version Attacks), επιθέσεις τοπικής επιδιόρθωσης (Local Repair Attacks), Επιθέσεις μηνυμάτων DIS (DIS Attacks), επιθέσεις γειτόνων (Neighbor Attacks), επιθέσεις στην κατάσταση αποθήκευσης (RPL Storing-mode Attacks), επιθέσεις ασυνέπειας του DODAG (DODAG Inconsistency Attacks) και επιθέσεις επανάληψης (Replay Attacks). Ενώ στο δεύτερο συμπεριλαμβάνονται οι επιθέσεις μαύρης τρύπας (Blackhole Attacks), οι επιθέσεις επιλεκτικής προώθησης (Selective Forwards Attacks), επιθέσεις καταβόθρας (Sinkhole Attacks), επιθέσεις σκουληκότρυπας (Wormhole Attacks), επιθέσεις κλωνοποίησης ID (Clone ID Attacks), επιθέσεις Sybil (Sybil Attacks) και επιθέσεις πλημμύρας μηνυμάτων HELLO (HELLO Flood Attacks).



Εικόνα 4.1 Διαχωρισμός επιθέσεων στο RPL.
Πηγή : "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things [22]

4.4.1 Επιθέσεις εξειδικευμένες στο RPL

Οι επιθέσεις που θα ανασκοπηθούν στο κεφάλαιο αυτό, εκμεταλλεύονται κατά κύριο λόγο το πεδίο βαθμίδας και το πεδίο έκδοσης από τα μηνύματα ελέγχου του DODAG, με σκοπό την αλλοίωση και την πλαστογράφηση των μηνυμάτων ελέγχου.

Α. Επιθέσεις Βαθμίδας / Rank Attacks

Στα άρθρα [22-26] δίνεται μία εκτενής ανάπτυξη της επίθεσης βαθμίδας στο RPL , οι συνέπειές τις και οι προτεινόμενοι τρόποι αντιμετώπισης της συγκεκριμένης επίθεσης. Σε ένα δίκτυο 6TiSCH που χρησιμοποιεί ως τοπολογία δικτύου το πρωτόκολλο RPL, υπάρχει το χαρακτηριστικό της βαθμίδας. Κατά την κάθοδο στο DODAG, όπως αναφέρθηκε στο κεφάλαιο 4.2, η βαθμίδα (Rank) αυξάνεται αι οι κόμβοι επιλέγουν γονέα με την καλύτερη δυνατή βαθμίδα.

Στην επίθεση βαθμίδας ο κακόβουλος κόμβος διαδίδει στο δίκτυο έναν μη αληθή αριθμό βαθμίδας, κατά κύριο λόγο χαμηλότερο από τον δικό του, ώστε να αλλάξει θέση στο DODAG και να βρεθεί κοντά στη ρίζα. Με αυτόν τον τρόπο ο κακόβουλος κόμβος γίνεται ελκυστικός για τους κόμβους παιδιά και εν συνεχεία προσελκύει μεγάλο όγκο της κίνησης που στοχεύει προς τη ρίζα της τοπολογίας. Οι επιθέσεις βαθμίδας χωρίζονται σε τρία είδη επιθέσεων, σε επιθέσεις μειωμένης βαθμίδας (Decreased Rank Attacks), σε επιθέσεις αυξημένης βαθμίδας (Increased Rank Attack) και επιθέσεις χειρότερου γονιού (Worst Parent Attacks) [22,24].

Στην πρώτη περίπτωση, οι κακόβουλοι κόμβοι προσπαθούν να αποκτήσουν μία πλεονεκτική θέση κοντά στον κόμβο ρίζα δίδοντας ψευδείς χαμηλότερες βαθμίδες, από αυτή που του αναλογεί. Στη δεύτερη περίπτωση, οι κακόβουλοι κόμβοι θέτουν τον εαυτό τους στις λιγότερο βέλτιστες θέσεις του DODAG, κοντά στα φύλλα του δέντρου, ώστε να γίνει δύσκολος ο εντοπισμός τους. Στην τρίτη περίπωση επίθεσης, οι κακόβουλοι κόμβοι επιλέγουν σκόπιμα ένα κόμβο γονέα με τη χαμηλότερη δυνατή κατάταξη.

Οι κόμβοι που επιτίθενται στο δίκτυο έχουν τη δυνατότητα να αμφισβητούν συνεχώς ή να εναλλάσσονται μεταξύ υποστήριξης και εναντίωσης στον κανόνα της ιεραρχίας. Στοχεύουν στη διατάραξη της σταθερότητα της δομής του δικτύου τροποποιώντας τον προτιμώμενο γονέα. Οι επιτιθέμενοι έχουν τη δυνατότητα να διανέμουν τα ενημερωμένα δεδομένα τους, μέσω μηνυμάτων DIO, σε κοντινούς κόμβους, ενισχύοντας έτσι το βάρος του ελέγχου. Παρ' όλα αυτά, η διαμόρφωση του δικτύου που περιβάλλει τον επιτιθέμενο κόμβο μπορεί ακόμη να βελτιωθεί. Σε περίπτωση που οι κόμβοι αποτύχουν να ενημερώσουν τις πληροφορίες δρομολόγησής τους, δεν αποστέλλονται πρόσθετα μηνύματα ελέγχου. Ωστόσο, αυτό θα οδηγήσει σε μια μη βέλτιστη τοπολογία, με αποτέλεσμα καθυστερήσεις στην κυκλοφορία χωρίς καμία μορφή ένδειξης.

Ως συνέπειες των παραπάνω επιθέσεων προκύπτουν βάση των [23,25] οι εξής:

i. Δημιουργία μη βέλτιστων διαδρομών στο DODAG και μη χρησιμοποίηση της βέλτιστης προϋπάρχουσας.
ii. Δημιουργία κύκλων στο DODAG.
iii. Καθυστέρηση στο δίκτυο λόγω της δρομολόγησης μέσα από τους επιτιθέμενους κόμβους
iv. Επιβάρυνση στον έλεγχο
v. Αύξηση των συγκρούσεων

Για την ύπαρξη άμυνας ενάντια της συγκεκριμένης επίθεσης οι συγγραφείς των άρθρων [22,23,24,26,27] προτείνουν τρεις διαφορετικούς τρόπους εξάλειψης την επίθεσης, τη μέθοδο

VeRA (Version Number and Rank Attack Authentication), τη μέθοδο TRAIL(Trust Anchor Interconnection Loop) και SVELTE , οι οποίες χρησιμοποιούνται και στις επόμενες επιθέσεις.

I. VeRA: Πρωτόκολλο ασφαλείας που έχει σχεδιαστεί για να ενισχύει την ακεραιότητα και την αυθεντικότητα των επικοινωνιών σε δικτυακά συστήματα, ιδίως σε σενάρια που είναι ευαίσθητα σε επιθέσεις αριθμού έκδοσης και βαθμίδας. Οι επιθέσεις αριθμού έκδοσης και βαθμίδας συχνά εξαπολύονται εναντίον πρωτοκόλλων δρομολόγησης δικτύου, όπου κακόβουλοι κόμβοι διαφημίζουν εσφαλμένες πληροφορίες δρομολόγησης για να διαταράξουν τη λειτουργία του δικτύου. Το VeRA αντιμετωπίζει αυτή την πρόκληση συνδυάζοντας κρυπτογραφικές τεχνικές και μηχανισμούς βασισμένους στην εμπιστοσύνη για την αυθεντικοποίηση των αριθμών έκδοσης και των βαθμίδων που δηλώνουν οι κόμβοι εντός του δικτύου. Οι ψηφιακές υπογραφές χρησιμοποιούνται για να επαληθεύσουν ότι οι πληροφορίες σχετικά με τους αριθμούς έκδοσης και τις βαθμίδες προέρχονται από μια έμπιστη οντότητα και δεν έχουν αλλοιωθεί κατά τη μετάδοσή τους. Επιπλέον, το VeRA αξιοποιεί έναν μηχανισμό για την αξιολόγηση της αξιοπιστίας των κόμβων όσον αφορά τη συμπεριφορά και τη συμβολή τους στο δίκτυο, ο οποίος παρέχει προστασία από την αποδοχή κακόβουλων ενημερώσεων. Αυτό διασφαλίζει ένα υγιές και ασφαλές περιβάλλον δικτύου χωρίς τον κίνδυνο να επιτραπεί στους αντιπάλους να κάνουν κατάχρηση του πρωτοκόλλου για τη διενέργεια επιβλαβών ενεργειών. Στο άρθρο [27] γίνεται μία αναλυτική μελέτη αξιολόγηση του πρωτοκόλλου VeRA.

II. TRAIL: Μέθοδος σχεδιασμένη με σκοπό τον εντοπισμό και τον μετριασμό των τοπολογικών ασυνεπειών στις δομές δικτύων, βελτιώνοντας το πρωτόκολλο VeRA, επιτρέποντας σε κάθε κόμβο εντός ενός δικτύου να επαληθεύει τη διαδρομή σύνδεσής του με τον κεντρικό κόμβο-ρίζα και να ανιχνεύει τυχόν περιπτώσεις αλλοίωσης της κατάταξης. Έχει τη δυνατότητα εντοπισμού του μεγαλύτερου υπο-DODAG που επηρεάζεται από ασυνέπειες στη σειρά κατάταξης. Κατά την ανίχνευση τέτοιων ασυμφωνιών, ο κόμβος ρίζα του επηρεαζόμενου υπο-DODAG μπορεί να ξεκινήσει μια τοπική διαδικασία επιδιόρθωσης ή να διακόψει τη σύνδεση με το προβληματικό υποδέντρο, επιλέγοντας αντ' αυτού εναλλακτικές διαδρομές δρομολόγησης. Το TRAIL λειτουργεί επικυρώνοντας την ανοδική διαδρομή προς τη ρίζα με ένα μήνυμα μετ' επιστροφής, αποφεύγοντας την ανάγκη για πολύπλοκες μεθόδους κρυπτογράφησης. Ένας κόμβος στέλνει ένα μήνυμα δοκιμής, που περιέχει ένα τυχαίο μη-κλειδί, στον γονέα του, ο οποίος στη συνέχεια προσθέτει τον βαθμό του και διαβιβάζει το μήνυμα προς τη ρίζα. Κάθε κόμβος κατά μήκος της διαδρομής ελέγχει ότι ο εισερχόμενος βαθμός είναι διαδοχικά υψηλότερος, εξασφαλίζοντας την ακεραιότητα της σειράς κατάταξης. Εάν διαπιστωθεί ασυμφωνία, το μήνυμα διακόπτεται και λαμβάνονται διορθωτικές ενέργειες. Αυτή η διαδικασία όχι μόνο επιβεβαιώνει τη νομιμότητα της κατάταξης που διαφημίζεται από τον γονέα ενός κόμβου, αλλά και επαληθεύει την ακεραιότητα της δομής του δικτύου χωρίς να βασίζεται σε βαριά κρυπτογράφηση, αν και σημειώνει προβλήματα κλιμάκωσης λόγω της γραμμικής αύξησης της επιβάρυνσης των μηνυμάτων με το μέγεθος του δικτύου. [26]

III. SVELTE Σύστημα ανίχνευσης εισβολών (Intrusion Detection System - IDS) που δημιουργήθηκε για να διασφαλίζει τα δίκτυα RPL από διάφορες απειλές ασφαλείας από το εσωτερικό και το εξωτερικό Το SVELTE χρησιμοποιεί έναν συνδυασμό κεντρικών και κατανεμημένων μηχανισμών, καθώς οι πιο εντατικές διεργασίες IDS μεταφέρονται στον 6LowPAN Border Router (6BR), ενώ οι ελαφρύτερες εργασίες αποστέλλονται στους υπόλοιπους κόμβους του δικτύου. Οι κρυπτογραφημένες επικοινωνίες βασίζονται σε πρότυπα ασφαλείας IPv6 όπως το IPsec, το CoAP ή το DLTS, αλλά δεν προστέθηκαν αναγνωριστικές ετικέτες στις επικεφαλίδες IP. Το SVELTE αποτελείται από έναν χαρτογράφο 6LoWPAN, ένα μικροσκοπικό τείχος προστασίας και μια μονάδα ανίχνευσης εισβολής. Αυτό το σύστημα είναι επίσης μη ανιχνεύσιμο από κακόβουλους κόμβους και παρέχει αποτελεσματική παρακολούθηση της δραστηριότητας και εντοπισμό επιθέσεων επιλεκτικής προώθησης [24].

Β. Επιθέσεις έκδοσης / Version Attacks

Σύμφωνα με τις μελέτες [22-24,26] οι επιθέσεις αριθμού έκδοσης εκμεταλλεύονται τον καθολικό τρόπο αποκατάστασης του DODAG, όπου αυξάνεται η έκδοσή του σε κάθε αποκατάσταση, αυξάνοντας κακόβουλα τον αριθμό έκδοσης του DODAG, οδηγώντας έτσι σε μια συνολική διαδικασία επιδιόρθωσης και ανακατασκευής της τοπολογίας του RPL από τους κόμβους,

επιτρέποντας την εξαπόλυση περαιτέρω επιθέσεων ή προκαλώντας διακοπή της λειτουργίας του δικτύου λόγω εξάντλησης των πόρων.

Η επίθεση αυτή βασίζεται στην έλλειψη μηχανισμών στο RPL που να επαληθεύουν την ακεραιότητα των κοινοποιούμενων αριθμών έκδοσης. Ως εκ τούτου, ο επιτιθέμενος μπορεί να εισάγει ψευδή μηνύματα DIO για να προκαλέσει ανεπιθύμητες αλλαγές στην τοπολογία, όπου δημιουργούνται μη βέλτιστες διαμορφώσεις δικτύου, πρόσθετες ασυνέπειες τοπολογίας και βρόχοι δρομολόγησης, οι οποίοι δημιουργούνται ειδικά από τους κόμβους του επιτιθέμενου και διαδίδονται περαιτέρω στο δίκτυο επηρεάζοντας τους κόμβους που βρίσκονται κοντά στον επιτιθέμενο. Οι επιπτώσεις αυτής της επίθεσης μπορεί να είναι σοβαρές, καθώς ο λόγος παράδοσης πακέτων μειώνεται σημαντικά (πάνω από 50% υπό ορισμένες συνθήκες), η μέση καθυστέρηση από άκρο σε άκρο μπορεί να αυξηθεί πάνω από έξι φορές, η επιβάρυνση ελέγχου μπορεί να φτάσει το 7500% και η κατανάλωση ενέργειας ανά αποστελλόμενο πακέτο μπορεί επίσης να αυξηθεί έως και 265%, υποβαθμίζοντας έτσι σοβαρά την απόδοση του δικτύου μέσω της σκόπιμης εξάντλησης των πόρων των κόμβων.

Όταν ένας κακόβουλος κόμβος εκμεταλλεύεται αυτή την αρχική αναδιοργάνωση σε όλο το δίκτυο, που ξεκίνησε όταν λαμβάνεται η αύξησή του στον αριθμό έκδοσης, μπορεί να προκαλέσει εκτεταμένη παραμόρφωση του δικτύου και να επιδεινώσει μόνο τον αντίκτυπο των προαναφερθέντων ζητημάτων. Άμυνες όπως το VeRa, το οποίο συμβάλει στον μετριασμό αυτών των επιθέσεων, επαληθεύοντας τους αριθμούς έκδοσης μέσω ψηφιακών υπογραφών και MAC ή το TRAIL, οι οποίες διασφαλίζουν την αυθεντικότητα των αλλαγών του αριθμού έκδοσης και της τοπολογίας είναι απολύτως απαραίτητες για τον μετριασμό των επιπτώσεών τους.

Γ. Επιθέσεις τοπικής επιδιόρθωσης / Local Repair Attacks

Οι μελέτες [22-24] αναφέρονται για τη σημαντικότητα της συγκεκριμένης απειλής σε ένα δίκτυο 6TiSCH. Ο κακόβουλος κόμβος μεταδίδει σήματα τοπικής επιδιόρθωσης, ενώ απουσιάζει κάποιο μεμπτό πρόβλημα στο δίκτυο. Με αυτόν τον τρόπο, ο κακόβουλος κόμβος υποχρεώνει το σύνολο των γειτόνων του στην επανεκτίμηση και επαναδημιουργίας διαδρομών στην τοπολογία μέσω αυτού. Όπως αναλύθηκε στο κεφάλαιο 4.2 το πρωτόκολλο RPL κάνει χρήση τοπικών και καθολικών αποκαταστάσεων, ώστε να είναι ικανό να ελέγχει ένα σταθερό δίκτυο.

Βέβαια, ο μηχανισμός τοπικής επιδιόρθωσης είναι σχεδιασμένος, ώστε να εξαρτάται από τους ενδιάμεσους κόμβους του δικτύου. Αυτή την εμπιστοσύνη που έχει το πρωτόκολλο στους κόμβους του , κάποιοι κακόβουλοι την εκμεταλλεύονται. Οι κακόβουλοι κόμβοι, λόγω της τυφλής εμπιστοσύνης του RPL, έχουν τη δικαιοδοσία να ξεκινούν περιττές τοπικές επισκευές διαδίδοντας ψευδείς πληροφορίες ή μηνύματα DIO με λανθασμένες βαθμίδες. Συνέπεια της επίθεσης αυτής είναι η επιβάρυνση των μηνυμάτων ελέγχου, η εξάντληση των πόρων των περιορισμένων κόμβων και εμμέσως η μείωση του λόγου παράδοσης του δικτύου. Τονίζεται όμως, ότι η καθυστέρηση από άκρο σε άκρο δεν επηρεάζεται , εφόσον η ιδανική δομή του δικτύου παραμένει ως έχει.

Οι συγγραφείς των παραπάνω μελετών προτείνουν τη χρήση κυρίως της TRAIL και της SVELTE ως τρόπους εξομάλυνσης της επίθεσης, αλλά δεν έχει αξιολογηθεί η επιτυχία τους μέχρι στιγμής.

Δ. Επιθέσεις μηνυμάτων DIS / DIS Attacks

Οι συγγραφείς των μελετών [22-24] και κυρίως της [20] αναφέρονται στην επίθεση DIS και τις επιπτώσεις της στο δίκτυο. Η επίθεση DIS, όπως και η επίθεση τοπικής επιδιόρθωσης χρησιμοποιεί για κακόβουλο λόγο τη διαδικασία του πρωτοκόλλου RPL για την ενσωμάτωση νέων κόμβων στο δίκτυο. Ο επιτιθέμενος αποστέλλει στο σύνολο των γειτόνων του μηνύματα DIS, με αποτέλεσμα να χειραγωγεί τις προϋποθέσεις επαναφοράς του αλγόριθμου Trickle. Οι γείτονες με τη σειρά τους ξεκινούν να αποστέλλουν μηνύματα DIO (Unicast DIS) ή να ξεκινούν τη διαδικασία τοπικής επιδιόρθωσης (Broadcast DIS).

Αποτέλεσμα της εκμετάλλευσης της αποστολής των μηνυμάτων DIS είναι η χειραγώγηση της ροής των μηνυμάτων ελέγχου του δικτύου, με αποτέλεσμα να υπάρχει αυξημένη καθυστέρηση από άκρο σε άκρο, επιπλέον επιβάρυνση ελέγχου, εξάντληση ενεργειακών πόρων και πιθανή συμφόρηση του δικτύου. Στο άρθρο [22] συγκεκριμένα αναφέρεται και η διαφορά μεταξύ του Unicast DIS Attack με του Broadcast DIS Attack. Στην πρώτη περίπτωση διαταράσσεται η διαδικασία ανταλλαγής μηνυμάτων DIO μεταξύ των κόμβων , ενώ στη δεύτερη περίπτωση διπλασιάζεται η καθυστέρηση μηνυμάτων από άκρο σε άκρο.

Η πρόκληση που παρουσιάζουν αυτές οι επιθέσεις για τα συστήματα ανίχνευσης εισβολών (IDS) που βασίζονται σε ανωμαλίες ή προδιαγραφές είναι σημαντική, δεδομένης της διακριτικής αλλά και επιδραστικής φύσης τους. Παρά τη συνεχιζόμενη απειλή των επιθέσεων DIS, η έρευνα για εξειδικευμένες στρατηγικές μετριασμού παραμένει περιορισμένη και δεν υπάρχει κάποιος συγκεκριμένος τρόπος μετριασμού της επίθεσης αυτής. Οι προσπάθειες του IETF για την προσαρμογή των αποκρίσεων των κόμβων στα μηνύματα DIS σηματοδοτούν μια πιθανή προσέγγιση για τον μετριασμό αυτών των επιθέσεων, αλλά απαιτούν περαιτέρω διερεύνηση και επικύρωση.

Ε. Επιθέσεις γειτόνων / Neighbor Attacks

Σύμφωνα με τα άρθρα [22-24] η επίθεση γειτόνων αναγνωρίζεται ως μια ιδιαίτερα αποδιοργανωτική απειλή. Αυτή η μορφή επίθεσης περιλαμβάνει έναν κακόβουλο κόμβο που απλώς προωθεί τα μηνύματα DIO που λαμβάνει σε γειτονικούς κόμβους χωρίς καμία τροποποίηση. Στόχος αυτής της στρατηγικής είναι η παραποίηση της αντιλαμβανόμενης τοπολογίας του δικτύου, προκαλώντας τους κόμβους να δίνουν λανθασμένα προτεραιότητα σε έναν κόμβο εκτός εμβέλειας με πλεονεκτική θέση ως προτιμώμενο γονέα τους, λόγω της αμετάβλητης διάδοσης των μηνυμάτων DIO από τον αντίπαλο.

Οι επιπτώσεις των επιθέσεων γειτόνων, αν και δεν είναι εμφανείς, εκδηλώνουν ,κυρίως, μία μικρή αύξηση στην καθυστέρηση από άκρο σε άκρο. Ωστόσο, έχει την ικανότητα να προκαλέσει πολύ μεγαλύτερη ζημία στο δίκτυο, αν συνδυαστεί και με άλλα είδη επιθέσεων στο RPL, όπως οι επιθέσεις DIS. Στη συγκεκριμένη περίπτωση, ένας κακόβουλος κόμβος θα μπορούσε να εκμεταλλευτεί τις επιθέσεις DIS για να συλλάβει μηνύματα DIO με ανώτερες μετρήσεις και να τα αναπτύξει σε μια επίθεση γείτονα, μεγεθύνοντας έτσι σημαντικά τον αποδιοργανωτικό της αντίκτυπο.

Η αντιμετώπιση αυτών των επιθέσεων είναι ιδιαίτερα δύσκολη λόγω της κρυφής φύσης των ενεργειών του κακόβουλου κόμβου στο δίκτυο. Αν και τα συγκεκριμένα μέτρα ασφαλείας συζητούνται ελάχιστα στην υπάρχουσα βιβλιογραφία, ορισμένα συστήματα ανίχνευσης εισβολών (IDS), όπως τα SVELTE και τα IDS που βασίζονται στις προδιαγραφές RPL, φαίνεται να έχουν δυνατότητες εντοπισμού των επιθέσεων αυτών. Επιπλέον, στρατηγικές ελέγχου που βασίζονται στην τοπολογία του δικτύου, οι οποίες λαμβάνουν υπόψη τα δεδομένα θέσης και εμβέλειας μετάδοσης, μπορεί να προσφέρουν μία καλή προσέγγιση για την ανίχνευση τέτοιων απειλών.

Η συγκεκριμένη κατηγορία επίθεσης, συνδυασμένη με άλλες μορφές κακόβουλων δραστηριοτήτων, αποτελεί μια εξελιγμένη πρόκληση για την ποιότητα των υπηρεσιών στα δίκτυα 6TiSCH. Η πολυπλοκότητα της ανίχνευσης και του μετριασμού τέτοιων απειλών υπογραμμίζει την κρίσιμη ανάγκη για συνεχή έρευνα και την ανάπτυξη προηγμένων, προσαρμοσμένων λύσεων ασφάλειας που αντιμετωπίζουν τις ξεχωριστές προκλήσεις που παρουσιάζουν οι ρυθμίσεις δικτύων που βασίζονται σε RPL.

ΣΤ. Επιθέσεις στην κατάσταση αποθήκευσης / RPL Storing-mode Attacks

Στις μελέτες [22,24] γίνεται ανάλυση των επιθέσεων το RPL , όταν αυτό βρίσκεται σε κατάσταση

αποθήκευσης (storing-mode). Οι συγγραφείς τονίζουν ότι το προαναφερθέν είδος επίθεσης στοχεύει στην παραβίαση της ακεραιότητας των επόμενων πινάκων δρομολόγησης. Οι επιθέσεις μπορούν να χωριστούν σε τρείς υποκατηγορίες : (i) Επιθέσεις υπερφόρτωσης πινάκων δρομολόγησης, (ii) επιθέσεις ασυνέπειας DAO και (iii) επιθέσεις παραποίησης πινάκων δρομολόγησης.

Στην πρώτη υποκατηγορία, ένας κακόβουλος κόμβος υπερφορτώνει με διαδρομές, οι οποίες στην πραγματικότητα δεν υπάρχουν μέσα στο δίκτυο, τον πίνακα δρομολόγησης ενός κόμβου και τις μεταφέρει με μηνύματα DAO στους γονείς του κόμβου. Με αυτόν τον τρόπο, μόλις γεμίσει ο πίνακας δρομολόγησης του κόμβου, δεν θα μπορεί να δέχεται αυθεντικά μηνύματα DAO από καλόβουλους κόμβους και να κατασκευάζει ακριβείς διαδρομές [24]. Στη δεύτερη υποκατηγορία, ο κακόβουλος κόμβος εκμεταλλεύεται την μηχανισμό επιδιόρθωσης του RPL. Αποτέλεσμα που μπορεί να προκαλέσει η συγκεκριμένη επίθεση είναι η απομόνωση ενός υπό-DODAG από το δίκτυο ή στη δημιουργία μη βέλτιστων διαδρομών στο δίκτυο [22]. Στην τρίτη υποκατηγορία επίθεσης, ένας κακόβουλος κόμβος αποστέλλει ψευδείς πληροφορίες δρομολόγησης σε άλλους έγκυρους, και τις προσθέτους στα DAO μηνύματα [24].

Οι δύο τελευταίες υποκατηγορίες επιθέσεων RPL στην κατάσταση αποθήκευσης έχουν ως αποτέλεσμα την αύξηση της καθυστέρησης από άκρο σε άκρο, και τον χαμηλό λόγο παράδοσης πακέτων (Packet Deliver Ratio – PDR) [24], ενώ για την πρώτη δεν έχουν αναλυθεί οι επιπτώσεις της στο δίκτυο [22].

Μέχρι πρότινος, δεν έχει υπάρξει ένας καθιερωμένος τρόπος αντιμετώπισης μετριασμού των παραπάνω επιθέσεων. Έχει προταθεί η εφαρμογή ενός δυναμικού μηχανισμού κατωφλιού (Dynamic threshold Mechanism – DTM), ο οποίος θα έχει τη δυνατότητα να καθορίζει χρόνο και κυρίως τον ρυθμό επαναφοράς του χρονοδιακόπτη του αλγορίθμου Trickle. Μερικές προσομοιώσεις της DTM αποδεικνύουν ι την αποτελεσματικότητά της στην ελαχιστοποίηση της επιβάρυνσης ελέγχου, των απωλειών πακέτων και της χρήσης ενέργειας στο δίκτυο [28].

Ζ. Επιθέσεις ασυνέπειας DODAG / DODAG Inconsistency Attacks

Σύμφωνα με τα άρθρα [22,24], οι επιθέσεις ασυνέπειας DODAG γίνεται εκμετάλλευση των προεπιλεγμένων λειτουργιών αυτοθεραπείας που χρησιμοποιεί το RPL. Οι κακόβουλοι κόμβοι χειραγωγούν τις σημαίες ‘O’ και ‘R’ στις επικεφαλίδες των πακέτων. Η σημαία ‘O’ χρησιμοποιείται από τους κακόβουλους κόμβους κατά την κίνηση πάνω ή κάτω στο RPL, ενώ η σημαία ‘R’ όταν αιτούνται αίτημα για μία επιδιόρθωση. Με αυτή τη χειραγώγηση των σημαιών, τα πακέτα που έχουν αποσταλεί από τους κακόβουλους κόμβους υποχρεώνουν τους έγκυρους κόμβους να τα απορρίψουν και εν συνεχεία να αιτηθούν τοπική επιδιόρθωση. Κύρια συνέπεια της επίθεσης είναι η επιβράδυνση της απόδοσης του δικτύου

Η βιβλιογραφία της επίθεσης δεν επιδεικνύει κάποιον αποτελεσματικό μηχανισμό για την αντιμετώπιση της παραπάνω επίθεσης. Έχει προταθεί ένας απλός περιορισμός της συχνότητας που χρησιμοποιείται ο χρονοδιακόπτης του αλγορίθμου trickle, ο οποίος όμως δεν είναι αρκετός για την πρόληψη από την επίθεση. Η αντιμετώπιση των επιθέσεων ασυνέπειας DAG απαιτεί βαθιά κατανόηση του πρωτοκόλλου RPL και την ανάπτυξη προηγμένων στρατηγικών ανίχνευσης και μετριασμού που μπορούν να προσαρμόζονται στη δυναμική φύση των συνθηκών και των απειλών του δικτύου.

Η. Επιθέσεις επανάληψης / Replay Attacks

Βάση των μελετών [22,24,26,29], οι επιθέσεις επανάληψης θεωρούνται από τις πιο επικίνδυνες για την ασφάλεια των δικτύων 6TiSCH. Οι επιθέσεις επανάληψης στοχεύουν στη μείωση της σταθερότητας της τοπολογίας του δικτύου και της αποδοτικότητας της δρομολόγησης. Μία επίθεση επανάληψης λαμβάνει μέρος με έναν πολύ απλό τρόπο. Οι κακόβουλοι κόμβοι που εξαπολύουν την επίθεση συλλαμβάνουν μηνύματα DIO,DIS και DAO από τους γείτονες και εκείνοι με τη σειρά τους τα αναμεταδίδουν, με σκοπό την εισαγωγή ξεπερασμένων

πληροφοριών στο δίκτυο.

Μία παρεμφερής επίθεση είναι και η επίθεση καταστολής DIO (DIO Suppression Attack), η οποία επηρεάζει τον αλγόριθμο Trickle. Η λογική της επίθεσης , όπως και της μητρικής της είναι πολύ απλή. Ο κακόβουλος κόμβος απλά επαναλαμβάνει συνεχώς μηνύματα DIO, που έχει κρυφακούσει από τους άμεσους γείτονές του, στο σύνολο των γειτόνων του. Όσο περισσότερα DIO μηνύματα λάβουν οι έγκυροι κόμβο, τόσο συγκρατούν τα δικά τους DIO μηνύματα. Αυτό έχει ως αποτέλεσμα αρκετοί έγκυροι κόμβοι του δικτύου να παραμείνουν στην αφάνεια[29].

Και στις δύο περιπτώσεις, επιβραδύνεται η δρομολόγηση στο δίκτυο, μειώνεται ο ρυθμός παράδοσης πακέτων, αλλά και υπάρχει περίπτωση να αποκοπεί ένα υπο-DODAG από το σύνολο του δικτύου. Το RPL παρέχει έναν ικανό τρόπου μετρίασης της επίθεσης, την προαιρετική λειτουργία προστασίας επανάληψης. Βέβαια, ο χρόνος σχηματισμού δικτύου επιβαρύνεται, αυξάνεται η κατανάλωση ενέργειας των κόμβων και επιβαρύνεται ο έλεγχος πάνω στο δίκτυο.

Μία ακόμη πιο επικίνδυνη επίθεση είναι η επίθεση επανάληψης κατάταξης [26]. Οι κακόβουλοι κόμβοι χειραγωγούν τις πληροφορίες βαθμίδας που δέχονται από τους γονείς τους και χρησιμοποιεί τη βαθμίδα του γονέα του για τη διαφήμιση του ιδίου στο δίκτυο. Έτσι, τοποθετούνται υψηλά στην ιεραρχία του RPL. Παρά τον μηχανισμό προστασίας επανάληψης του RPL, τα δυναμικά διαμορφωμένα δίκτυα παραμένουν εκτεθειμένα και ευάλωτα. Η αντιμετώπιση αυτών των τρωτών σημείων απαιτεί ειδική προσπάθεια για την ανάπτυξη και την εφαρμογή προσαρμοστικών και ισχυρών μέτρων ασφαλείας.

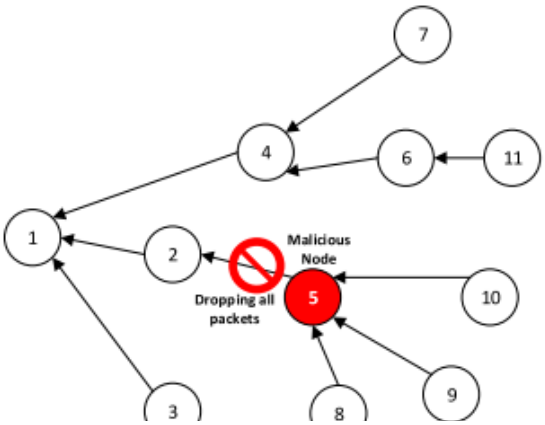
4.4.2 Κληρονομημένες επιθέσεις από WSN.

Ένα δίκτυο 6TiSCH αποτελεί μέλος του IoT. Το IoT με τη σειρά του εφαρμόζει τους κανόνες από τα WSN. Από τις έρευνες [22,23,30] προκύπτει το γεγονός ότι αρκετές, αν όχι όλες, από τις επιθέσεις στα WSNs έχουν προσαρμοστεί και στο IoT, όπου ανήκει και το δίκτυο 6TiSCH. Οι επιθέσεις που θα ανασκοπηθούν στο κεφάλαιο αφορούν επιθέσεις δρομολόγησης.

Α. Επιθέσεις επιλεκτικής προώθησης και μαύρης τρύπας / Selective forward and blackhole Attacks

Σύμφωνα με τους συγγραφείς των [23,30] οι επιθέσεις επιλεκτικής προώθησης αποτελούν σημαντικό κίνδυνο για την ασφάλεια ενός δικτύου 6TiSCH. Αφορούν, κατά βάση, δίκτυα πολλαπλών διαδρομών (multihop), όπου θεωρητικά οι κόμβοι μεταφέρουν με συνέπεια τα μηνύματα στο δίκτυο. Στη συγκεκριμένη επίθεση, οι κακόβουλοι κόμβοι εμποδίζουν τη μετάδοση συγκεκριμένων μηνυμάτων.

Κατά παρόμοιο τρόπο λειτουργούν και οι επιθέσεις μαύρης τρύπας. Στην επίθεση μαύρης τρύπας, ένας κόμβος επιλέγει σκόπιμα να μην μεταφέρει, και να «ρίξει», πακέτα θέτοντας σε κίνδυνο την ανακάλυψη και υποστηρίζοντας την παράκαμψη από τους γειτονικούς κόμβους, έως πιο συγκαλυμμένες μεθόδους όπου ο επιτιθέμενος προωθεί επιλεκτικά πακέτα για να μην κινήσει υποψίες. Στόχος της είναι η διακοπή της επικοινωνίας ή η τροποποίηση της ροής δεδομένων από συγκεκριμένους κόμβους, διασφαλίζοντας παράλληλα ότι οι υπόλοιποι κόμβοι συνεχίζουν να λειτουργούν κανονικά.



Εικόνα 4.2: Παράδειγμα επίθεσης μαύρης τρύπας.
Πηγή : Routing Attacks and Mitigation Methods for RPL-Based Internet of Things [22]

Τόσο στις επιθέσεις μαύρης τρύπας, όσο και στις επιθέσεις επιλεκτικής προώθησης η αποτελεσματικότητά τους αυξάνεται εάν συμμετέχουν ενεργά στη διαδικασία ροής δεδομένων. Η μελέτη [23] υπογραμμίζει τις επιπτώσεις και των δύο επιθέσεων στο δίκτυο. Αρχικά, το δίκτυο γίνεται ασταθές λόγω της αυξημένης ποσότητας μηνυμάτων DIO που διοχετεύονται και δημιουργούνται καθυστερήσεις στη διάδοση των πακέτων δεδομένων.

Ο Raoof κ.α στη μελέτη [22] έχουν συγκεντρώσει το σύνολο των τρόπων μετριασμού των παραπάνω δύο επιθέσεων. Η πρώτη επίθεση αντιμετωπίζεται κυρίως με τη χρήση κρυπτογράφησης , ενώ η δεύτερη με συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems – IDS). Δύο βασικές ιδέες αντιμετώπισης των επιθέσεων είναι η δρομολόγηση πηγής, όπου μετριάζεται η επίπτωση της επίθεσης επιλεκτικής προώθησης, και η κρυπτογράφηση πακέτων, όπου δεν επιτρέπεται στον κακόβουλο κόμβο να γνωρίζει τα πρωτόκολλα που βρίσκονται σε χρήση.

Στη συνέχεια, προτείνονται δύο τεχνικές βάση επιβεβαίωσης (Acknowledgement based methods), η τεχνική Parent Fail-Over, όπου η ρίζα θέτει σε μαύρη λίστα κόμβους που δε στέλνουν μήνυμα για έναν προκαθορισμένο χρόνο, και Heartbeat, όπου χρησιμοποιείται IPSec με ενθυλακωμένο φορτίο ασφαλείας (Encapsulated Security Payload - ESP) για να εμποδίσουν τους επιτιθέμενους κόμβους να διακρίνουν τα πακέτα ICMPv6.

Προτείνονται, επίσης, τρεις παρόμοιες προσεγγίσεις βάση εμπιστοσύνης (trust-based methods). Στην πρώτη, οι κόμβοι υπολογίζουν τιμές εμπιστοσύνης για τους γείτονές τους και τις χρησιμοποιούν για την επιλογή του προτιμώμενου. Στη δεύτερη προσέγγιση, όπως και στην πρώτη, υπολογίζονται οι τιμές εμπιστοσύνης , αλλά αθροίζονται με τιμές φήμης, οι οποίες χρησιμοποιούνται για τον εντοπισμό κακόβουλων κόμβων. Στην τρίτη προσέγγιση, απαιτείται η ύπαρξη ενός συν-επεξεργαστή εμπιστοσύνης πλατφόρμας (Trusted Platform Module – TPM), ο οποίος υπάρχει σε κάθε κόμβο του δικτύου και χειρίζεται την κρυπτογράφηση των πακέτων και υπολογίζει μετρικές για την εύρεση κακόβουλων κόμβων.

Τέλος, ανασκοπούνται IDS βασισμένα σε στατιστικές και μαθηματικές μεθόδους (Statistical/Mathematical Based methods), οι οποίες κατά βάση εντοπίζουν και τα δύο είδη

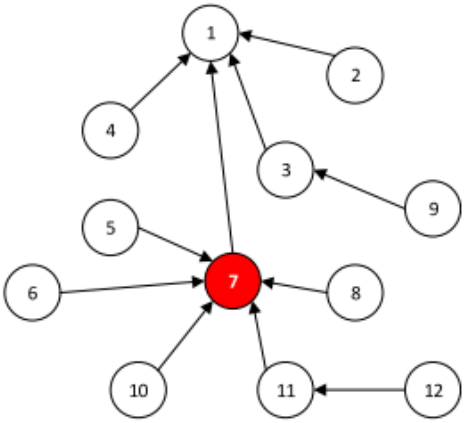
επιθέσεων, και την τεχνική SVELTE που έχει αναλυθεί στο κεφάλαιο 4.4.1.

Β. Επιθέσεις καταβόθρας / Sinkhole Attacks

Οι επιθέσεις καταβόθρας αποτελούν σημαντικό κίνδυνο για την ασφάλεια των δικτυακών συστημάτων, όπου ένας κακόβουλος κόμβος, με τη χρήση μηνυμάτων στο δίκτυο, παρουσιάζεται παραπλανητικά ως η πιο αποδοτική διαδρομή για τα δεδομένα του δικτύου, με στόχο της προσέλκυση της κίνησης των δεδομένων από κοντινούς κόμβους και να καθιερώσει τον επιτιθέμενο ως σημαντικό κόμβο για τη ροή πληροφοριών. Οι επιθέσεις καταβόθρας ενισχύονται, όταν συνδυάζονται με άλλες κακόβουλες δραστηριότητες, όπως επιθέσεις μαύρης τρύπας, σκουληκότρυπας και επιλεκτικής προώθησης [22,23,30].

Η επικοινωνία, που έχει πέσει θύμα υποκλοπής από έναν κακόβουλο κόμβο, διατρέχει τον κίνδυνο τροποποίησης, παραποίησης ή κατάχρησης. Η θεμελιώδης φύση της επίθεσης είναι η ικανότητά της να υπονομεύει τους αλγορίθμους δρομολόγησης δικτύου, καθώς ένας επιτιθέμενος μπορεί να χειραγωγήσει έναν παραβιασμένο κόμβο ώστε να φαίνεται πιο ελκυστικός στους γείτονές του προωθώντας μια καλύτερη διαδρομή, συχνά μέσω παραποίησης ή επανάληψης των ανακοινώσεων διαδρομής.

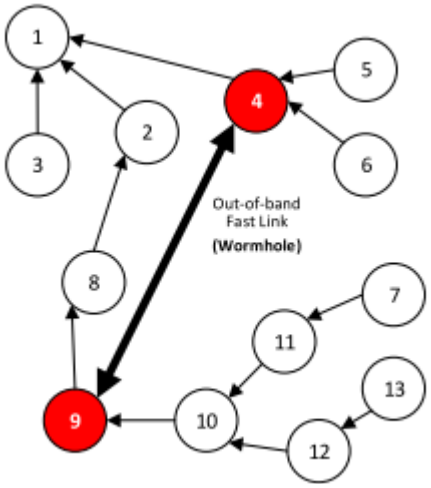
Το άρθρο [22] προτείνει τρόπους αντιμετώπισης για το παρών πρόβλημα. Χρησιμοποιούνται οι ίδιες προσεγγίσεις βάση εμπιστοσύνης , όπως και στις επιθέσεις μαύρης τρύπας/επιλεκτικής προώθησης, η τεχνική SVELTE και ένας στατιστικός/μαθηματικός μηχανισμός, αυτός της επαλήθευσης κατάταξης, όπου χρησιμοποιείται αλυσίδα κατακερματισμού μίας διαδρομής για την σωστή επαλήθευση τοπολογικών κατατάξεων [23].



Εικόνα 4.3: Παράδειγμα επίθεσης καταβόθρας.
Πηγή : Routing Attacks and Mitigation Methods for RPL-Based Internet of Things [22]

Γ. Επιθέσεις σκουληκότρυπας / Wormhole Attacks

Σύμφωνα με τα άρθρα [22,23,30] οι επιθέσεις σκουληκότρυπας αποτελούν έναν τρόπο επίθεσης δρομολόγησης, όπου κακόβουλοι κόμβοι δημιουργούν κρυφές από την τοπολογία διαδρομές που ανακατευθύνουν την κυκλοφορία του δικτύου, παρακάμπτοντας τις συνήθεις διαδρομές που ορίζονται από τα πρωτόκολλα δρομολόγησης του δικτύου. Οι σκουληκότρυπες χρησιμοποιούνται από τους κακόβουλους κόμβους ως οι συντομότερες διαδρομές. Έτσι, εξαπατώνται οι έγκυροι κόμβοι παρέχοντας ψευδείς πληροφορίες σχετικά με την πραγματική τοπολογία και τις αποστάσεις μεταξύ τους. Οι επιθέσεις σκουληκότρυπας διαταράσσουν τον μηχανισμό δρομολόγησης και την τοπολογία ενός δικτύου δημιουργώντας μια εναλλακτική διαδρομή για τη μετάδοση πακέτων που δεν είναι διαθέσιμη στα εξουσιοδοτημένα μέλη του δικτύου.



Εικόνα 4.4: Παράδειγμα επίθεσης σκουληκότρυπας.
Πηγή : Routing Attacks and Mitigation Methods for RPL-Based Internet of Things [22]

Η λογική της τοποθέτησης κακόβουλων κόμβων δημιουργεί την ψευδαίσθηση ότι οι κόμβοι βρίσκονται πιο κοντά από ότι στην πραγματικότητα, αναμεταδίδοντας πακέτα μέσω μιας σκουληκότρυπας. Αυτό μπορεί να οδηγήσει σε επιβλαβείς συνέπειες, όπως η δημιουργία μιας καταβόθρας στο σημείο εξόδου, όπου η κυκλοφορία εκτρέπεται λανθασμένα κατά μήκος του κακόβουλου καναλιού. Οι σκουληκότρυπες έχουν την ικανότητα τροποποίησης των πληροφοριών δρομολόγησης, με αποτέλεσμα να δημιουργούνται συνθήκες αγώνα δρομολόγησης, όπου οι κόμβοι κάνουν επιλογές με βάση ανακριβή ή πρόωρα δεδομένα δρομολόγησης που λαμβάνουν μέσω της σκουληκότρυπας, οδηγώντας σε αλλοιωμένους πίνακες και διαδρομές δρομολόγησης του δικτύου.

Το άρθρο [22] παρέχει και διαχωρίζει τις υπάρχουσες τεχνικές μετριασμού των επιθέσεων σκουληκότρυπας. Αρχικά οι τεχνικές βάση τοποθεσίας (Location based methods) εγκαθιδρύουν τη συσχέτιση μεταξύ κόμβων ή πακέτων και των συγκεκριμένων γεωγραφικών ή λογικών τους θέσεων εντός του δικτύου, χρησιμοποιώντας συστήματα GPS, υπολογισμούς του Χρόνου Γύρου (Round Trip Time - RTT) ή στρώματα Link/PHY. Έπειτα, χρησιμοποιούνται μαθηματικές/στατιστικές μέθοδοι, όπου χρησιμοποιούνται συστημάτων ανίχνευσης εισβολών θεωρίας παιγνίων και πιστοποίησης δέντρων Merkle, τα οποία σχηματίζονται αντίστροφα από τα φύλλα προς τη ρίζα. Τέλος, χρησιμοποιείται και σε αυτήν την περίπτωση η τεχνική SVELTE.

Δ. Επιθέσεις κλωνοποίησης ID και Sybil / Clone ID and Sybil Attacks

Οι συγγραφείς των άρθρων [22,23,30] θέτουν τις επιθέσεις κλωνοποίησης ID και τις επιθέσεις Sybil στην ίδια κατηγορία, λόγω του παρόμοιου τρόπου λειτουργίας τους. Και στις δύο περιπτώσεις επιθέσεων κακόβουλοι κόμβοι προσποιούνται έγκυρους κόμβους, με σκοπό να θέσουν ασταθή την ακεραιότητα και τη λειτουργία του δικτύου.

Στην πρώτη περίπτωση επίθεσης, την κλωνοποίηση ID, ένας κακόβουλος κόμβος υποκλέπτει την ταυτότητα ενός έγκυρου κόμβου, με σκοπό την αλλοίωση της κυκλοφορίας του. Στη δεύτερη περίπτωση επίθεσης, την επίθεση Sybil, ένας κακόβουλος κόμβος υποκλέπτει πολλαπλές ταυτότητες από τους έγκυρους κόμβους του δικτύου, με αποτέλεσμα να του δίνεται η δυνατότητα επηρεασμού μεγάλου τμήματος του δικτύου. Στις επιθέσεις Sybil, δημιουργείται, λόγω των πολλών ταυτοτήτων που υποκλέπτει ένας κακόβουλος κόμβος, ανοχή σε σφάλματα. Έτσι, επηρεάζεται σε μεγάλο βαθμό η σταθερότητα και η ακεραιότητα του δικτύου. Εκμεταλλευόμενοι τις επιθέσεις Sybil, οι αντίπαλοι μπορούν να ισχυριστούν ψευδώς ότι βρίσκονται σε πολλαπλές τοποθεσίες, επηρεάζοντας την αποτελεσματικότητα και την αξιοπιστία των αποφάσεων γεωγραφικής δρομολόγησης.

Στο άρθρο [22] δίνονται τέσσερις διαφορετικές τεχνικές αντιμετώπισης των δύο επικίνδυνων επιθέσεων : (i) τεχνικές βάση εμπιστοσύνης, (ii) τεχνικές βάση τοποθεσίας, (iii) κατανεμημένος πίνακας κατακερματισμού και (iv) τεχνικές βάση στατιστικής/μαθηματικών. Η πρώτη τεχνική αναλύει τις συνδέσεις μεταξύ γειτόνων και τα μοτίβα κινητικότητας των κόμβων. Στη δεύτερη τεχνική χρησιμοποιούνται πληροφορίες για τη γεωγραφική θέση ενός κόμβου πάνω στην τοπολογία του δικτύου. Στην Τρίτη τεχνική υλοποιείται μία συνάρτηση κατακερματισμού για την παρακολούθηση και την ανίχνευση κακόβουλων κόμβων. Στην τελευταία τεχνική δημιουργούνται μοτίβα υπογραφής και εισάγονται στην παρακολούθηση της συμπεριφοράς και την αριθμητική ανάλυση στον αλγόριθμο ανίχνευσης.

Ε. Επιθέσεις πλημμύρας μηνυμάτων HELLO / HELLO Flood Attacks

Οι επιθέσεις πλημμύρας μηνυμάτων HELLO αποτελούν μία από τις πιο εξελιγμένες επιθέσεις στα δίκτυα 6TiSCH. Διαταράσσουν τα πρωτόκολλα χειραψίας στο δίκτυο, ιδιαίτερα το πρωτόκολλο IPv6 σε δίκτυο RPL. Οι επιτιθέμενοι κόμβοι χειραγωγούν τους έγκυρους κόμβους εκμεταλλευόμενοι την εξάρτηση του πρωτοκόλλου από μηνύματα HELLO, ή αλλιώς DIO. Με αυτόν τον τρόπο, προκαλούνται νέες διαδρομές με γείτονες περισσότερο επωφελείς για την επίθεση. Με το που εφαρμοστεί η επίθεση, ο κακόβουλος κόμβος έχει τις επιλογές διακοπής της μετάδοσης ή επιστροφής σε κανονικά επίπεδα ισχύος [22,30]. Αυτή η ενέργεια μπορεί να έχει ως αποτέλεσμα τον τερματισμό γειτονικών γνήσιων κόμβων, διακοπή της επικοινωνίας και ίσως συμφόρηση του δικτύου λόγω αύξησης της επιβάρυνσης των μηνυμάτων ελέγχου.

Η επίθεση πλημμύρας HELLO εκμεταλλεύεται την εγγενή φύση μετάδοσης των πρώτων διαφημίσεων του δικτύου για να προκαλέσει χάος και να βλάψει την αρχιτεκτονική του δικτύου και τη δρομολόγηση. Είναι ζωτικής σημασίας να εντοπιστούν και να αντιμετωπιστούν οι αδυναμίες που αποκαλύπτονται από αυτή την επίθεση προκειμένου να προστατευτεί η αξιοπιστία και η απόδοση των δικτύων που βασίζονται στο RPL και σε άλλα κατανεμημένα συστήματα. Το άρθρο [22] αναφέρει ότι οι υπάρχοντες τρόποι αυτοθεραπείας του RPL είναι αρκετοί για την καταπολέμηση της συγκεκριμένης επίθεσης, αλλά υπογραμμίζει ότι σε περίπτωση συνδυασμού της επίθεσης HELLO με άλλες, τότε ο μετριασμός της γίνεται εξαιρετικά δύσκολος.

4.5 Επιθέσεις στο πρωτόκολλο 6top

Στο παρών κεφάλαιο θα αναπτυχθούν οι δύο επιθέσεις που μπορεί να δεχθεί το πρωτόκολλο 6top , τον διασκορπισμό κυκλοφορίας (traffic dispersion) και τις επιθέσεις υπερφόρτωσης (overloading attacks). Οι επιθέσεις στο πρωτόκολλο 6top αφορούν τις συναλλαγές για τη διαχείριση των πόρων στον πυρήνα της αρχιτεκτονικής 6TiSCH, με αποτέλεσμα να επηρεάζονται αρνητικά οι βασικές λειτουργίες, η αποδοτικότητα του δικτύου και η κατανάλωση ενέργειας από τους κόμβους θύματα [31]. Στη συνέχεια, θα δοθούν τρόποι αντιμετώπισης των επιθέσεων, αν αυτοί υπάρχουν.

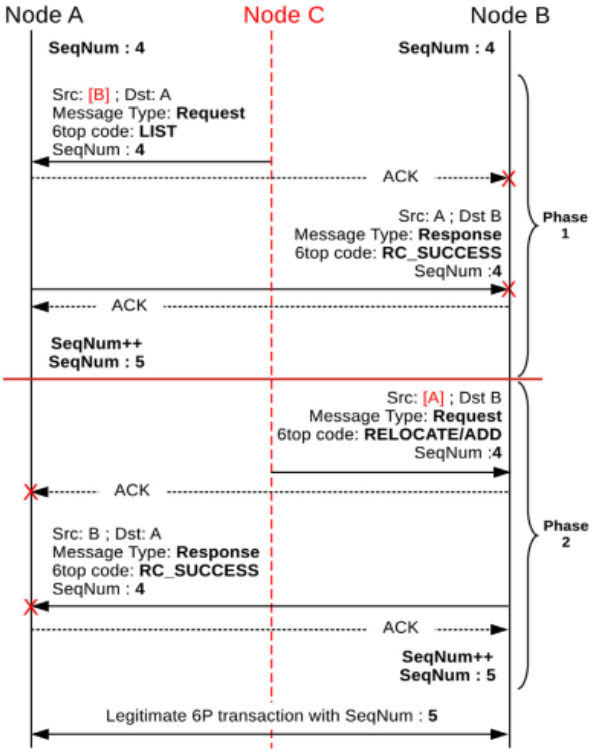
4.5.1 Μοντέλο επιθέσεων

Στα άρθρα [21,31] αναλύεται διεξοδικά το μοντέλο της επίθεσης στο πρωτόκολλο 6top και ο τρόπος που η επίθεση εξαπολύεται στις συναλλαγές διαχείρισης πόρων. Ο εχθρικός κόμβος θεωρείται ως εσωτερική οντότητα στο δίκτυο και έχουν τον έλεγχο ενός ή πολλών κόμβων. Έχοντας αυτή την θέση, μπορεί να επηρεάσει το δίκτυο σε μεγάλο βαθμό, είτε με πρόκληση απώλειας πακέτων, είτε με κατανάλωση ενέργειας. Η ισχύς του επιτιθέμενου πηγάζει από τον έλεγχό που έχει στους κρίσιμους πόρους του δικτύου, ιδίως του συμμετρικού κλειδιού του δικτύου που μοιράζονται όλοι οι κόμβοι [21]. Αυτή η μη εξουσιοδοτημένη πρόσβαση υπονομεύει τη μυστικότητα και την αξιοπιστία των επικοινωνιών του δικτύου.

Οι έγκυροι κόμβοι, που έχουν χειραγωγηθεί από τους κακόβουλους κόμβους, μπορούν να επηρεάσουν την κυκλοφορία στο δίκτυο υποκλέπτοντας, τροποποιώντας και δημιουργώντας μηνύματα. Προκαλείται, δηλαδή, κίνδυνος στην ασφάλεια λειτουργίας του δικτύου. Έχουν, επίσης, την ιδιότητα τα μηνύματα που δημιουργούν να φαίνονται γνήσια και ασφαλή, πράγμα που θέτει ακόμη πιο δύσκολο τον εντοπισμό τους. Επιπλέον, η επάρκεια του αντιπάλου στην παραποίηση των διευθύνσεων MAC προέλευσης αυτών των τροποποιημένων επικοινωνιών εισάγει περαιτέρω επίπεδα περιπλοκότητας στον εντοπισμό και τον μετριασμό αυτών των κινδύνων.

Οι κακόβουλοι κόμβους προσπαθούν να χειραγωγήσουν τις μηνύματα συναλλαγών του πρωτοκόλλου 6top, που επιτρέπουν την ύπαρξη συναλλαγών εντός του δικτύου. Οι επιτιθέμενοι μπορούν να χειραγωγήσουν και να δημιουργήσουν ψευδή μηνύματα για να πάρουν τον έλεγχο της κατάστασης και να πραγματοποιήσουν δόλιες συναλλαγές μεταξύ στοχευμένων κόμβων, προκαλώντας παρατυπίες στον προγραμματισμό. Ως αποτέλεσμα, οι κόμβοι-θύματα λειτουργούν με ανταγωνιστικά χρονοδιαγράμματα, δίνοντας την ψευδή εντύπωση συγχρονισμού, γεγονός που εμποδίζει την ακεραιότητα του χρονοδιαγράμματος και τη συνολική αξιοπιστία του δικτύου [31].

Για την επίθεση σε μία συναλλαγή 6top,όπως φαίνεται και στην εικόνα 4.5, θεωρούμε έναν ενδιάμεσο κακόβουλο κόμβο (C) που στοχεύει σε δύο γειτονικούς (A,B), οι οποίοι έγκυροι και έχουν πρόγραμμα λειτουργίας στο 6TiSCH. Ο κακόβουλος κόμβος παράγει ένα νέο-ψεύτικο χρονοδιάγραμμα για να μεγιστοποιήσει την επίθεση. Ο C παίρνει τη μορφή του A και πραγματοποιεί συναλλαγή 6P με τον B ως A, με σκοπό να μεταφέρει το ψεύτικο χρονοδιάγραμμά του στον κόμβο B. Μετά από τη συναλλαγή αυτή ο κόμβος B θεωρεί ότι μοιράζεται το νέο πρόγραμμα με τον A ενώ αυτό στην πραγματικότητα δεν ισχύει [31]. Η επίθεση αυτή συμβαίνει σε δύο βήματα.



Εικόνα 4.5 : Μοντέλο επίθεσης σε 6P συναλλαγή.
Πηγή: Vulnerabilities of the 6P protocol for the Industrial Internet of Things: Impact analysis and mitigation.[31]

Στο πρώτο βήμα, ο κόμβος C προσποιείται ότι είναι ο κόμβος B για να κάνει μία συναλλαγή 6P LIST με τον κόμβο A. Ο A απαντά με μια επιβεβαίωση επιπέδου σύνδεσης και με το τρέχον πρόγραμμά του, το οποίο υποτίθεται ότι μοιράζεται με τον B. Αφού λάβει μια επιβεβαίωση από τον B, ο A ενημερώνει τον αριθμό ακολουθίας του σε 5, παρόλο που ο B δεν γνωρίζει την αυξημένη τιμή. Ο κόμβος C υποκλέπτει την απάντηση του A, αποκτώντας πρόσβαση στο αρχικό χρονοδιάγραμμα του A, ενώ ο B παραμένει ανυποψίαστος για την πραγματική συναλλαγή. Η συμβατική απάντηση του πρωτοκόλλου του B δεν εμποδίζει την επίθεση, με αποτέλεσμα να υπάρχει διαφορά στους αριθμούς ακολουθίας μεταξύ του A και του B για τις κοινές συναλλαγές τους. Ο A προχωρά με βάση τη λανθασμένη πεποίθηση μιας ολοκληρωμένης συναλλαγής με τον B [21,31].

Στο δεύτερο βήμα, κόμβος C δημιουργεί ένα νέο χρονοδιάγραμμα, το S', για να πραγματοποιήσει μια κακόβουλη συναλλαγή 6P με τον κόμβο B. Παίρνει τη μορφή του κόμβου A, χρησιμοποιώντας την προηγούμενη τιμή του αριθμού ακολουθίας (SeqNum) 4. Σε αυτό το σημείο της κακόβουλης συναλλαγής δημιουργούνται οι προϋποθέσεις για επιθέσεις όπως ο διασκορπισμός κυκλοφορίας και η υπερφόρτωση. Ο κόμβος B αποδέχεται το παραπλανητικό αίτημα, δημιουργεί μια απάντηση και αλλάζει την τιμή του SeqNum σε 5, συγχρονιζόμενος με τον SeqNum του A. Ο κόμβος A δεν γνωρίζει τις ψευδείς ανταλλαγές και αγνοεί την επιβεβαίωση και την απάντηση. Στο τέλος της δεύτερης φάσης, οι κόμβοι A και B συγχρονίζονται με SeqNum 5, αποτρέποντας ανωμαλίες σε μελλοντικές συναλλαγές. Ωστόσο, αυτός ο συγχρονισμός καλύπτει μια βαθύτερη διαφωνία, εμποδίζοντας την άμεση επικοινωνία και θέτοντας σε κίνδυνο την αποτελεσματικότητα της αρχιτεκτονικής του δικτύου [21.31].

4.5.2 Διασκορπισμός Κυκλοφορίας / Traffic Dispersion

Σύμφωνα με τους συγγραφείς των άρθρων [21,31] η επίθεση διασκορπισμού κυκλοφορίας υπονομεύει την επικοινωνία μεταξύ δύο γειτονικών κόμβων, A και B, σε ένα δίκτυο 6TiSCH, διακόπτοντας τη ροή μηνυμάτων σύμφωνα με το αμοιβαία συμφωνημένο χρονοδιάγραμμα. Στο πλαίσιο του DODAG του RPL, ο κόμβος A θεωρεί τον κόμβο B ως τον προτιμώμενο γονέα του. Η επίθεση εκμεταλλεύεται τη σκόπιμη αλλαγή αυτού του χρονοδιαγράμματος για να παρεμποδίσει την κρίσιμη διαδικασία μετάδοσης δεδομένων που είναι απαραίτητη για τη λειτουργία του δικτύου.

Αυτή η επίθεση πραγματοποιείται σε δύο στάδια, όπως έχει αναφερθεί στο μοντέλο της επίθεσης στο κεφάλαιο 4.5.1. Αρχικά, ο επιτιθέμενος, ο οποίος έχει αναλάβει τον έλεγχο ενός εκτεθειμένου κόμβου C, εκτελεί μια χειραγωγημένη συναλλαγή 6P LIST για να αποκτήσει το αρχικό χρονοδιάγραμμα επικοινωνίας, S μεταξύ των A και B. Στη συνέχεια, ο αντίπαλος προσποιείται εκ νέου ότι είναι ο κόμβος A προκειμένου να πείσει τον B να δεχθεί ένα τροποποιημένο χρονοδιάγραμμα, S', χρησιμοποιώντας μια χειραγωγημένη συναλλαγή 6P, είτε DELETE είτε RELOCATE. Ο πυρήνας αυτής της χειραγώγησης είναι η ικανότητα του αντιπάλου να μεταφέρει τις λειτουργίες του κόμβου B από το αρχικό χρονοδιάγραμμα S στο νέο επιβληθέν χρονοδιάγραμμα S', αποκόπτοντας έτσι τη σύνδεση επικοινωνίας με τον κόμβο A.

Η επίθεση επικεντρώνεται κυρίως στην κατανομή των κελιών εντός του κοινού χρονοδιαγράμματος μεταξύ των κόμβων A και B. Στην παραλλαγή DELETE, ο κόμβος B εξαπατάται ώστε να εξαλείψει το κοινό κελί με τον A, με αποτέλεσμα να δημιουργείται μια κατάσταση όπου ο κόμβος B εκτελεί ένα άδειο χρονοδιάγραμμα S', ενώ ο A παραμένει στο αμετάβλητο χρονοδιάγραμμα S. Αντίθετα, η παραλλαγή RELOCATE συνεπάγεται ότι ο B πείθεται να αντικαταστήσει το κοινό κελί με τον A με ένα νέο κελί c2. Η προσδοκία του B για μηνύματα από τον A στο νέο αυτό κελί, το οποίο δεν ακολουθεί το αρχικό χρονοδιάγραμμα S, υποχρεώνει στη διακοπή της επικοινωνίας.

Ο κακόβουλος στόχος της επίθεσης είναι η διαταραχή του καναλιού επικοινωνίας μεταξύ των A και B, εμποδίζοντας τη ροή πληροφοριών προς τον κόμβο-ρίζα και, κατά συνέπεια, θέτοντας σε κίνδυνο τη διαθεσιμότητα και την ακεραιότητα του δικτύου. Αυτή η εσκεμμένη παρεμβολή όχι μόνο διαχωρίζει τους στοχευμένους κόμβους, αλλά αποτελεί επίσης σημαντικό κίνδυνο για τη γενική αξιοπιστία του δικτύου, υπογραμμίζοντας την κρίσιμη απαίτηση για ισχυρούς μηχανισμούς ασφαλείας εντός της αρχιτεκτονικής 6TiSCH για τη μείωση αυτών των αδυναμιών Στο άρθρο [31] δίνεται στη συνέχεια αναλυτικά το αντίκτυπο της επίθεσης στο δίκτυο με μετρήσεις, πράγμα το οποίο δεν ασχολείται η παρούσα εργασία.

4.5.3 Επιθέσεις υπερφόρτωσης / Overloading Attacks

Σύμφωνα με τα [21,31] η επίθεση υπερφόρτωσης στοχεύει στην υπονόμευση της ενεργειακής απόδοσης ενός κόμβου B σε ένα δίκτυο 6TiSCH, αναγκάζοντάς τον να αναθέσει περισσότερα κελία για λήψη (RX), με αποτέλεσμα την υπερβολική χρήση ενέργειας. Βασίζεται στη δομή του DODAG, όπου ο κόμβος A ορίζεται ως ο προτιμώμενος γονέας του κόμβου B. Ο επιτιθέμενος χειραγωγεί το κοινόχρηστο χρονοδιάγραμμα μεταξύ των κόμβων A και B, εξαπατώντας τον B να προσθέσει περισσότερα κελιά RX ισχυριζόμενος ψευδώς ότι αυτό θα βελτιώσει την επικοινωνία. Αυτή η χειραγώγηση διευκολύνεται από μια παραπλανητική συναλλαγή 6P ADD κατά τη δεύτερη φάση επίθεσης.

Πριν εξαπολυθεί η επίθεση, οι κόμβοι A και B ακολουθούσαν ένα κοινόχρηστο χρονοδιάγραμμα που ονομάζεται S, το οποίο περιλαμβάνει ένα κοινό κελί c1. Ο B εφάρμοσε ένα τροποποιημένο χρονοδιάγραμμα, το S', το οποίο περιλαμβάνει ένα επιπλέον κελί, το c2, υποθέτοντας ότι ο A συναίνεσε σε αυτό για μελλοντική επικοινωνία. Ωστόσο, ο A επιμένει να ακολουθεί το αρχικό χρονοδιάγραμμα, αγνοώντας τις τροποποιήσεις του B.

Η επίθεση στον κόμβο B οδηγεί στη σπατάλη ενός δυνητικά πολύτιμου κελιού, υποδεικνύοντας κακή κατανομή των πόρων δικτύωσης, και σε συστηματική αύξηση της χρήσης ενέργειας του B,

καθώς παρακολουθεί ενεργά το κελί c2 για εισερχόμενα σήματα από τον A που δεν θα ληφθούν ποτέ. Αυτό μειώνει την ενεργειακή απόδοση του B και αποδυναμώνει τη συνολική διάρκεια λειτουργίας και την αξιοπιστία του κόμβου στο δίκτυο. Στο άρθρο [31] δίνεται στη συνέχεια αναλυτικά το αντίκτυπο της επίθεσης στο δίκτυο με μετρήσεις, πράγμα το οποίο δεν ασχολείται η παρούσα εργασία.

4.5.4 Τρόποι αντιμετώπισης/μετριασμού των επιθέσεων

Σύμφωνα με τα αποτελέσματα της έρευνας [31], οι επιθέσεις διασκορπισμού κυκλοφορίας δεν γίνονται αντιληπτές από το ζευγάρι των κόμβων που δέχεται την επίθεση. Αυτό συμβαίνει, διότι ο κόμβος που έχει υποκλαπεί δεν παρουσιάζει κάποια παράνομη συμπεριφορά στο δίκτυο με αποτέλεσμα ο κόμβος θύμα να μην έχει κάποιο τρόπο αντίληψης της παρατυπίας. Ο παραβιασμένος κόμβος αφαιρεί ή μετακινεί RX κελιά που ο κόμβος-θύμα έχει προγραμματίσει με τον προτιμώμενο γονέα του και στη συνέχεια ενσωματώνει τα αφαιρεθέντα κελιά στο δικό του χρονοδιάγραμμα για να αναγνωρίσει τα πακέτα δεδομένων που μεταδίδονται από τον κόμβο-θύμα. Κανένας από τους κόμβους του ζεύγους θυμάτων δεν προκαλεί υποψίες.

Στο δεύτερο είδος επίθεσης ,όμως, το ζεύγος θύμα μπορεί να ελέγξει μέσω μίας διαδικασίας τοπικής παρακολούθησης, εάν υπάρχει κάποια παρατυπία. Αυτό μπορεί να συμπεριληφθεί στην υπάρχουσα συνάρτηση χρονοπρογραμματισμού σε κάθε κόμβο του δικτύου. Η συνάρτηση χρονοπρογραμματισμού έχει τη δυνατότητα να ανιχνεύει αν τα νέα κελιά RX χρησιμοποιούνται ενεργά για τη λήψη πακέτων δεδομένων. Η απουσία πακέτων δεδομένων σε μια συγκεκριμένη κυψέλη για ένα συγκεκριμένο χρονικό διάστημα μπορεί να θεωρηθεί ως ένδειξη μιας ανωμαλίας χρονοπρογραμματισμού που οδηγεί σε αναποτελεσματικότητα.

Για την εκτέλεση αυτού το τρόπου αντιμετώπισης, το άρθρο [31] προτείνει την τροποποίηση της συνάρτηση χρονοπρογραμματισμού με την ενσωμάτωση μιας επιπλέον διαδικασίας επαλήθευσης για τη χρήση των κυψελών RX. Κάθε κόμβος παρακολουθεί τακτικά τη χρήση των κυψελών RX που του έχουν ανατεθεί, παρακολουθώντας τον αριθμό των πακέτων δεδομένων που ελήφθησαν για κάθε κυψέλη κατά την προηγούμενη περίοδο παρακολούθησης. Εάν η χρήση μιας κυψέλης RX πέσει κάτω από ένα ορισμένο όριο, ο κόμβος αφαιρεί τη συγκεκριμένη κυψέλη από το πρόγραμμά του.

Η επιλογή της σωστής διάρκειας για την περίοδο παρακολούθησης περιλαμβάνει την εξισορρόπηση του κινδύνου της αφαίρεσης των κυττάρων που εξακολουθούν να χρησιμοποιούνται με την περιττή κατανάλωση ενέργειας που συμβαίνει μέχρι την τελική αφαίρεση των άχρηστων κυττάρων RX από το τρέχον πρόγραμμα. Η συναλλαγή 6P DELETE δεν αποτελεί αξιόπιστη μέθοδο για την αφαίρεση μη αναγκαίων κυττάρων RX, καθώς η συναλλαγή θα τερματιστεί με σφάλμα.

Συμπεράσματα

Εν κατακλείδι, Το άρθρο διερευνά τις ανησυχίες για την ασφάλεια στα δίκτυα 6TiSCH, τα οποία χρησιμοποιούν τα πλαίσια IEEE 802.15.4, TSCH, RPL και 6P. Αυτά τα πρωτόκολλα είναι απαραίτητα για την εποπτεία της επικοινωνίας σε δίκτυα χαμηλής ισχύος και με απώλειες, όπως τα πλαίσια IoT. Ωστόσο, παρέχουν επίσης πιθανούς κινδύνους ασφάλειας. Προκειμένου να αντιμετωπιστούν αυτά τα ζητήματα, είναι απαραίτητο να υιοθετηθεί μια ολοκληρωμένη προσέγγιση που περιλαμβάνει ασφαλή σχεδιασμό πρωτοκόλλων, ανθεκτικά μέτρα διαχείρισης δικτύου και συνεχή επιτήρηση για μη φυσιολογικές δραστηριότητες. Είναι επιτακτική ανάγκη για το μέλλον των δικτύων 6TiSCH, τα οποία είναι ζωτικής σημασίας για κρίσιμες εφαρμογές IoT, να διαθέτουν προσαρμοστικά μέτρα ασφαλείας που να μπορούν να αντιδρούν στις αυξανόμενες απειλές.

Συντμήσεις/Αρκτικόλεξα

IoT	Internet of Things
WG	Working Group
IPv6	Internet Protocol version 6
TSCH	Time Slotted/Scheduled Channel Hopping
MTSCH	Mobile Timeslotted Channel Hopping
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
6TiSCH	Ipv6 over 6TiSCH
6LoWPAN	Ipv6 over Low Power Wireless Personal Area Networks
PAN	Personal Area Network
RPL	Routing Protocol for Low Power and Lossy Networks
CoAP	Constrained Application Protocol
MAC	Medium Access Control
WSN	Wireless Sensor Network
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CFP	Contention Free Period
CAP	Contention Access Period
GTS	Guaranteed Time Slots
TDMA	Time Division Multiple Access
DSME	Deterministic Synchronous Multichannel Extension
EB	Enhanced Beacon
FastA	Fast Association
LLDN	Low Latency Deterministic Network
LLN	Low power and Lossy Networks
AMCA	Asynchronous multi channel adaptation
BLINK	Radio Frequency Identification Blink
FCF	Frame Control Field
ASN	Absolute Slot Number
CCA	Clear Channel Assessment
RVF	Random Vertical Filling
RHF	Random Horizontal Filling
DTMC	Discrete Time Markov Chain
MBS	Model based beacon scheduling
JP	Join Proxy
SF	Scheduling Function

IE	Information Element
MSF	Minimal Scheduling Function
TX	Transmit
RX	Receive
SAX	Symbolic Aggregate ApproXimation
CRC	Cyclic Redundancy Check
PDR	Packet Delivery Ratio
BRR	Backbone Router
PCE	Path Communication Entity
DODAG	Destination Oriented Directed Acyclic Graph
DIS	DODAG Information Solicitation
DIO	DODAG Information Object
DAO	Destination Advertisement Object
DAO-ACK	Destination Advertisement Object Acknowledgement
ETX	Expected Transmission Count
CoJP	Constrained Join Protocol
JRC	Join Registrar/Coordinator
PSK	Pre-Shared Key
VeRA	Version Number and Rank Attack Authentication
TRAIL	Trust Anchor Interconnection Loop
6BR	6LowPAN Border Router
DLTS	Deep Level Transient Spectroscopy
IDS	Intrusion Detection System
DTM	Dynamic threshold Mechanism
ESP	Encapsulated Security Payload
TPM	Trusted Platform Module
RTT	Round Trip Time

Βιβλιογραφία

[1] K. Ashton, “That ”internet of things thing,” RFiD Journal, vol. 22, pp. 97–114, 2009.

[2] D. Dujovne, T. Watteyne, X. Vilajosana and P. Thubert, "6TiSCH: deterministic IP-enabled industrial internet (of things)," in IEEE Communications Magazine, vol. 52, no. 12, pp. 36-41, December 2014, doi: 10.1109/MCOM.2014.6979984.

[3] D. De Guglielmo, S. Brienza, G. Anastasi,IEEE 802.15.4e: A survey,Computer Communications,Volume 88,2016,Pages 1-24,ISSN 0140-3664,https://doi.org/10.1016/j.comcom.2016.05.004.(https://www.sciencedirect.com/science/article/pii/S0140366416301980)

[4] J. T. Adams, "An introduction to IEEE STD 802.15.4," 2006 IEEE Aerospace Conference, Big Sky, MT, USA, 2006, pp. 8 pp.-, doi: 10.1109/AERO.2006.1655947.

[5] H. Kurunathan, R. Severino, A. Koubaa and E. Tovar, "IEEE 802.15.4e in a Nutshell: Survey and Performance Evaluation," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1989-2010, thirdquarter 2018, doi: 10.1109/COMST.2018.2800898.

[6] F. Chen, R. German and F. Dressler, "Towards IEEE 802.15.4e: A study of performance aspects," 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, 2010, pp. 68-73, doi: 10.1109/PERCOMW.2010.54706050.

[7] Gaglio, Salvatore, and G. Lo Re. Advances onto the Internet of Things. Vol. 349. Springer, 2014. Pages : 135-153

[8] Awati, Rahul. “What Is Time Division Multiple Access (TDMA)?” Networking, TechTarget, 7 June 2021,www.techtarget.com/searchnetworking/definition/TDMA. Accessed 08 Jan. 2024.

[9] P. Thubert, T. Watteyne, M. R. Palattella, X. Vilajosana and Q. Wang, "IETF 6TSCH: Combining IPv6 Connectivity with Industrial Performance," 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Taichung, Taiwan, 2013, pp. 541-546, doi: 10.1109/IMIS.2013.96.

[10] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy and P. Thubert, "IETF 6TiSCH: A Tutorial," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 595-615, Firstquarter 2020, doi: 10.1109/COMST.2019.2939407.

[11] J. Y. Ha, T. H. Kim, H. S. Park, S. Choi and W. H. Kwon, "An Enhanced CSMA-CA Algorithm for IEEE 802.15.4 LR-WPANs," in IEEE Communications Letters, vol. 11, no. 5, pp. 461-463, May 2007, doi: 10.1109/LCOMM.2007.061891.

[12] Buratti, Chiara & Verdone, R.. (2009). Performance Analysis of IEEE 802.15.4 Non Beacon-Enabled Mode. Vehicular Technology, IEEE Transactions on. 58. 3480 - 3493. 10.1109/TVT.2009.2014956.

[13] D. De Guglielmo, A. Seghetti, G. Anastasi and M. Conti, "A performance analysis of the network formation process in IEEE 802.15.4e TSCH wireless sensor/actuator networks," 2014 IEEE Symposium on Computers and Communications (ISCC), Funchal, Portugal, 2014, pp. 1-6, doi: 10.1109/ISCC.2014.6912607.

[14] E. Vogli, G. Ribezzo, L. A. Grieco and G. Boggia, "Fast join and synchronization schema in the IEEE 802.15.4e MAC," 2015 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), New Orleans, LA, USA, 2015, pp. 85-90, doi: 10.1109/WCNCW.2015.7122534.

[15] D. De Guglielmo, S. Brienza and G. Anastasi, "A Model-based Beacon Scheduling algorithm for IEEE 802.15.4e TSCH networks," 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Coimbra, Portugal, 2016, pp. 1-9, doi: 10.1109/WoWMoM.2016.7523517.

[16] Y. Al-Nidawi and A. H. Kemp, "Mobility Aware Framework for Timeslotted Channel Hopping IEEE 802.15.4e Sensor Networks," in IEEE Sensors Journal, vol. 15, no. 12, pp. 7112-7125, Dec. 2015, doi: 10.1109/JSEN.2015.2472276.

[17] X. Vilajosana, K. Pister, T. Watteyne, T.Vilajosana, Xavier, et al. “RFC 8180: Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration.” IETF Datatracker, datatracker.ietf.org/doc/html/rfc8180.

[18] Wang, Q., Vilajosana, X. and Watteyne, T.Wang, Q., et al. “6TiSCH Operation Sublayer (6top) Protocol (6P).” RFC Editor, 1 Nov. 1970, www.rfc-editor.org/rfc/rfc8480.html.

[19] Chang, T., Vučinić, M., Vilajosana, X., Duquennoy, S. and Dujovne, D. R.Chang, Tengfei, et al. “RFC 9033: 6TiSCH Minimal Scheduling Function (MSF).” IETF Datatracker, datatracker.ietf.org/doc/rfc9033/.

[20] A. Kalita, A. Brighente, M. Khatua and M. Conti, "Effect of DIS Attack on 6TiSCH Network Formation," in IEEE Communications Letters, vol. 26, no. 5, pp. 1190-1193, May 2022, doi: 10.1109/LCOMM.2022.3155992

[21] TY - CONF TI - Evaluation of Feasibility and Impact of Attacks Against the 6top Protocol in 6TiSCH Networks T2 - 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM) SP - 68 EP - 77 AU - G. Carignani AU - F. Righetti AU - C. Vallati AU - M. Tiloca AU - G. Anastasi PY - 2020 DO - 10.1109/WoWMoM49955.2020.00027 JO - 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM) IS - SN - VO - VL - JA - 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM) Y1 - 31 Aug.-3 Sept. 2020 ER -

[22] A. Raoof, A. Matrawy and C. -H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1582-1606, Secondquarter 2019, doi: 10.1109/COMST.2018.2885894.

[23] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 2015, pp. 1-6, doi: 10.1109/PERVASIVE.2015.7087034.

[24] Koosha, Mohammad, Behnam Farzaneh, and Shahin Farzaneh. "A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things." 2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT). IEEE, 2022.

[25] Le, Anhtuan, et al. "The impact of rank attack on network topology of routing protocol for low-power and lossy networks." IEEE Sensors Journal 13.10 (2013): 3685-3692.

[26] Perrey, Heiner, et al. "TRAIL: Topology authentication in RPL." arXiv preprint

arXiv:1312.0984 (2013).

[27] Dvir, Amit, and Levente Buttyan. "VeRA-version number and rank authentication in RPL." 2011 IEEE eighth international conference on mobile ad-hoc and sensor systems. IEEE, 2011.

[28] C. Pu, “Mitigating DAO inconsistency attack in RPL-based low power and lossy networks,” in Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC), Jan. 2018, pp. 570–574.

[29] Perazzo, Pericle, et al. "DIO suppression attack against routing in the Internet of Things." IEEE Communications Letters 21.11 (2017): 2524-2527.

[30] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1.2-3 (2003): 293-315.

[31] Righetti, Francesca, et al. "Vulnerabilities of the 6P protocol for the Industrial Internet of Things: Impact analysis and mitigation." Computer Communications 194 (2022): 411-432.