Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Πρωτόκολλα Δικτύου Ανθεκτικά σε Καταστροφές

Ηλίας Μιχαλακέας

Επιβλέπων Καθηγητής
Δρ. Αρτέμιος Γ. Βογιατζής

Δεκέμβριος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Πρωτόκολλα Δικτύου Ανθεκτικά σε Καταστροφές

Ηλίας Μιχαλακέας

Επιβλέπων Καθηγητής
Δρ. Αρτέμιος Γ. Βογιατζής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2018

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι η μελέτη της απόδοσης δικτυακών πρωτοκόλλων ανθεκτικών σε καταστροφές, από επιθέσεις που θίγουν τις απαιτήσεις της ασφάλειας και ειδικότερα την διαθεσιμότητα (availability).

Αρχικά, οριοθετείται το πρόβλημα της διαθεσιμότητας ως μία από τις τρεις βασικές απαιτήσεις ασφάλειας δικτύου. Προτείνεται η χρήση τεχνικών κωδικοποίησης δικτύου (network coding) για τη βελτίωση της διαθεσιμότητας, σε θεωρητικό και πειραματικό πλαίσιο.

Μελετώνται τα διάφορα είδη κωδικοποίησης δικτύου και επιλέγεται η Τυχαία Γραμμική Κωδικοποίηση Δικτύου (Random Linear Network Coding, RLNC), με βάση τα χαρακτηριστικά της, όπως η αξιοπιστία, η ευρωστία και η αύξηση της ρυθμαπόδοσης.

Αναπτύσσονται στη συνέχεια σενάρια επιθέσεων στη διαθεσιμότητα των δικτύων και αναλύεται ο τρόπος που μπορεί να αξιοποιηθεί το RLNC για την αντιμετώπισή τους. Για την επαλήθευση των παραπάνω, γίνεται πειραματική μελέτη και αξιολογούνται υλοποιήσεις του RLNC.

Τα αποτελέσματα της θεωρητικής και πειραματικής μελέτης αναδεικνύουν τις δυνατότητες του RLNC σε σενάρια χρήσης σε εντόνως εχθρικά περιβάλλοντα, και ιδιαίτερα τα οφέλη της επανα-κωδικοποίησης (re-coding) από ενδιάμεσους κόμβους, για τη μαζική αποστολή πακέτων σε μεγάλο πλήθος αποδεκτών, την αποστολή πακέτων με παράλληλη αναμετάδοση από πολλά ταυτόχρονα μονοπάτια και την αποστολή πακέτων με τη χρήση πολλών ενδιάμεσων αναμεταδοτών στη σειρά.

Summary

The goal of this dissertation is to study the performance of disaster resilient network protocols, during attacks against security requirements, and particularly the availability.

Initially, the problem of availability is defined as one of the three basic network security requirements. The use of network coding techniques is proposed in order to improve availability in a theoretical and experimental context.

The dissertation studies the various types of network coding and Random Linear Network Coding (RLNC) is selected based on its features, such as reliability, robustness and throughput enhancement.

Further, various attack scenarios on network availability are developed and the ways the use of RLNC can address them is analysed. In this respect, an experimental study and evaluations of RLNC implementations are performed so as to verify the above.

The results of the theoretical and experimental studies highlight RLNC's capabilities in scenarios in highly hostile environments, and particularly the benefits of re-coding by intermediate nodes, in cases of mass packet delivery to a large number of recipients, sending packets using parallel nodes over multiple paths simultaneously, as well as packet delivery using multiple intermediate nodes.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κο Αρτέμιο Γ. Βογιατζή για την πολύτιμη βοήθεια και καθοδήγηση για την εκπόνηση της μεταπτυχιακής διατριβής. Θα ήθελα, επίσης, να ευχαριστήσω την οικογένεια μου και ιδιαίτερα τη σύζυγο μου για την υπομονή που έδειξαν και την υποστήριξη που παρείχαν όλο αυτό το χρονικό διάστημα. Τέλος θα ήθελα να την αφιερώσω στις κόρες μου, Μαρία και Αγγελίνα, για να θυμούνται τη φωνή πίσω από την κλειστή πόρτα «ο μπαμπάς διαβάζει …».

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Τα δίκτυα επικοινωνίας αποτελούν μέρος της κρίσιμης υποδομής σε τοπικό, εθνικό και διεθνές επίπεδο. Παρουσιάζονται ιδιαίτερα ευάλωτα σε διαταραχές (disruptions) και καταστροφές (disasters), οι οποίες προκύπτουν από φυσικά (παράδειγμα: σεισμοί, καταιγίδες, τσουνάμι, εκρήξεις ηφαιστείων) ή ανθρωπογενή αίτια (παράδειγμα: κυβερνοπόλεμος, καταπιεστικά καθεστώτα, cracking, ανθρώπινα σφάλματα) και επιδρούν άμεσα ή έμμεσα (παράδειγμα: κατάρρευση ηλεκτρικού δικτύου) στη λειτουργία της δικτυακής υποδομής. Τα ανθεκτικά-σε-καταστροφές πρωτόκολλα δικτύου (disaster-resilient network protocols) είναι μια καινοτόμα προσέγγιση στη λειτουργία πρωτοκόλλων δικτύου, η οποία μπορεί να έχει πολλαπλές εφαρμογές για την ασφάλεια των δικτύων, ως προς τη διαθεσιμότητα, την ακεραιότητα, την εμπιστευτικότητα και την ιδιωτικότητα σε πολλαπλά σενάρια χρήσης.

Η παρούσα μεταπτυχιακή διατριβή αφορά στη μελέτη δικτυακών πρωτοκόλλων ανθεκτικών σε καταστροφές (disaster-resilient network protocols) και τη βελτίωση των χαρακτηριστικών ασφάλειας που μπορούν να προσφέρουν αξιοποιώντας τεχνικές network coding και παραλλαγών αυτών.

1.1. Βασικά Ερευνητικά Ερωτήματα

Το ερευνητικό ερώτημα που μελετάται στην παρούσα μεταπτυχιακή διατριβή είναι η βελτίωση της ασφάλειας των δικτύων και ειδικότερα της απαίτησης διαθεσιμότητας. Ειδικότερα, τίθεται το ερώτημα αν και πώς μπορούν να αξιοποιηθούν σε επίπεδο δικτύου πολλαπλά μονοπάτια δρομολόγησης, τα οποία είναι *ταυτόχρονα* διαθέσιμα, ώστε να βελτιωθεί η ανθεκτικότητά του σε σενάρια φυσικών καταστροφών (τυχαίες ενέργειες) αλλά και κακόβουλων ανθρώπινων επεμβάσεων (στοχευμένες ενέργειες). Προς αυτή την κατεύθυνση, τίθεται προς διερεύνηση η τεχνική network coding.

1.2. Αναγκαιότητα και Σπουδαιότητα Έρευνας

Τα δίκτυα επικοινωνιών αποτελούν πλέον δομικό στοιχείο της σύγχρονης κοινωνίας της πληροφορίας και όσο εξελίσσονται σε πολυπλοκότητα, εύρος, χωρητικότητα, προκύπτουν νέες προκλήσεις στην προσπάθεια προστασίας τους από φυσικές καταστροφές και κακόβουλες ανθρώπινες ενέργειες. Τα αποτελέσματα τέτοιων γεγονότων είναι η υποβάθμιση της επικοινωνίας, η διακοπή της επικοινωνίας ή η υποκλοπή της και είναι αναγκαίο να αναπτυχθούν στρατηγικές αντιμετώπισης τους. Σχετικά θέματα μελετώνται την τρέχουσα περίοδο στο ευρωπαϊκό δίκτυο ερευνητών COST Action RECODIS (Resilient communication services protecting end-user applications from disaster-based failures) με τη συμμετοχή της Κύπρου, της Ελλάδας και πολλών άλλων χωρών.

1.3. Δομή της Διατριβής

Τα επόμενα κεφάλαια δομούνται ως εξής. Το κεφάλαιο 2 αφορά στη βιβλιογραφική ανασκόπηση (literature review) και περιγραφή της στάθμης της τεχνικής (state-of-the-art) αφενός μεν σε θέματα ασφάλειας δικτύων, με έμφαση στις απαιτήσεις διαθεσιμότητας (availability), αφετέρου δε στην έννοια και τις εφαρμογές της Κωδικοποίησης Δικτύου[1] (network coding). Το κεφάλαιο 3 διατυπώνει το ερευνητικό ερώτημα για την αντιμετώπιση θεμάτων διαθεσιμότητας, ως απαίτηση ασφάλειας του δικτύου. Παρέχει επίσης μία θεωρητική αποτίμηση της καταλληλότητας του network coding. Το κεφάλαιο 4 αφορά σε μία αξιολόγηση των διαθέσιμων υλοποιήσεων τεχνικών network coding καθώς και πειραματικής μελέτης επιλεγμένων σεναρίων λειτουργίας δικτύων μέσω προσομοίωσης για την αποτίμηση της διαθεσιμότητας. Το κεφάλαιο 5 παρουσιάζει και αναλύει τα αποτελέσματα και ευρήματα της πειραματικής μελέτης. Το κεφάλαιο 6, τέλος, περιγράφει τα συμπεράσματα της μελέτης μας και

[1] Επισημαίνεται ότι η ορθή απόδοση του όρου coding στην ελληνική γλώσσα είναι «κωδιίκευση», ωστόσο για λόγους συμβατότητας με την υπάρχουσα ακαδημαϊκή βιβλιογραφία, διατηρήθηκε στο παρόν κείμενο η απόδοση «κωδικοποίηση» καίτοι αφορά στον όρο «codification» (πβ. http://www.eleto.gr/download/TermsOnFora/TermsOnFora.pdf). Κατά συνέπεια «κωδικοποίηση δικτύου» αντί του «δικτυακή κωδίκευση».

οριοθετεί μελλοντικές κατευθύνσεις εργασίας στο αντικείμενο της μεταπτυχιακής διατριβής.

Κεφάλαιο 2
Βιβλιογραφική Ανασκόπηση

2.1. Ασφάλεια Δικτύων

Στις μέρες μας τα δίκτυα επικοινωνιών χρησιμοποιούνται σε όλους τους τομείς της ζωής, όπως πολιτικούς, οικονομικούς, επαγγελματικούς, ακόμα και στρατιωτικούς. Η ασφάλεια δικτύων έχει αναχθεί σε μείζον θέμα που σχετίζεται άμεσα με την εθνική στρατηγική, την εθνική οικονομία, την εύρυθμη λειτουργία εταιρειών ή οργανισμών, αλλά και τις προσωπικές ζωές των ανθρώπων. Αν δεν μπορεί να εξασφαλιστεί, τότε οι αρνητικές συνέπειες, οικονομικές, κοινωνικές, πολιτικές και περιβαλλοντικές θα είναι μεγάλες σε όλη την ανθρωπότητα. Η ασφάλεια θεωρείται, δηλαδή, πλέον βασική προϋπόθεση για τη λειτουργία ενός δικτύου.

Το NSIT Computer Security handbook ορίζει τον όρο ασφάλεια πληροφοριακών συστημάτων ως (Stallings, 2011, p. 9):

«*Η προστασία που παρέχεται σε ένα αυτοματοποιημένο πληροφοριακό σύστημα με στόχο την τήρηση της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των πόρων του πληροφοριακού συστήματος (συμπεριλαμβανομένων του υλικού, λογισμικού, πληροφορίας/δεδομένων και τηλεπικοινωνιών).*»

Αυτός ο ορισμός εισαγάγει τρεις βασικές απαιτήσεις που βρίσκονται στην καρδιά της ασφάλειας πληροφοριακών συστημάτων:

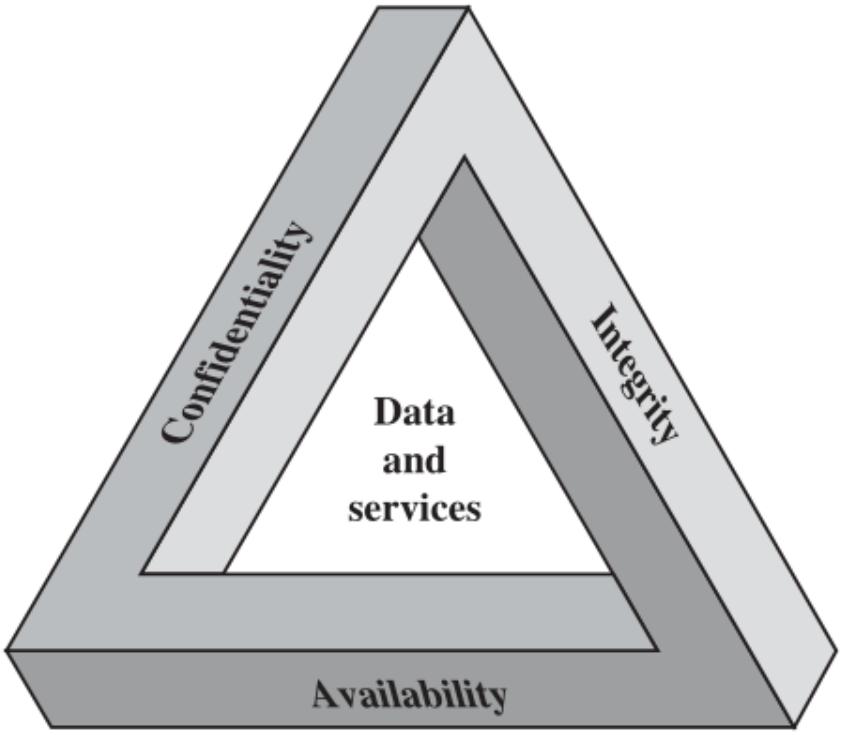
- **Εμπιστευτικότητα** (Confidentiality): ο όρος αυτός αφορά σε δύο έννοιες:
    - **Εμπιστευτικότητα δεδομένων** (Data confidentiality): εξασφαλίζει ότι η προσωπική ή εμπιστευτική πληροφορία δεν αποκαλύπτεται σε μη εξουσιοδοτημένα άτομα.

- **Ιδιωτικότητα** (Privacy): εξασφαλίζει ότι το άτομο ελέγχει ή επηρεάζει το τί πληροφορίες σχετικά με αυτό, συλλέγονται και αποθηκεύονται και από ποιόν και σε ποιόν μπορεί να αποκαλυφθούν.

- **Ακεραιότητα** (Integrity): ο όρος αυτός σχετίζεται με δύο έννοιες:
  - **Ακεραιότητα δεδομένων** (Data integrity): εξασφαλίζει ότι οι πληροφορίες και τα προγράμματα μεταβάλλονται μόνο με καθορισμένο και εξουσιοδοτημένο τρόπο.
  - **Ακεραιότητα συστήματος** (System integrity): εξασφαλίζει ότι ένα σύστημα εκτελεί τις προγραμματισμένες λειτουργίες του, χωρίς εκούσιες ή ακούσιες παρεμβάσεις.

- **Διαθεσιμότητα** (Availability): Εξασφαλίζει ότι ένα σύστημα λειτουργεί απρόσκοπτα και είναι διαθέσιμο στους εξουσιοδοτημένους χρήστες του όποτε απαιτείται η χρήση του.

Αυτές οι τρεις έννοιες συχνά αναφέρονται ως τριάδα CIA (Confidentiality, Integrity, Availability)



Σχήμα 1 Οι τρεις πλευρές της ασφάλειας δεδομένων και υπηρεσιών (Stallings, 2011, p. 10)

και ενσαρκώνουν τις θεμελιώδεις αρχές ασφαλείας τόσο για δεδομένα όσο και για πληροφοριακά και υπολογιστικά συστήματα. Η λίστα περιλαμβάνει και άλλες απαιτήσεις ασφαλείας που μπορούν να περιγράψουν καλύτερα πιο εξειδικευμένες έννοιες, όμως οι παραπάνω είναι οι βασικότερες.

2.1.1. Διαθεσιμότητα Δικτύων και Κρίσιμες Υποδομές

Μεγάλη έμφαση στην ασφάλεια δικτύων έχει δοθεί κυρίως στις απαιτήσεις εμπιστευτικότητας και ακεραιότητας με αποτέλεσμα τη δημιουργία πολλών πρωτοκόλλων ασφαλείας και προτύπων, ανάμεσα στα οποία είναι το Secure Socket Layer (SSL), το Transport Layer Security (TLS), το Secure IP (IPSec), το Secure HTTP (S-HTTP), το secure e-mail (PGP, S/MIME), το Secure Shell (SSH) και το Kerberos.

Η διαθεσιμότητα των δικτύων, όμως, δεν έχει τύχει ανάλογης προσοχής (Qadir & Quadri, 2016). Μέχρι και πριν μερικά χρόνια τα δίκτυα εκλαμβάνονταν ως «δεδομένα» και συνεχώς διαθέσιμα. Τυχόν αστοχίες θεωρούνταν ως *παροδικά* φαινόμενα που συνήθως αποδίδονταν ή αντιμετωπίζονταν ως βλάβες.

Είναι πλέον κατανοητό και αποδεκτό ότι αυτή η θεώρηση πρέπει να αλλάξει, καθώς η σημερινή κοινωνία είναι βαθύτατα εξαρτημένη από την επιγραμμική (online) επικοινωνία και τη διαθεσιμότητα της πληροφορίας σε ψηφιακή μορφή. Η διαθεσιμότητα παίζει καθοριστικό ρόλο για τις απαιτήσεις (εμπιστευτικότητας και ακεραιότητας) της ασφάλειας δικτύων, γιατί και οι δύο είναι άμεσα εξαρτώμενες από την διαθεσιμότητα. Χωρίς αυτή δεν έχουν καν λόγο ύπαρξης. Αν δεν είναι διαθέσιμη η πληροφορία δε μπορεί να εφαρμοστεί κανένα άλλο χαρακτηριστικό της ασφάλειας.

Ο ρόλος των τηλεπικοινωνιακών δικτύων και του διαδικτύου (Internet) θεωρείται πλέον κρίσιμος σε όλες τις εκφάνσεις της λειτουργίας του κράτους και των υπηρεσιών, όπως ασφάλεια, υγεία, οικονομία αλλά και κοινωνική ζωή των πολιτών. Η σπουδαιότητα των τηλεπικοινωνιών οδήγησε την Ευρωπαϊκή Επιτροπή (Bisogni et al., 2004), τον Οκτώβριο του 2004 , στο να τις συμπεριλάβουν στη λίστα των κρίσιμων υποδομών (critical infrastructures), ως μέρος της μάχης ενάντια στην τρομοκρατία. Ειδικά το Ηνωμένο Βασίλειο έχει κατατάξει τις επικοινωνίες στο λίστα των δέκα πιο κρίσιμων εθνικών υποδομών (Telecommunications Networks – A Vital Part of the Critical National Infrastructure).

Η ψηφιοποίηση των υπηρεσιών κοινής ωφέλειας και κρατικών υποδομών και η διασύνδεσή και αλληλεξάρτηση τους συνεχώς και αυξάνεται. Για παράδειγμα η νέα γενιά έξυπνων δικτύων ηλεκτρικής ενέργειας (Smart Grid) που ενσωματώνει έξυπνα ενέργειες προερχόμενες από όλα τα συνδεδεμένα μέρη με στόχο να παρέχει αποδοτικότερα συντηρήσιμη, ασφαλή και οικονομική ενέργεια (Bojkovic & Bakmaz, 2012). Η συγκεκριμένη υποδομή επιτρέπει την αμφίδρομη επικοινωνία μεταξύ του παρόχου ενέργειας και των τελικών καταναλωτών, με τη χρήση ενός τεράστιου εύρους τεχνολογιών επικοινωνίας, όπως οπτικές ίνες, DLS, GSM, GPRS, EDGE, PLC, Wi-Fi (Elyengui, Bouhouchi & Ezzedine, 2013), όπου η αλληλεξάρτηση τους είναι θεμελιώδης και οι πληροφορίες που ανταλλάσσονται περιλαμβάνουν όχι μόνο στοιχεία πελατών και κατανάλωσης, αλλά και στοιχεία ελέγχων, οδηγίες προς εκτέλεση ή προς συσκευές, αναδρομολόγηση ροής ενέργειας και κινδυνεύει από επιθέσεις που μπορούν να προκαλέσουν blackout, υπερφόρτωση ή και να ρίξουν το δίκτυο ενέργειας σε μια ή περισσότερες χώρες (Mattioli & Moulinos, 2015).

Μολονότι είναι γεγονός ότι κυβερνοεπιθέσεις πραγματοποιούνται ολοένα και με μεγαλύτερη συχνότητα και ένταση, είτε δε δημοσιοποιούνται είτε δεν τους δίνεται ιδιαίτερη δημοσιότητα, με αποτέλεσμα να δημιουργείται μια ψευδής αίσθηση ασφάλειας και να υπάρχει άγνοια για τις συνέπειες τους στις ζωές και τις περιουσίες των πολιτών. Οι κυβερνήσεις, επιχειρήσεις και ιδιώτες γίνονται στόχος κυβερνοεπιθέσεων με εκθετικό ρυθμό. Παράλληλα, οι κρίσιμες δικτυακές υποδομές, ακόμα και αυτές που μέχρι σήμερα θεωρούνταν απαραβίαστες, έχουν γίνει δημοφιλής στόχος για άτομα ή ομάδες ατόμων, που φημολογείται ότι μπορεί και να είναι και χρηματοδοτούμενες από άλλα κράτη. Αυτό το γεγονός καταδεικνύει πόσο ευάλωτες είναι οι πόλεις, πολιτείες και κράτη και πόσο σημαντική είναι η επίτευξη μιας γενικευμένης ευελιξίας κινδύνου στο πρόσωπο τέτοιων απειλών (Wagner, 2018) (Staudemayer et al., 2018).

2.1.2. Επιθέσεις στη Διαθεσιμότητα Δικτύων

Υπάρχουν πολλά παραδείγματα όπου το Internet «γονάτισε» από την πολλή κίνηση, εκούσια και ακούσια (Denial of Service attacks ή Distributed Denial of Service attacks). Σε αυτές τις επιθέσεις στόχος είναι η εξάντληση των πόρων του συστήματος που

δέχεται την επίθεση, με αποτέλεσμα να μη μπορεί να εξυπηρετήσει τους κανονικούς του χρήστες.

Μία μεγάλη επίθεση DDoS έγινε το Φεβρουάριο του 2018 με στόχο το GitHub[2], μια υπηρεσία διαχείρισης κώδικα που χρησιμοποιείται από εκατομμύρια προγραμματιστές. Η μέγιστη εισερχόμενη κίνηση μετρήθηκε στα 1,3 TB το δευτερόλεπτο, στέλνοντας 126,9 εκατομμύρια πακέτα το δευτερόλεπτο. Στη συγκεκριμένη επίθεση δε χρησιμοποιήθηκαν botnet, καθώς οι επιτιθέμενοι εκμεταλλεύτηκαν την αδυναμία στον μηχανισμό caching μιας δημοφιλούς βάσης δεδομένων, που οδήγησε στην ενίσχυση της επίθεσης τους κατά 50.000 φορές. Τρεις μήνες μετά την επίθεση και ενώ ο αριθμός των ευάλωτων συσκευών, μετά την παγκόσμια κινητοποίηση, μειώθηκε από 50.000 σε μόλις 3.500, ο όγκος των επιθέσεων παρέμεινε σταθερός. Το γεγονός αυτό κατέδειξε ότι το χρονικό διάστημα ανάμεσα στην ανακάλυψη ενός νέου τύπου επίθεσης (και τη πρώτη επίδειξη των δυνατοτήτων της) και την μετατροπή της σε όπλο, μπορεί να είναι πολύ μικρό[3].

Μια άλλη επίθεση DDoS το πρώτο τρίμηνο του 2018 διήρκησε 12 ημέρες, η μεγαλύτερη χρονικά από το 2015, και όπως καταγράφηκε από τα εργαστήρια Kaspersky προήλθε από botnet επηρεάζοντας συνολικά 79 χώρες (Rayome, 2018). Το ίδιο έτος πραγματοποιήθηκε μεγάλης κλίμακας επίθεση DDoS στον ιστότοπο KrebsOnSecurity.com, η οποία τον έθεσε εκτός λειτουργίας για τέσσερις ημέρες. Η επίθεση πραγματοποιήθηκε από περίπου 24.000 παραβιασμένες συσκευές IoT (Internet of Things) και η σφοδρότητα της (μέχρι και 620 Gbps) οδήγησε τον τεχνολογικό γίγαντα Akamai, που είχε υπό την προστασία του τον ιστότοπο, να υποχωρήσει και να αφήσει τον ιστότοπο απροστάτευτο, γιατί είχαν αρχίσει να επηρεάζονται και οι υπόλοιποι πελάτες του[4].

Ένα άλλο παράδειγμα επίθεσης DDoS πραγματοποιήθηκε το 2015 στην ProtonMail, μια μικρή νεοφυή εταιρεία τεχνολογίας ασφαλούς ηλεκτρονικής αλληλογραφίας με έδρα την Ελβετία. Ήταν μια από τις μεγαλύτερες για την εποχή της. Κατά τη διάρκεια της

[2] Famous DDoS Attacks | The Largest DDoS Attacks Of All Time, CloudFlaire (2018)
https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/
[3] The Rise And Fall Of Memcached, NETSCOUT (2018, May 29)
https://www.netscout.com/news/blog/rise-and-fall-memcached
[4] Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K, Krebs on Security (2018, May 7)
https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/

επίθεσης, που διήρκησε πολλές ημέρες, τέθηκαν εκτός λειτουργίας βασικές υποδομές της εταιρείας, όπως το πρωτεύον κέντρο δεδομένων (datacenter) και χρειάστηκε η συνδρομή άλλων εταιρειών, αλλά και κυβερνητικών υπηρεσιών για την αντιμετώπισή της (Patterson, 2015).

Δε λείπουν όμως και ακούσιες επιθέσεις από λάθη ή αστοχίες. Τον Οκτώβριο του 2016, ένας δεκαοκτάχρονος βρίσκοντας ένα bug στο iOS μέσω ενός JavaScript exploit, θέλησε να αστειευτεί με τους φίλους του, στέλνοντας τους μια έκδοσή του, όπου θα εμφανίζονταν ενοχλητικά αναδυόμενα παράθυρα (Cimpanu, 2016). Έστειλε όμως κατά λάθος μια έκδοση που καλούσε τις αστυνομικές αρχές των ΗΠΑ (911) και το μοιράστηκε με 12.000 άτομα στο Twitter. Τα 1.849 άτομα που πάτησαν το σύνδεσμο ενεργοποίησαν κλήσεις στο κινητό τους στον αριθμό 911, με αποτέλεσμα, τουλάχιστον σε μια Πολιτεία, να θέσουν εκτός λειτουργίας το τηλεφωνικό σύστημα της αστυνομίας.

Ένα άλλο παράδειγμα είναι αυτό του χρήστη του Reddit που είχε εγκαταστήσει μια εφαρμογή ανοικτού κώδικα, η οποία μέσω ενός desktop widget έκανε ανανέωση στην αρχική σελίδα του ιστότοπου Reddit κάθε ένα λεπτό (Morris, 2011). Λόγω λανθασμένης ρύθμισης τελικά έκανε ανανέωση κάθε ένα millisecond, με αποτέλεσμα τη πρόκληση κίνησης της τάξης μεγέθους των 40 GB την ημέρα και τον αποκλεισμό του από την υπηρεσία (τουλάχιστον προσωρινά μέχρι να λυθεί η παρεξήγηση).

2.1.3. Τεχνικές Πρόληψης και Αντιμετώπισης Επιθέσεων

Για την αντιμετώπιση τέτοιων επιθέσεων έχουν αναπτυχθεί διάφορες τεχνολογίες που έχουν ως κύριο στόχο να απομονώσουν την «κακή» κίνηση. Σε αυτά τα συστήματα συγκαταλέγονται και τα Συστήματα Πρόληψης Εισβολών (Intrusion Prevention Systems, IPS). Αυτά τα συστήματα είτε σε μορφή λογισμικού είτε ολοκληρωμένου συστήματος, τοποθετούνται σε διάφορα στρατηγικά σημεία του δικτύου, με στόχο την ανάλυση της κίνησης, τη λήψη αποφάσεων και την εκτέλεση αυτοματοποιημένων ενεργειών. Για την αναγνώριση κακόβουλων κινήσεων ή ενεργειών χρησιμοποιούνται διάφορες τεχνικές, όπως αναγνώριση βάσει γνωστών αποτυπωμάτων, αναγνώριση ανωμαλιών ή και ανώτερες τεχνικές τεχνητής νοημοσύνης και μάθησης (Das & Nene, 2017). Όταν εντοπίσουν μια τέτοια κίνηση συνήθως οι ενέργειες που εκτελούν είναι η απόρριψη πακέτων ή η αποσύνδεση ώστε να μη φτάσει η κίνηση στον προορισμό της.

Η συνεισφορά των IPS στην ασφάλεια του δικτύου είναι μεγάλη, καθώς έχουν τη δυνατότητα να αναγνωρίζουν κακόβουλες ενέργειες και λογισμικά (malware), να τις σταματούν αλλά και να καταγράφουν από που έχουν προέλθει. Μειώνουν την έκθεση σε κίνδυνο για πολλά λογισμικά και υπηρεσίες, δίνοντας τον απαραίτητο χρόνο στους κατασκευαστές να ανιχνεύσουν τυχόν αδυναμίες και κερκόπορτες (backdoors).

Υπάρχουν όμως και αρκετά μειονεκτήματα, όπως οι συχνά λανθασμένες αποφάσεις, είτε θετικές όπου το σύστημα μπορεί να μπλοκάρει μια θεμιτή κίνηση γιατί απλά είναι έξω από τα συνηθισμένα με αποτέλεσμα την άρνηση της υπηρεσίας σε ένα χρήστη, είτε αρνητικές, όπου επιτρέπεται σε μια κακόβουλη κίνηση να εισέλθει στο δίκτυο. Ένα ακόμη μειονέκτημα είναι ότι παράγουν έναν τεράστιο όγκο συναγερμών (alert), ιδίως αυτά τα συστήματα που βασίζονται σε ένα μόνο τρόπο ανίχνευσης.

Το κόστος είναι μία σημαντική παράμετρος, καθώς για να έχει ένα δίκτυο τη καλύτερη προστασία θα πρέπει να εγκατασταθούν στοιχεία IPS σε πολλά σημεία του, που επιπλέον έχει και σαν συνέπεια τη μείωση της απόδοσης του δικτύου καθώς πολλά πακέτα δικτύου μπορεί να πρέπει να εξεταστούν πολλαπλές φορές κατά τη διαδρομή τους στο δίκτυο (Urrutia, Ierace & Bassett, 2005).

Μία άλλη τεχνολογία που χρησιμοποιείται συνδυαστικά είναι τα firewall. Πρόκειται για τείχη προστασίας συνήθως ανάμεσα σε ένα ιδιωτικό δίκτυο και το διαδίκτυο. Είναι σχεδιασμένα να παρακολουθούν την κίνηση που περνάει από αυτά και ακολουθώντας συγκεκριμένους κανόνες με τους οποίους έχουν ρυθμιστεί να επιτρέπουν σε πακέτα να περνάνε ή να τα απορρίπτουν. Οι κανόνες αυτοί μπορεί να είναι από πολύ απλοί έως και αρκετά πολύπλοκοι. Για παράδειγμα μπορεί να μετράται σε μια συγκεκριμένη χρονική περίοδο (παράθυρο χρόνου) ο αριθμός των πακέτων ανά πηγή και αν ξεπερνάει ένα συγκεκριμένο όριο να θεωρείται κακόβουλη κίνηση και να απορρίπτεται, χωρίς όμως να επηρεάζει προγενέστερη θεμιτή κίνηση από άλλη πηγή εν εξελίξει (Apiecionek & Makowski, 2015).

Μία άλλη θεώρηση είναι ότι μια θεμιτή επικοινωνία από μια συγκεκριμένη πηγή έχει μια λογική και αναμενόμενη ένταση (αριθμό πακέτων στη μονάδα του χρόνου), ενώ μια κακόβουλη επίθεση θα προσπαθήσει να στείλει πακέτα από πολλές τυχαίες πλαστές διευθύνσεις (για την απόκρυψη της ταυτότητας της, αλλά και για να δημιουργήσει την εικόνα ότι προέρχεται από πολλούς τυχαίους χρήστες) με αποτέλεσμα η κίνηση ανά διεύθυνση τελικά να είναι πολύ μικρή. Έτσι σε περίπτωση εντοπισμού επίθεσης DoS

(Denial Of Service) επιτρέπεται σε πακέτα από πηγές με λογική κίνηση και απορρίπτονται πακέτα από πηγές με στατιστικά πολύ χαμηλή κίνηση (Xu & Lee, 2004).

Τα firewall, όπως και κάθε εργαλείο, έχουν τις αδυναμίες τους. Δεν μπορούν να αποτρέψουν επιθέσεις που εκκινούν μέσα από το ίδιο το δίκτυο που καλούνται να προστατεύσουν ή από επιθέσεις σε κερκόπορτες. Μπορεί επίσης, εσφαλμένα να αποτρέψουν την πρόσβαση εξουσιοδοτημένου χρήστη σε αγαθά, οδηγώντας σε μία «εσωτερική» επίθεση άρνησης παροχής υπηρεσίας. Επίσης η παραμετροποίησή τους είναι πολύπλοκη και αν γίνει λανθασμένα δημιουργεί μία λανθασμένη αίσθηση ασφάλειας.

Τα firewall πολλές φορές ρυθμίζονται να επιτρέπουν μια κίνηση με βάση το είδος της (για παράδειγμα κίνηση email). Αυτό δε σημαίνει ότι μπορούν να παρέχουν προστασία από κακόβουλο περιεχόμενο που εμπεριέχεται σε αυτή (για παράδειγμα δεν προστατεύουν από ιούς που μεταφέρονται με email) (Advantages And Disadvantages Of Firewalls Computer Science Essay, 2016) (CCNA Security: Operational Strength & Weaknesses of Firewalls, n.d.).

Μια άλλη τεχνική είναι η Λευκή Λίστα (Whitelisting), που χρησιμοποιείται συνήθως για την αντιμετώπιση επιθέσεων SYN flooding. Οι επιθέσεις αυτές αποτελούν μία από τις κλασσικές επιθέσεις DoS που καταχράται τη διαδικασία χειραψίας TCP με στόχο να γεμίσει η ουρά των αιτημάτων σύνδεσης και να μην μπορούν να εξυπηρετηθούν τα πραγματικά/έγκυρα αιτήματα. Η τεχνική λευκής λίστας βασίζεται στη δημιουργία μιας λίστας, συνήθως με τη μορφή πίνακα, χρηστών/πελατών (συνήθως διευθύνσεις IP), τους οποίους ο εξυπηρετητής (server) θεωρεί εξουσιοδοτημένους/θεμιτούς. Χρησιμοποιώντας αυτή τη λίστα, αποφασίζεται αν οι νέες συνδέσεις θα προχωρήσουν ή όχι.

Ο πίνακας της λευκής λίστας αρχικά συμπληρώνεται από το διαχειριστή του συστήματος (εδώ μπορεί να χρησιμοποιηθεί το ιστορικό παλαιότερων συνδέσεων). Σε περίπτωση επίθεσης, αν η διεύθυνση IP που προσπαθεί να συνδεθεί είναι καταχωρημένη στη λίστα, η σύνδεση προχωράει κανονικά χρησιμοποιώντας την ουρά αιτημάτων, ενώ αν δεν είναι, αντιμετωπίζεται με την τεχνική του syncookie (όταν γεμίζει η ουρά ο server συνεχίζει τη διαδικασία για νέα αιτήματα, στέλνοντας πίσω μηνύματα SYN+ACK, χωρίς να τηρεί τα SYN στην ουρά, αλλά αποθηκεύοντας το sequence number σαν να ήταν cookie, ώστε σε περίπτωση σύνδεσης να μπορέσει να

ανασυνθέσει το αρχικό SYN) (Kim et al., 2008). Στη διάρκεια της επίθεσης η λίστα μπορεί να αυξηθεί με την προσθήκη IP που κατάφεραν να πραγματοποιήσουν σύνδεση, άρα είναι και έγκυρες, και μειώνεται αν ξεπεραστεί ένα κατώφλι μισο-ανοικτών (half-open) συνδέσεων ή αν γεμίσει η ουρά αιτημάτων, που σημαίνει ότι κάτι δε λειτουργεί σωστά και πρέπει να αρχικοποιηθεί πάλι η λίστα (Kim et al., 2008).

Στην πράξη έχει παρατηρηθεί ότι, αρκετές φορές, η διαχείριση μίας λευκής λίστας και η επικαιροποίησή της, για την αποφυγή εσφαλμένων παραλήψεων ή καταχωρήσεων, δεν πραγματοποιείται σε ικανοποιητικό βαθμό (The UGLY Truth Behind the Practice of IP Whitelisting..., 2018).

Έτσι με την πάροδο των ετών, λίστες αντί να συντηρούνται συχνά και συστηματικά, μειώνοντας ή τουλάχιστον συγκρατώντας τον αριθμό των διευθύνσεων IP που περιέχουν, τείνουν να αυξάνονται σε όγκο, με αδικαιολόγητες (έλλειψη κατάλληλης τεκμηρίωσης) συσσωρεύσεις διευθύνσεων.

Η ταξινόμηση της κίνησης (traffic classification) είναι μία τεχνική για την προστασία των δικτύων από κακόβουλη κίνηση, όπου χρησιμοποιώντας μεθόδους ευφυών συστημάτων, όπως ασαφή συστήματα (Alsirhani, Sampalli & Bodorik, 2018) και νευρωνικά δίκτυα (Kiziloren & Germen, 2007), γίνεται προσπάθεια ανίχνευσης επιθέσεων DoS. Ο διαχωρισμός της κανονικής (normal, legitimate) κίνησης από κάποια ανωμαλία λόγω επίθεσης, όπως DoS ή σάρωση πορτών (port scanning) είναι αρκετά δύσκολη υπόθεση. Η επιλογή των σωστών χαρακτηριστικών και η μείωση του μεγάλου αριθμού παραμέτρων ώστε να είναι εφικτή η αναγνώριση προτύπων (pattern recognition) ή η μηχανική εκμάθηση (machine learning), είναι καθοριστικής σημασίας (Aborujilah et al., 2013).

2.1.4. Περίσσεια Πόρων και Διαθεσιμότητα Δικτύου

Όλες οι παραπάνω τεχνολογίες και τεχνικές έχουν ως κύριο στόχο να φιλτράρουν, διαχωρίσουν, απομονώσουν και ουσιαστικά να μειώσουν την ανεπιθύμητη κίνηση. Μία διαφορετική προσέγγιση άμυνας είναι η αύξηση της χωρητικότητας και των πόρων του δικτύου, δηλαδή η δημιουργία περίσσειας (redundancy). Η προσέγγιση αυτή αντιμετωπίζεται ως τώρα ως *εφεδρική* λύση, σε περίπτωση αστοχίας των κύριων γραμμών σύνδεσης.

Στο (Leschiutta et al., 2007) η αξιοπιστία ενός συστήματος βελτιώνεται με τη δημιουργία περίσσειας μέσω πολλαπλών κόμβων και συνδέσεων, ώστε το δίκτυο να συνεχίσει να λειτουργεί σε περίπτωση σφάλματος σε έναν ή περισσότερους κόμβους, είτε λόγω ακραίων καιρικών συνθηκών είτε προβλημάτων παροχής ενέργειας είτε επανεκκινήσεων συσκευών, λόγω προσωρινής απώλειας ενέργειας ή μερικής βλάβη συσκευής. Ομοίως στο (Zhu, 2012) αναφέρεται η περίσσεια ως η κοινή λύση για την αποφυγή σφαλμάτων υλικών ή αστοχιών λογισμικού ενώ στο (Al-Khateeb, Al-Irhayim & Al-Khateeb, 2010) η περίσσεια νοείται ξεκάθαρα ως μια *δευτερεύουσα* διαδρομή για τη βελτίωση της αξιοπιστίας και την εξασφάλιση της ποιότητας της επικοινωνίας.

Στο (Devashryee, 2016) η βλάβη είναι αυτή που θα οδηγήσει στη δημιουργία περίσσειας στο δίκτυο με την έννοια της επιδιόρθωσης και ανάκτησης της λειτουργίας του δικτύου. Μερικά παραδείγματα τέτοιων βλαβών από τον πραγματικό κόσμο είναι τα εξής:

- 17 Ιουλίου 2015, ένα κομμένο καλώδιο οπτικών ινών αποκόπτει τρεις Κομητείες στην Καλιφόρνια των ΗΠΑ για 22 ώρες από το διαδίκτυο και την τηλεφωνία.
- 8 Ιουλίου 2015, μία αστοχία σε δρομολογητή θέτει εκτός λειτουργίας το σύστημα κρατήσεων της United Airlines για 90 λεπτά, με αποτέλεσμα 60 πτήσεις να ακυρωθούν και 800 να καθυστερήσουν.
- 6 Ιουλίου 2015, ένα κομμένο καλώδιο οπτικών ινών έχει ως αποτέλεσμα οι Βόρειες Μαριάνες Νήσοι να αποσυνδεθούν από το διαδίκτυο για περίπου δύο ημέρες.
- 11 Μαρτίου 2011, ο μεγαλύτερος σεισμός στην σύγχρονη ιστορία της Ιαπωνίας, σε συνδυασμό με το τσουνάμι που ακολούθησε, κατέστρεψαν τηλεπικοινωνιακά συστήματα μεταγωγής και υποβρύχια καλώδια διεθνών επικοινωνιών (Gomes et al., 2016).
- 26 Δεκεμβρίου 2006, σεισμός στη νότια Ταϊβάν είναι υπεύθυνος για διακοπές στις διεθνείς επικοινωνίες Κίνας, Χονγκ Κονγκ, Κορέας, Ιαπωνίας και Ταϊβάν, λόγω των ταυτόχρονων βλαβών σε επτά υποβρύχιες συνδέσεις παροχής διαδικτύου ανάμεσα σε Ασία και Βόρεια Αμερική (Gomes et al., 2016).
- 29 Αυγούστου 2005, ο τυφώνας «Κατρίνα» προκαλεί τεράστιες ζημιές, εκτός των άλλων, και στις τηλεπικοινωνιακές υποδομές (Gomes et al., 2016).

2.1.5. Μη Συμβατικά Πρωτόκολλα Δρομολόγησης

Η σύγχρονη θεώρηση των δικτύων και ιδιαίτερα των ασύρματων θέτει τη διαθεσιμότητα ως πρώτη και κύρια προτεραιότητα εκ νέου. Σε αυτή τη θεώρηση, πολλαπλά μονοπάτια χρησιμοποιούνται *ταυτόχρονα κάθε στιγμή* για τη δρομολόγηση της κίνησης. Τα παραδοσιακά πρωτόκολλα δρομολόγησης ad-hoc χρησιμοποιούν μόνο μία μοναδική διαδρομή για κάθε παραλήπτη. Αντίθετα, τα σύγχρονα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών (multipath routing) διανέμουν την κίνηση μέσα από διαφορετικές διαδρομές για τον ίδιο παραλήπτη, συνήθως για διαφορετικές ροές δεδομένων την κάθε μία.

Μια τέτοια περίπτωση multipath routing είναι το Split Multipath Routing (SMR), το οποίο δημιουργεί πολλαπλές διαδρομές από την πηγή στον παραλήπτη. Η πρώτη συνήθως είναι αυτή με την μικρότερη καθυστέρηση και για τις υπόλοιπες επιλέγονται όσες έχουν όσο το δυνατόν μη κοινά τμήματα με την πρώτη, αλλά επίσης και τον μικρότερο αριθμό ενδιάμεσων κόμβων (Lee & Gerla, 2001).

Ένα άλλο πρωτόκολλο που ανήκει στα κατά απαίτηση (on-demand) πρωτόκολλα ανεύρεσης διαδρομών δρομολόγησης, είναι το πρωτόκολλο Dynamic Source Routing (DSR) (Nasipuri, Castaneda & Das, 2001). Το DSR χρησιμοποιείται για να παράσχει έναν εύκολο μηχανισμό διανομής της κίνησης και εξισορρόπησης του φορτίου του δικτύου, αλλά και να αυξήσει την ανθεκτικότητα σε σφάλματα. Βέβαια η χρησιμοποίηση τέτοιων πρωτοκόλλων στην περίπτωση του TCP είναι πιο δύσκολη και δεν αποφέρει πάντα τα επιθυμητά αποτελέσματα, λόγω του μεγάλου προβλήματος της παραλαβής πακέτων, από διαφορετικές διαδρομές, με τη λάθος σειρά (Lim, Xu & Gerla, 2003). Η βέλτιστη λύση δίνεται με τη χρήση, πάλι, των εναλλακτικών διαδρομών ως εφεδρικών.

Το πρωτόκολλο Ad-hoc On-demand Distance Vector (AODV) είναι ένα πρωτόκολλο δρομολόγησης σχεδιασμένο για κινητά ασύρματα δίκτυα ad hoc (Mobile Ad-hoc Networks, MANET). Αν ένας κόμβος ή πηγή θέλει να στείλει ένα μήνυμα σε έναν παραλήπτη, τότε κάνει μια ευρεία εκπομπή (broadcast) ενός αιτήματος δρομολόγησης (routing request) στο δίκτυο. Οι υπόλοιποι κόμβοι προωθούν το αίτημα και καταγράφουν τον κόμβο που το έστειλε. Αυτό έχει ως αποτέλεσμα να φτάσει στον παραλήπτη ένα πλήθος αιτημάτων δρομολόγησης από διαφορετικές διαδρομές. Αν

υπάρχει ένας κόμβος που γνωρίζει ήδη τη διαδρομή προς τον παραλήπτη, απαντάει με μία απάντηση δρομολόγησης (routing reply), η οποία ταξιδεύει προς τα πίσω μέχρι την πηγή, μέσω των κόμβων που πέρασε το αρχικό αίτημα δρομολόγησης. Στην αντίθετη περίπτωση ο παραλήπτη παραλαμβάνει το αίτημα δρομολόγησης και χρησιμοποιεί τη διαδρομή με τα λιγότερα ενδιάμεσα βήματα (hop). Όταν μια επικοινωνία αποτύχει ένα μήνυμα σφάλματος (routing error) επιστρέφεται πίσω στην πηγή (Vu, 2014). Καθώς η παραπάνω διαδικασία πραγματοποιείται μόνο όταν απαιτείται επιτυγχάνεται χαμηλή κατανάλωση ενέργειας.

Τα Δίκτυα Ανθεκτικά σε Καθυστέρηση (Delay Tolerant Networks, DTN) είναι δίκτυα τα οποία μπορούν να διαχειριστούν μεγάλες καθυστερήσεις, ακόμη και της τάξης ημερών (Voyiatzis, 2012). Αναφέρονται στη βιβλιογραφία και ως Δίκτυα Ανθεκτικά σε Διαταραχές (Disruption Tolerant Networks). Σε αυτά τα δίκτυα τις περισσότερες φορές δεν υπάρχει πλήρης διαδρομή από την πηγή στον παραλήπτη ή, όταν υπάρχει, είναι αρκετά ασταθής.

Η δρομολόγηση σε δίκτυα DTN βασίζεται περισσότερο σε αποφάσεις προώθησης από κόμβο σε κόμβο, παρά στην εύρεση μιας πλήρους διαδρομής δρομολόγησης από πηγή σε παραλήπτη (Liu, Tang & Yu, 2012). Για αυτή την περίπτωση τα πρωτόκολλα ασύρματων δικτύων ad hoc (για παράδειγμα DRS και AODV) δε λειτουργούν ικανοποιητικά (Bai et al., 2014). Χρησιμοποιούνται δύο κατηγορίες πρωτοκόλλων δρομολόγησης: τα πρωτόκολλα μη ελεγχόμενης αναπαραγωγής (uncontrolled replication routing) και τα πρωτόκολλα ελεγχόμενης αναπαραγωγής (controlled replication routing), που γενικά επιτυγχάνουν μεγαλύτερο ρυθμό πακέτων που λαμβάνονται με κόστος τη χρονική καθυστέρηση στη λήψη (Bai et al., 2014). Στην πρώτη κατηγορία ανήκει το πρωτόκολλο επιδημιακής δρομολόγησης (epidemic routing protocol) που βασίζεται σε απλές τεχνικές δρομολόγησης πλημμυρίδας (flood routing) και πετυχαίνει μικρούς χρόνους παράδοσης με κόστος όμως σε ενέργεια και κατανάλωση εύρους ζώνης. Στη δεύτερη κατηγορία ανήκουν τα πρωτόκολλα Spray & Wait και όλες οι παραλλαγές τους όπως για παράδειγμα Binary Spray & Wait (BSW), Spray & Focus (SF) και Adaptive Spray & Wait (R-ASW), που βελτιώνουν ρυθμό παράδοσης πακέτων μειώνοντας το «φόρτωμα» του δικτύου με «άχρηστη» πληροφορία (Liu, Tang & Yu, 2012).

Έχουν, λοιπόν, προταθεί πολλά πρωτόκολλά με διαφορετικά σημεία αριστοποίησης για την επίτευξη διαφορετικών και ενίοτε αλληλο-συγκρουόμενων στόχων, όπως έγκαιρη παράδοση, κατανάλωση ενέργειας, πλήθος παραληπτών, ρυθμός πακέτων που λαμβάνονται από ένα παραλήπτη, χρονική καθυστέρηση στη λήψη, κατανάλωση εύρους ζώνης.

2.2. Κωδικοποίηση Δικτύου (Network Coding)

Τα επικοινωνιακά δίκτυα από τις αρχές του 1960, οπότε και δημιουργήθηκε ένα από τα μεγαλύτερα δίκτυα μεταγωγής πακέτων, το ARPANET (το πρώτο που χρησιμοποιούσε το πρωτόκολλο TCP/IP, που αργότερα εξελίχθηκε στο σημερινό διαδίκτυο), έχουν εξελιχθεί δραματικά. Παραδόξως, όμως, η μετάδοση ενός πακέτου βασίζεται ακόμα στην ίδια βασική αρχή που βασιζόταν και τότε, τη λογική δηλαδή της μετακίνησης όπως με ένα αυτοκίνητο: πληροφορίες ή άνθρωποι ταξιδεύουν, αλλά πάντα ξεχωριστά και ως μια συνεχής οντότητα. Σε όλες τις δεκαετίες που ακολούθησαν, αυτή η βασική θεώρηση διατηρήθηκε σε όλα τα μέρη ενός δικτύου (δρομολογητές, αποθηκευτικές συσκευές κλπ.) για να μπορέσει να λειτουργήσει (Vu, 2014).

Από τις πρώιμες ήδη μελέτες σε ψηφιακά συστήματα (Tooley, 1963), φάνηκε ότι η ενσωμάτωση λειτουργιών λογικής διόρθωσης σφαλμάτων σε λογικά κυκλώματα και η εισαγωγή περίσσειας πληροφορίας, ακόμα και στο χαμηλό επίπεδο των ολοκληρωμένων κυκλωμάτων, μπορεί να οδηγήσει σε ένα υψηλότερο βαθμό αξιοπιστίας από ότι οι κλασσικές τεχνικές.

Το 1956 τα (Ford & Fulkerson, 1956) και (Elias, Feinstein & Shannon, 1956) έδειξαν ότι η μέγιστη τιμή της ροής σε ένα δίκτυο ισούται με την τιμή της ελάχιστης τομής, παρουσιάζοντας το θεώρημα «Ελάχιστης Τομής – Μέγιστης Ροής» (Min-Cut Max-Flow).

Έως τις αρχές του 21ου αιώνα, η έννοια της κωδικοποίησης (coding) στα (τηλεπικοινωνιακά) δίκτυα, αφορούσε στην

- Κωδικοποίηση Πηγής (Source Coding), ως ένα μέσο συμπίεσης της πληροφορίας στην πηγή, με στόχο την αύξηση της αποδοτικότητας της μετάδοσης, και την

- Κωδικοποίηση Καναλιού (Channel Coding), την λειτουργία, δηλαδή, προσθήκης περίσσιων bits στην πληροφορία με στόχο να γίνει πιο αξιόπιστη, μετατρέποντας ένα θορυβώδες κανάλι σε αθόρυβο.

Το 2000 το πρωτοπόρο άρθρο (Ahlswede et al., 2000) άλλαξε τη μέχρι τότε θεώρηση με την εισαγωγή της έννοιας της ροής της πληροφορίας (information flow), για να δείξει, ότι ο συνδυασμός της πληροφορίας μπορεί να αυξήσει την χωρητικότητα ενός δικτύου πάνω από την τιμή που έχει επιτευχθεί με την παραδοσιακή δρομολόγηση και να προσεγγίσει το όριο του θεωρήματος Min-Cut Max-Flow. Αυτή η προσέγγιση οδήγησε στην γέννηση μιας νέας περιοχής έρευνας, την Κωδικοποίηση Δικτύου (Network Coding).

Η κωδικοποίηση δικτύου αφορά σε μία νέα λειτουργία σε επίπεδο πακέτου: οι κόμβοι του δικτύου εκτελούν κάποιες λειτουργίες κωδικοποίησης. Έτσι ένας κόμβος μπορεί να συνδυάζει και να «κωδικοποιεί» ένα ή περισσότερα πακέτα εισόδου, δηλαδή να δημιουργεί συναρτήσεις των πακέτων σε ένα νέο, κωδικοποιημένο πακέτο, αντί απλά να τα προωθεί αυτούσια, όπως τα έχει παραλάβει. Με άλλα λόγια, οι ροές δεδομένων που έχουν παραχθεί ανεξάρτητα δεν είναι υποχρεωτικό να κρατηθούν χωριστά όταν διαδίδονται στο δίκτυο. Για παράδειγμα στο επίπεδο δικτύου οι ενδιάμεσοι κόμβοι μπορούν να εκτελούν δυαδικές πράξεις, όπως προσθέσεις, σε ανεξάρτητα bitstream (Nazer & Gastpar, 2011), ενώ στο φυσικό επίπεδο, όπως σε οπτικά δίκτυα, οι ενδιάμεσοι κόμβοι μπορούν να υπερθέτουν τα εισερχόμενα οπτικά σήματα (Fragouli & Soljanin, 2006).

Η κωδικοποίηση δικτύου μπορεί να αυξήσει το ποσό της ροής της πληροφορίας σε ένα δίκτυο γιατί η ροή πληροφορίας (information flow) είναι ουσιωδώς διαφορετική από την ροή είδους (commodity flow) (Rashmi, Shah & Kumar, 2010). Σε αντίθεση με τις παραδοσιακές μεθόδους, όπου οι ενδιάμεσοι κόμβοι περιορίζονται στο να προωθούν τα εισερχόμενα πακέτα ή σύμβολα, στην κωδικοποίηση δικτύου επιτυγχάνεται μεγάλο κέρδος στην απόδοση και στην αξιοπιστία μετάδοσης, επιτρέποντας σε ενδιάμεσους κόμβους του δικτύου να εκτελούν αλγεβρικές πράξεις στα εισερχόμενα δεδομένα. Η κωδικοποίηση δικτύου μπορεί να θεωρηθεί ότι αποτελεί γενίκευση των τεχνικών διόρθωσης σφαλμάτων (Error Correcting Codes), όπου όμως η περίσσεια εφαρμόζεται στον χώρο και όχι στο χρόνο (Bassoli et al., 2013).

2.3. Θεωρία Κωδικοποίησης Δικτύου

2.3.1. Βασικοί ορισμοί

Έστω ένα δίκτυο που αποτελείται από ένα κατευθυνόμενο γράφο, όπου κάθε ακμή του γράφου έχει μια καθορισμένη κατεύθυνση που μπορεί να μεταδίδει δεδομένα. Ο γράφος θεωρείται ότι δεν περιέχει κύκλους, δηλαδή είναι ακυκλικός. Ένας κόμβος στον γράφο είναι μια πηγή που παράγει συγκεκριμένο αριθμό συμβόλων στη μονάδα του χρόνου. Κάθε σύμβολο θεωρείται ότι ανήκει σε ένα πεπερασμένο πεδίο F_q μεγέθους q και η τιμή του έχει επιλεγεί τυχαία από την πηγή.

Κάθε ακμή έχει μια καθορισμένη χωρητικότητα, δηλαδή τον αριθμό των συμβόλων που μπορεί να μεταδώσει στη μονάδα του χρόνου. Ο ρυθμός της πηγής και οι χωρητικότητες των ακμών θεωρούνται μη αρνητικοί ακέραιοι. Ένα υποσύνολο των κόμβων είναι δέκτες και όλοι οι δέκτες χρειάζονται όλα τα δεδομένα που παράγει η πηγή. Αυτό ονομάζεται ένα δίκτυο πολυεκπομπής, δηλαδή ένα δίκτυο με ταυτόχρονη διάδοση της ίδιας πληροφορίας σε πολλαπλούς δέκτες.

Κάθε κόμβος του δικτύου μπορεί να επεξεργάζεται και να συνδυάζει την πληροφορία που λαμβάνει από τους διαφορετικούς κόμβους και να την μεταφέρει στις εξερχόμενες ακμές του. Το πρόβλημα της Κωδικοποίησης Δικτύου, είναι ο καθορισμός αυτών των συνδυασμών, που εκτελούν οι κόμβοι του δικτύου, ώστε να διασφαλίζεται ότι όλα τα σύμβολα της πηγής θα παραληφθούν από όλους τους δέκτες.

Διαδρομή: ονομάζεται μια ακολουθία διαδοχικών ακμών, ενώ **μονοπάτι** μια διαδρομή χωρίς επανάληψη ακμών. **Ακυκλικός** γράφος είναι ένας γράφος χωρίς κύκλους, δηλαδή μονοπάτια που τα άκρα τους να ταυτίζονται.

Ροή: η ροή σε μια ακμή αναπαριστά τον αριθμό των συμβόλων που μεταδίδει, στη μονάδα του χρόνου, σε ένα σύστημα και που προφανώς δε μπορεί να είναι μεγαλύτερη από την χωρητικότητα της ακμής. Σύμφωνα με τον 1ο κανόνα του Κίρκοφ (Kirchhoff) σε κάθε ενδιάμεσο κόμβο η ροή που εισέρχεται σε έναν κόμβο πρέπει να ισούται με αυτή που εξέρχεται. Αυτό τουλάχιστον ισχύει σε παραδοσιακά δίκτυα, όπου κανένας ενδιάμεσος κόμβος δε μπορεί να αποθηκεύει ή να παράγει τίποτα από μόνος του, παρά μόνο να μεταδίδει αυτό που λαμβάνει. Θεωρώντας μια εικονική ακμή στην πηγή και μια

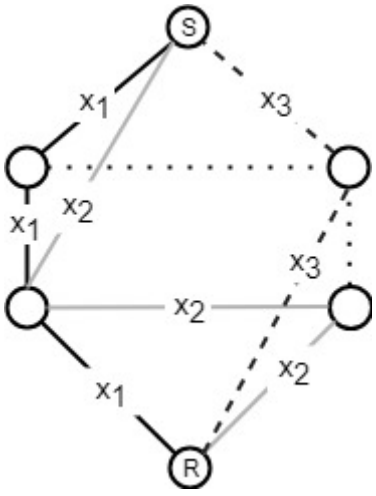
στον δέκτη, με ροές ίσες με το ρυθμό παραγωγής συμβόλων στην πηγή, η αμιγής ροή προς το δίκτυο ισούται με την ροή που εξέρχεται του δικτύου. Αυτή η τιμή της ροής είναι η τιμή της ροής όλου του δικτύου.

Η Τομή και η χωρητικότητα της: τομή ονομάζεται ο διαχωρισμός του δικτύου σε 2 μέρη, S και S_c. Η πηγή ανήκει στο S και ο δέκτης στο S_c. Η συνολική χωρητικότητα όλων των ακμών που οδηγούν από τους κόμβους του S στους κόμβους του S_c, ονομάζεται χωρητικότητα της τομής. Η χωρητικότητα της ελάχιστης τομής του δικτύου, είναι η ελάχιστη τιμή των χωρητικοτήτων όλων των τομών του δικτύου (Rashmi, Shah & Kumar, 2010).

2.3.2. Θεώρημα Ελάχιστης Τομής – Μέγιστης Ροής

Έστω ένας γράφος $G = (V, E)$ με ακμές μοναδιαίας χωρητικότητας (δηλαδή ένα σύμβολο στη μονάδα του χρόνου), μια πηγή S και έναν δέκτη R. Αν η ελάχιστη τομή μεταξύ S και R είναι ίση με h, τότε η πληροφορία που μπορεί να σταλεί από τον S στον R έχει μέγιστο ρυθμό h. Ισοδύναμα, υπάρχουν ακριβώς h διαδρομές, με διαφορετικές ακμές, ανάμεσα σε S και R.

Με άλλα λόγια, η μέγιστη τιμή της ροής του δικτύου ισούται με την χωρητικότητα της ελάχιστης τομής του δικτύου. Για παράδειγμα στο Σχήμα 2 υπάρχουν τρεις διαδρομές με διαφορετικές ακμές ανάμεσα σε S και R και η ελάχιστη τομή έχει χωρητικότητα 3, όσο και ο μέγιστος ρυθμός μετάδοσης (μέγιστη ροή).



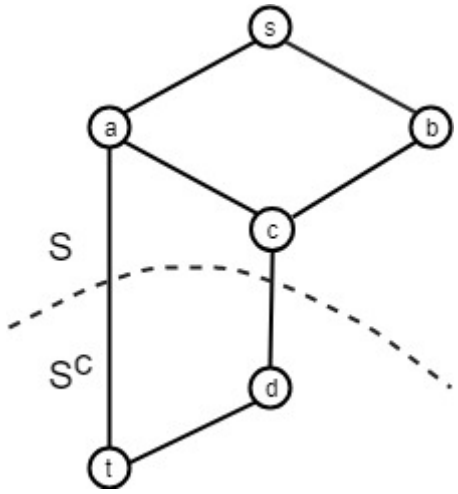
Σχήμα 2 Διαδρομές μονοεκπομπής (Fragouli & Soljanin, 2006)

2.3.3. Θεώρημα Menger

Ο αριθμός των διαδρομών χωρίς κοινές ακμές (edge-disjoint) από την πηγή στον δέκτη, ισούται με την μέγιστη ροή του δικτύου. Στην περίπτωση ακμών με μη μοναδιαίες χωρητικότητες, κάθε ακμή μπορεί να θεωρηθεί ότι χωρίζεται σε πολλαπλές παράλληλες ακμές μοναδιαίας χωρητικότητας, ώστε να μπορεί να εφαρμοστεί το θεώρημα.

Έτσι σε ένα δίκτυο με έναν μόνο δέκτη, ένας αριθμός συμβόλων που ισούται με τη χωρητικότητα της ελάχιστης τομής του δικτύου, μπορεί να μεταδοθεί από την πηγή στον δέκτη στη μονάδα του χρόνου, με το κάθε σύμβολο να μεταδίδεται από διαφορετική διαδρομή χωρίς κοινές ακμές.

Στο Σχήμα 3 η χωρητικότητας της τομής είναι δύο σύμβολα στη μονάδα του χρόνου και μπορεί να επιβεβαιωθεί ότι αυτή είναι και η τιμή της χωρητικότητας της ελάχιστης τομής του δικτύου. Όντως υπάρχουν μόνο δύο διαδρομές χωρίς κοινές ακμές από την πηγή στον δέκτη, οπότε η μέγιστη ροή του δικτύου είναι 2.



Σχήμα 3 Τομή σε ένα δίκτυο (Rashmi, Shah & Kumar, 2010)

2.3.4. Βασικό Θεώρημα Κωδικοποίησης Δικτύου

Ορισμός: Η Κωδικοποίηση Δικτύου είναι μια τεχνική που επιτρέπει στους κόμβους να συνδυάζουν αρχικά πακέτα σε ένα κωδικοποιημένο πακέτο προς αποστολή, αντί απλά να τα προωθούν ένα προς ένα, με στόχο την αύξηση της χωρητικότητας του δικτύου.

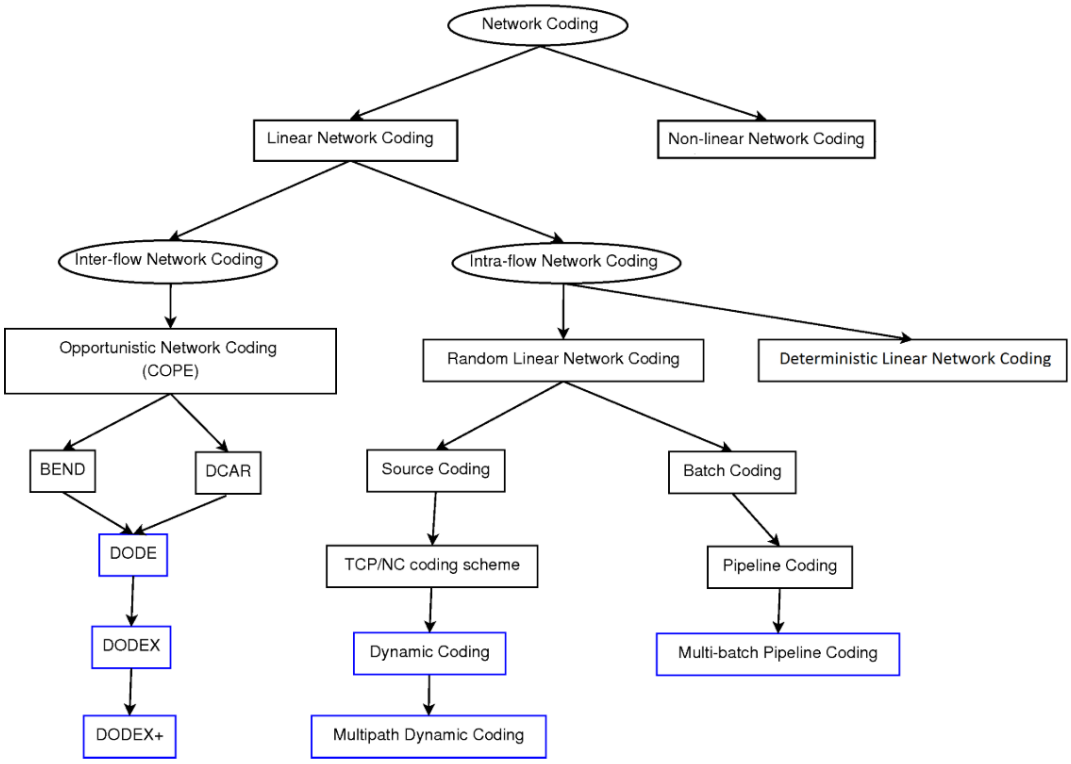
Θεώρημα: Έστω κατευθυνόμενος ακυκλικός γράφος $G = (V, E)$ με ακμές μοναδιαίας χωρητικότητας, h πηγές με μοναδιαίο ρυθμό, τοποθετημένες στην ίδια κορυφή του

γράφου και N δέκτες. Ας υποθέσουμε ότι η τιμή της ελάχιστης τομής για κάθε δέκτη είναι h. Τότε υπάρχει ένα σχήμα πολυεκπομπής πάνω σε ένα αρκετά μεγάλο πεπερασμένο πεδίο F_q, στο οποίο ενδιάμεσοι κόμβοι συνδυάζουν γραμμικά τα εισερχόμενα πληροφοριακά σύμβολα πάνω στο F_q, που διανέμει την πληροφορία από τις πηγές ταυτόχρονα σε κάθε δέκτη με ρυθμό ίσο με h.

Δηλαδή αν οι ενδιάμεσοι κόμβοι μπορούν, όχι μόνο να προωθούν, αλλά και να συνδυάζουν σωστά την εισερχόμενη πληροφορία, τότε μπορεί να προσεγγιστεί το όριο για πολύ-εκπομπή (Li, Yeung & Cai, 2003) και όλοι οι αποδέκτες να λαμβάνουν την πληροφορία με τον ίδιο ρυθμό που θα την λάμβαναν αν είχαν την αποκλειστική πρόσβαση σε όλους τους πόρους του δικτύου (Fragouli & Soljanin, 2006).

2.3.5. Είδη Κωδικοποίησης

Οι βασικές κατηγορίες κωδικοποίησης δικτύου φαίνονται στο Σχήμα 4 (Vu, 2014) (Bhatia, Patel & Narmawala, 2011):



Σχήμα 4 Είδη Κωδικοποίησης (Vu, 2014)

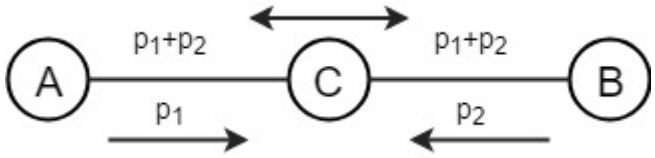
Αρχικά διακρίνονται σε:

- *Γραμμική Κωδικοποίηση Δικτύου (Linear Network Coding LNC)*: χρησιμοποιούνται γραμμικοί συνδυασμοί των πακέτων για την παραγωγή των κωδικοποιημένων πακέτων, κυρίως προσθέσεις και πολλαπλασιασμοί, σε ένα αλγεβρικό πλαίσιο σε ένα πεπερασμένο πεδίο F_q (Koetter & Medard, 2001). Επειδή οι πράξεις πραγματοποιούνται πάνω στο πεδίο Galois (ένα πεδίο που περιέχει πεπερασμένο αριθμό στοιχείων), οι συνδυασμοί των συμβόλων που προκύπτουν, έχουν το ίδιο μέγεθος που έχει και ένα χωριστό σύμβολο (Segovia, 2012).

- *Μη Γραμμική Κωδικοποίηση Δικτύου (Nonlinear Network Coding)*: υπάρχουν περιπτώσεις που με την γραμμική κωδικοποίηση δε μπορεί να επιτευχθεί η μέγιστη χωρητικότητα του δικτύου και χρησιμοποιούνται μη-γραμμικοί συνδυασμοί των πακέτων.

Από την κατηγορία των γραμμικών κωδικοποιήσεων διακρίνονται οι εξής:

- *Κωδικοποίηση δικτύου inter-flow*: πρόκειται για κωδικοποίηση πακέτων από πολλαπλές ροές σε ένα κοινό κόμβο και χρησιμοποιείται συνήθως για τη βελτίωση της ρυθμαπόδοσης (throughput). Ένα τέτοιο παράδειγμα είναι η οπορτουνιστική (ευκαιριακή) κωδικοποίηση δικτύου (Opportunistic Network Coding ONC) που συνδυάζει πακέτα (για παράδειγμα με exclusive-OR, XOR) από ροές που ταξιδεύουν σε αντίθετες κατευθύνσεις, σε ένα ενδιάμεσο κόμβο που ονομάζεται «κωδικοποιητής», όπως φαίνεται στο Σχήμα 5.



Σχήμα 5 Παράδειγμα οπορτουνιστικής κωδικοποίησης (Vu, 2014)

- *Κωδικοποίηση δικτύου intra-flow*: είναι η κωδικοποίηση πακέτων από την ίδια ροή και συνήθως χρησιμοποιείται για τη βελτίωση της αξιοπιστίας. Τέτοιο παράδειγμα είναι η Τυχαία Γραμμική Κωδικοποίηση Δικτύου (Random Linear Network Coding, RLNC), ένας κατανεμημένος αλγόριθμος κωδικοποίησης (Ho et al., 2003) (Ho et al., 2006). Με τη σειρά της διακρίνεται σε:

- *Τύπου κωδικοποίησης πηγής (source coding)*: όπου η πηγή παράγει κωδικοποιημένα πακέτα μαζί με κωδικοποιημένα πακέτα περίσσειας και τα στέλνει στον παραλήπτη. Εδώ οι ενδιάμεσοι κόμβοι απλά προωθούν τα πακέτα στον προορισμό τους.

- *Τύπου κωδικοποίησης δέσμης (batch coding):* όπου η πηγή παράγει κωδικοποιημένα πακέτα μαζί με κωδικοποιημένα πακέτα περίσσειας και τα στέλνει στον παραλήπτη. Εδώ οι ενδιάμεσοι κόμβοι εκτελούν επανα-κωδικοποίηση, παράγοντας και μεταδίδοντας νέους γραμμικούς συνδυασμούς των πακέτων προς τον παραλήπτη.

Ένα άλλο παράδειγμα είναι η Ντετερμινιστική (Αιτιοκρατική) Γραμμική Κωδικοποίηση Δικτύου (Deterministic Linear Network Coding, DLNC), όπου ειδικοί αλγόριθμοι χρησιμοποιούνται για την ανεύρεση συντελεστών κωδικοποίησης που θα εξασφαλίσουν τη γραμμική ανεξαρτησία των κωδικοποιημένων πακέτων.

2.4. Τυχαία Γραμμική Κωδικοποίηση Δικτύου (RLNC)

Ας θεωρήσουμε μια πηγή που έχει ένα μήνυμα να στείλει. Μπορούμε να δούμε αυτό το μήνυμα ως μια αλληλουχία από πακέτα $p_1, p_2, \ldots$ Το n-ιοστό πακέτο του αρχικού μηνύματος λέγεται ότι έχει δείκτη n. Ένα πακέτο p_j μπορεί να θεωρηθεί ως ένα διάνυσμα στο πεπερασμένο πεδίο F_q μεγέθους q, ομαδοποιώντας τα bit ενός πακέτου σε L ομάδες (γκρουπ) μεγέθους $log_2(q)$ bit, οι οποίες ονομάζονται σύμβολα:

$$p_j = [p_{j1} \quad p_{j2} \quad \cdots \quad p_{jL}]$$

Για παράδειγμα σε ένα κλασσικό δίκτυο ένα πακέτο μπορεί να αποτελείται από 1.400 byte, οπότε αν χρησιμοποιηθεί το πεπερασμένο πεδίο F_{256} (μεγέθους $q = 256$), τότε μπορεί να θεωρηθεί ότι αποτελείται από $L = 1.400$ σύμβολα μεγέθους $log_2(256) = 8$ bit το κάθε ένα.

Ένας κόμβος, εκτός από το να προωθεί τα εισερχόμενα πακέτα, μπορεί επίσης να εκτελεί γραμμική κωδικοποίηση σε αυτά. Αυτό σημαίνει ότι ένας κόμβος μπορεί να μεταδίδει ένα πακέτο που παράγεται από το γραμμικό συνδυασμό των αντίστοιχων

διανυσμάτων των εισερχόμενων N πακέτων, με συντελεστές επιλεγμένους από το πεδίο F_q. Για παράδειγμα μπορεί να εκπέμψει, για $N = 2$, το

$$\boldsymbol{x_1} = c_{11}\boldsymbol{p_1} + c_{12}\boldsymbol{p_2}$$

και

$$\boldsymbol{x_2} = c_{21}\boldsymbol{p_1} + c_{22}\boldsymbol{p_2}$$

όπου $c_{11}, c_{12}, c_{21}, c_{22} \in F_q$.

Αν υποθέσουμε, λοιπόν, ότι τα πακέτα αποτελούνται από L σύμβολα, τότε μπορεί να γραφτεί με τη μορφή πίνακα:

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1L} \\ x_{21} & x_{22} & \cdots & x_{2L} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \cdot \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1L} \\ p_{21} & p_{22} & \cdots & p_{2L} \end{bmatrix}$$

ή συνοπτικά

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \cdot \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

ή

$$X = C \cdot B$$

όπου B είναι τα αρχικά πακέτα, γνωστό και ως *διάνυσμα πληροφορίας*, C ονομάζεται ο πίνακας συντελεστών κωδικοποίησης (coefficient matrix) σε ένα πεδίο Galois και X είναι το νέο κωδικοποιημένο πακέτο μήκους L συμβόλων (Sundararajan et al., 2011).

Σε αλγεβρική μορφή:

$$x_i = \sum_{j=1}^{N} c_{ij} p_j$$

όπου για κάθε κωδικοποιημένο πακέτο x_ι, που ονομάζεται διάνυσμα πληροφοριών (information vector), υπάρχει η ακολουθία συντελεστών $(c_{\iota 1}, \ldots, c_{\iota N})$, που ονομάζεται διάνυσμα κωδικοποίησης (encoding vector), και περιέχει τους τοπικούς συντελεστές κωδικοποίησης του πακέτου.

Η ίδια διαδικασία ακολουθείται και για την επανα-κωδικοποίηση από τους ενδιάμεσους κόμβους (εφόσον πραγματοποιείται) και το συνολικό αποτέλεσμα μπορεί πάλι να

αποτυπωθεί ως μια τέτοια γραμμική σχέση με το συνολικό πίνακα κωδικοποίησης. Ο κάθε κόμβος ενσωματώνει στην επικεφαλίδα (header) των κωδικοποιημένων πακέτων που παράγει τους αντίστοιχους συντελεστές κωδικοποίησης ως διάνυσμα συντελεστών (coefficient vector). Αυτή η επιβάρυνση του πακέτου είναι πολύ μικρή και μειώνεται καθώς αυξάνει το μέγεθος των ομάδων, γιατί το μέγεθος των συντελεστών, για δοθέν/δεδομένο δίκτυο, παραμένει πάντα σταθερό (Ho et al., 2006). Για παράδειγμα συνδυάζονται $N = 50$ πακέτα, μεγέθους 1.400 byte το καθένα, σε ένα πεπερασμένο πεδίο F_{256}, δηλαδή το κάθε πακέτο αποτελείται από $L = 1.400$ σύμβολα των 8 bit, τότε σε κάθε κωδικοποιημένο πακέτο πρέπει να ενσωματωθούν 50 συντελεστές μεγέθους 8 bit και η επιβάρυνση είναι $^{50 \cdot 8}/_{1.400 \cdot 8} = 0{,}0357$ δηλαδή περίπου 3,5% (Chou & Wu, 2007).

Με τη λήψη των πακέτων x_1 και x_2 ή γενικά ενός ικανού πλήθους κωδικοποιημένων πακέτων, πρέπει να αντιστραφεί ο πίνακας C με τη μέθοδο απαλοιφής Gauss-Jordan και να εφαρμοστούν οι γραμμικές σχέσεις στα παραληφθέντα πακέτα για την ανάκτηση των αρχικών πακέτων $\boldsymbol{p_1}$ και $\boldsymbol{p_2}$. Σε μορφή πινάκων η διαδικασία αποκωδικοποίησης είναι:

$$\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1L} \\ p_{21} & p_{22} & \cdots & p_{2L} \end{bmatrix} = C^{-1} \cdot \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1L} \\ x_{21} & x_{22} & \cdots & x_{2L} \end{bmatrix}$$

ή

$$B = C^{-1} \cdot X$$

Γενικά αν ο παραλήπτης έχει λάβει M γραμμικές εξισώσεις με N αγνώστους, πρέπει $M \geq N$ από τις οποίες τουλάχιστον οι N να είναι γραμμικά ανεξάρτητες.

Η σωστή επιλογή των συντελεστών κωδικοποίησης έχει σημαντικό ρόλο, ώστε να παραχθούν όσο το δυνατότερο περισσότερες γραμμικά ανεξάρτητες σχέσεις. Στο RLNC αυτή η επιλογή γίνεται από κάθε κόμβο *τυχαία* και τελείως ανεξάρτητα από τους υπόλοιπους. Η σπουδαιότητα και τα οφέλη αυτής της τεχνικής καταδεικνύονται στο παρακάτω θεώρημα (Ho et al., 2003):

Θεώρημα: Για ένα εφικτό πρόβλημα πολυεκπομπής με ανεξάρτητες ή γραμμικά συσχετισμένες πηγές, και μια κωδικοποίηση δικτύου όπου όλοι ή μερικοί συντελεστές επιλέγονται ανεξάρτητα και ομοιόμορφα πάνω σε όλα τα στοιχεία ενός πεπερασμένου

πεδίου F_q ($q = 2^s$) (μερικοί συντελεστές μπορεί να έχουν σταθερές τιμές, αρκεί να διατηρείται η εφικτότητα του δικτύου), η πιθανότητα όλοι οι δέκτες να μπορούν να αποκωδικοποιήσουν τα αρχική πληροφορία είναι τουλάχιστον $(1 - d/q)^v$ με $q > d$, όπου d είναι ο αριθμός των δεκτών και v είναι ο μέγιστος αριθμός των συνδέσμων (ενδιάμεσων κόμβων) που λαμβάνουν σήματα με ανεξάρτητους τυχαίους συντελεστές σε κάθε ομάδα συνδέσμων που καθιστούν μια λύση ροής από όλες τις πηγές σε οποιονδήποτε δέκτη.

Το RLNC διασφαλίζει σε μεγάλο βαθμό την γραμμική ανεξαρτησία των παραγόμενων σχέσεων. Για παράδειγμα αν σε μια ροή μονο-εκπομπής μέσα από τρεις κόμβους σε ένα ασύρματο δίκτυο, επιλεγεί το πεπερασμένο πεδίο F_{2^s} με s=8 bit, δηλαδή q=256, η πιθανότητα ο δέκτης να μπορέσει να αποκωδικοποιήσει τα πακέτα είναι $(1 - 1/256)^1 = 0{,}996$, που είναι πολύ μεγάλη πιθανότητα (Vu, 2014). Έτσι γίνεται και πρακτικά εφαρμόσιμο, καθώς ο κάθε κόμβος μπορεί να επιλέγει με αυτό τον τρόπο, κατανεμημένα και ανεξάρτητα, τους συντελεστές κωδικοποίησης χωρίς να χρειάζεται να γνωρίζει την τοπολογία του δικτύου ή το πώς λειτουργούν οι υπόλοιποι κόμβοι.

2.4.1. Γενιές

Στην πρακτική εφαρμογή του RLNC τα πακέτα ομαδοποιούνται σε πολλές διαδοχικές δεσμίδες με το ίδιο προκαθορισμένο μέγεθος, οι οποίες ονομάζονται γενιές (generations) (Segovia, 2012). Το μέγεθος της γενιάς g και το πως παράγονται οι γενιές έχει καθοριστική σημασία για την απόδοση της κωδικοποίησης δικτύου.

Οι γενιές βοηθούν στην μείωση της πολυπλοκότητας της διαδικασίας αποκωδικοποίησης, καθώς οι υπολογισμοί σε έναν πίνακα αποκωδικοποίησης σταθερού μεγέθους είναι αρκετά απλοί. Τα δεδομένα αποκωδικοποιούνται αφού πρώτα *ολόκληρη* η γενιά έχει παραληφθεί επαρκώς, προσθέτοντας έτσι μια καθυστέρηση αποκωδικοποίησης. Επιπλέον όλα τα κωδικοποιημένα πακέτα μιας γενιάς πρέπει να αποκωδικοποιηθούν επιτυχώς, πριν αρχίσει να αποστέλλεται η επόμενη γενιά. Αν μια γενιά απορριφθεί (για παράδειγμα, δεν ελήφθησαν αρκετά νέα πακέτα), ο κόμβος αποστολής της γενιάς πρέπει να ξαναστείλει τη συγκεκριμένη γενιά, οδηγώντας σε περαιτέρω αύξηση της καθυστέρησης.

Με την εισαγωγή της έννοιας της γενιάς, η αλγεβρική μορφή της εξίσωσης γραμμικού συνδυασμού των πακέτων γράφεται ως

$$x_i = \sum_{j=1}^{g} c_{ij} p_{(l-1)\times g+j}$$

όπου l είναι ο αριθμός της γενιάς ($l > 0$).

Ο αριθμός της γενιάς που ανήκει το πακέτο προστίθεται στην επικεφαλίδα του πακέτου. Συνήθως, ένα μόνο byte είναι αρκετό για αυτό το σκοπό, εισάγοντας αμελητέα επιβάρυνση.

2.4.2. Είδη Τυχαίας Γραμμικής Κωδικοποίησης Δικτύου

Μπορούν εδώ να αναφερθούν δύο συγκεκριμένα είδη RLNC:

- *Pipeline Coding*: εδώ τα πακέτα κωδικοποιούνται και αποκωδικοποιούνται σταδιακά, αντί να περιμένει ο κόμβος να συγκεντρώσει όλη τη γενιά. Έτσι αν έχουν παραληφθεί όλα τα πακέτα μέχρι και αυτό με δείκτη k, μπορεί να παραχθεί ένα κωδικοποιημένο πακέτο με συνδυασμό των πακέτων από 1 έως k:

$$x_i = \sum_{j=1}^{k} c_{ij} p_{(l-1)\times N+j}$$

- *Transmission Control Protocol with Network Coding (TCP/NC)*: σε ένα περιβάλλον με απώλειες, όπως τα ασύρματα δίκτυα, οι τυχαίες απώλειες εκλαμβάνονται από το πρωτόκολλο TCP ως συμφόρηση στο δίκτυο (network congestion), με αποτέλεσμα τη μείωση του ρυθμού αποστολής, οδηγώντας στη μείωση της απόδοσης του δικτύου. Το TCP/NC έχει προταθεί για την επίλυση αυτού το προβλήματος, με στόχο την ενσωμάτωση της κωδικοποίησης δικτύου στο επίπεδο των πρωτοκόλλων TCP και IP, ως ένα επίπεδο κωδικοποίησης ανάμεσα στο επίπεδο μεταφοράς (TCP) και το επίπεδο δικτύου (IP) (Sundararajan et al., 2011).

  Το TCP/NC αλλάζει μόνο το μηχανισμό παραγωγής πακέτων και επιβεβαίωσης. Όποτε το πρωτόκολλο TCP θέλει να στείλει ένα πακέτο, το TCP/NC παράγει και μεταδίδει τουλάχιστον ένα κωδικοποιημένο πακέτο, το οποίο συνδυάζει αυτό το

πακέτο με άλλα πακέτα που δεν έχουν επιβεβαιωθεί ακόμα, ώστε να αντιμετωπίσει το πρόβλημα των τυχαίων απωλειών. Στο TCP/NC μόνο η πηγή κωδικοποιεί, δηλαδή αν υπάρχουν ενδιάμεσοι κόμβοι το μόνο που κάνουν είναι να προωθούν τα πακέτα. Ο παραλήπτης με τη σειρά του επιβεβαιώνει κάθε βαθμό ελευθερίας, δηλαδή γραμμικούς συνδυασμούς που συνεισφέρουν ένα νέο κομμάτι πληροφορίας, αν και ακόμα μπορεί να μην έχει ανακτηθεί κανένα αρχικό πακέτο. Με αυτό το τρόπο ουσιαστικά οι απώλειες κρύβονται από το επίπεδο λειτουργίας του πρωτοκόλλου TCP.

2.4.3. Διαδικασία Κωδικοποίησης και Αποκωδικοποίησης

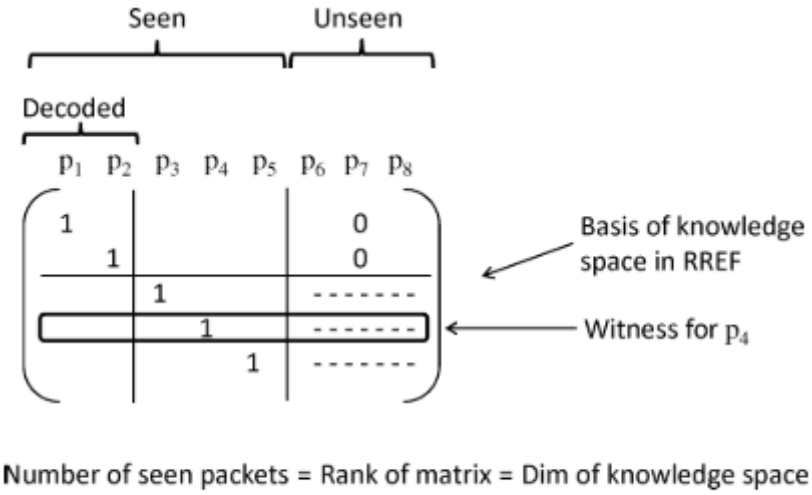
Για την καλύτερη κατανόηση της διαδικασίας κωδικοποίησης και αποκωδικοποίησης είναι απαραίτητη η εισαγωγή κάποιων νέων ορισμών:

Ορισμός 1 [«έχει δει ένα πακέτο»]: ένας κόμβος λέγεται ότι έχει δει ένα πακέτο p_n αν έχει αρκετή πληροφορία για να υπολογίσει ένα γραμμικό συνδυασμό της μορφής $p_n + y$ όπου y είναι ένας γραμμικός συνδυασμός που περιλαμβάνει πακέτα με δείκτες μεγαλύτερους του n. Η έννοια του «*έχει δει*» ένα πακέτο είναι η φυσική επέκταση της έννοιας της «*αποκωδικοποίησης*». Για παράδειγμα αν ένα πακέτο p_n έχει αποκωδικοποιηθεί, τότε το «*έχει δει*» επίσης με y=0.

Ορισμός 2 [«γνώση ενός κόμβου»]: Η γνώση ενός κόμβου είναι το σύνολο των γραμμικών συνδυασμών των αρχικών πακέτων που μπορεί να υπολογίσει, με βάση την πληροφορία που έχει λάβει μέχρι μια δεδομένη χρονική στιγμή.

Πρόταση 1: αν ένας κόμβος «*έχει δει*» ένα πακέτο p_n, τότε γνωρίζει ακριβώς έναν γραμμικό συνδυασμό της μορφής $p_n + y$, όπου y είναι γραμμικός συνδυασμός που περιλαμβάνει πακέτα που «*δεν έχει δει*».

Ορισμός 3 (*«μάρτυρας»*): Ο παραπάνω γραμμικός συνδυασμός ονομάζεται *μάρτυρας* ότι «*έχει δει*» το p_n.



Σχήμα 6 Τα πακέτα όπως τα έχει δει ο κόμβος (Sundararajan et al., 2011)

Ο αριθμός των πακέτων που «*έχει δει*» είναι ίσος με την τάξη του πίνακα και ίσος με τον αριθμό των βαθμών ελευθερίας που έχουν παραληφθεί μέχρι τη δεδομένη χρονική στιγμή. Ένα κωδικοποιημένο πακέτο που αυξάνει αυτή τη διάσταση, δηλαδή παρέχει πληροφορία, ονομάζεται *καινοτόμο*.

Παράδειγμα: έστω ότι ένας κόμβος γνωρίζει τους παρακάτω γραμμικούς συνδυασμούς

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

Αφού οι παραπάνω σχέσεις είναι γραμμικά ανεξάρτητες περιμένουμε ο βαθμός να είναι 2, άρα και ο αριθμός των πακέτων που «*έχει δει*» να είναι 2. Όντως η πρώτη σχέση $x_1 = p_1 + p_2$ ικανοποιεί τον ορισμό 1 και ο κόμβος «έχει δει» το πακέτο p_2. Αν αφαιρέσουμε τις 2 σχέσεις μεταξύ τους, τότε $z = x_1 - x_2 = p_2 - p_3$, οπότε και το p_2 «έχει δει» αφού ικανοποιεί τον ορισμό. Η σχέση x_2 είναι ο μάρτυρας του p_1 και η σχέση z ο μάρτυρας του p_2.

Η διαδικασία έχει ως εξής:

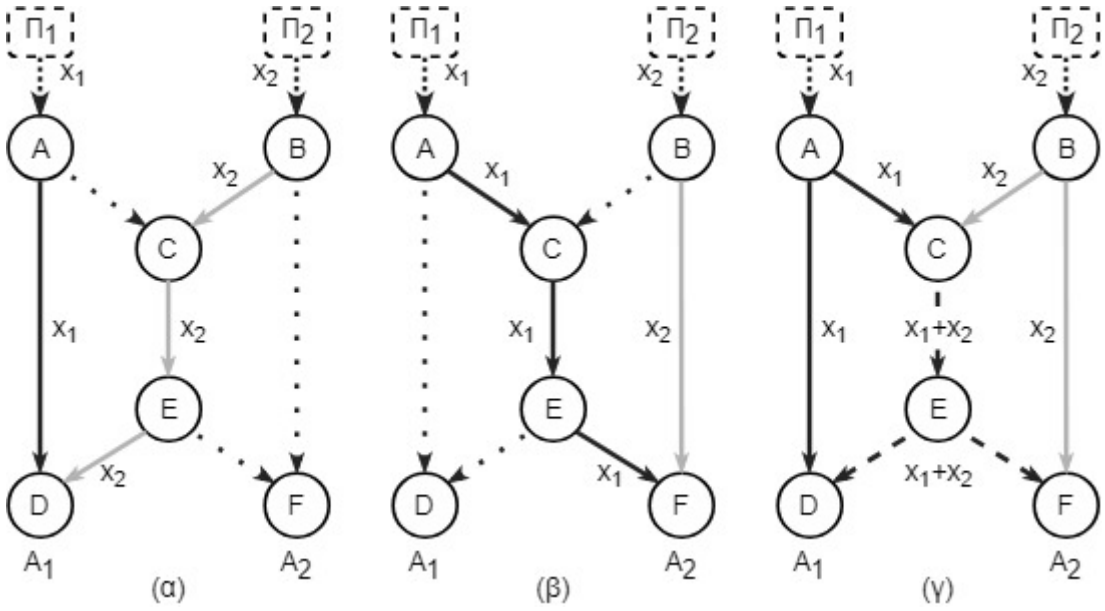
- Τα διανύσματα κωδικοποίησης και πληροφορίας που λαμβάνονται με τα πακέτα, αποθηκεύονται σε έναν πίνακα, τον πίνακα αποκωδικοποίησης
- Κάθε κωδικοποιημένο πακέτο που λαμβάνεται προστίθεται στην τελευταία γραμμή του πίνακα

- Κάθε μη καινοτόμο πακέτο καταγράφεται ως σειρά από μηδενικά με την απαλοιφή Gauss και αγνοείται.

2.5. Σενάρια Χρήσης

2.5.1. Δίκτυο Πεταλούδας

Το πιο χαρακτηριστικό παράδειγμα για την κατανόηση της κωδικοποίησης δικτύου είναι αυτό που ονομάζεται δίκτυο πεταλούδας (Butterfly Network), όπως φαίνεται παρακάτω. Ας υποθέσουμε ότι έχουμε δύο πηγές (πομπούς) Π_1, Π_2 και δύο παραλήπτες (δέκτες) A_1 και A_2 και ότι η επικοινωνία γίνεται σε συγκεκριμένα χρονικά διαστήματα. Κάθε πηγή παράγει ένα bit σε κάθε χρονοθυρίδα (μονάδα χρόνου), το οποίο συμβολίζεται ως x_1 και x_2 αντίστοιχα (Fragouli & Soljanin, 2006).



Σχήμα 7 Δίκτυο πεταλούδας (Fragouli & Soljanin, 2006)

Αν ο δέκτης A_1 χρησιμοποιούσε αποκλειστικά όλους τους πόρους του δικτύου, τότε θα μπορούσε να λάβει και τα δύο μηνύματα. Όντως, θα μπορούσαμε να δρομολογήσουμε το bit x_1 από την πηγή Π_1 στη διαδρομή {AD} και το bit x_2 από την πηγή Π_2 μέσω της διαδρομής {BC, CE, ED} όπως φαίνεται στο Σχήμα 7(α). Ομοίως, αν ο δέκτης A_2 χρησιμοποιούσε αποκλειστικά όλους τους πόρους του δικτύου, θα μπορούσε και αυτός να λάβει και τα δύο μηνύματα, με τη δρομολόγηση του bit x_1 από την πηγή A_1 μέσω της

διαδρομής {AC, CE, EF} και το bit x_2 από την πηγή Π_2 μέσω της διαδρομής {BF}, όπως φαίνεται στο Σχήμα 7(β).

Αν όμως θεωρήσουμε ότι και οι δύο δέκτες θέλουν να λάβουν ταυτόχρονα τα μηνύματα και από τις δύο πηγές (πολύ-εκπομπή), τότε παρουσιάζεται σύγκρουση στη χρήση της σύνδεσης CE, καθώς κάθε σύνδεση μπορεί να στείλει ένα μόνο bit ανά μονάδα χρόνου. Το επιθυμητό θα ήταν να μπορέσουμε να στείλουμε και τα δύο bit x_1 και x_2 ταυτόχρονα και στους δύο δέκτες.

Χρησιμοποιώντας τη κωδικοποίηση δικτύου και επιτρέποντας τους ενδιάμεσους κόμβους όχι μόνο να προωθούν τις εισερχόμενες ροές πληροφορίας, αλλά να μπορούν να τις επεξεργάζονται, θα μπορούσε ο κόμβος C να πάρει το άθροισμα XOR (πρόσθεση στο δυαδικό χώρο) των bit x_1 και x_2 και να δημιουργήσει ένα τρίτο bit $x_3 = x_1 \oplus x_2$ και να το στείλει μέσω της σύνδεσης CE. Έτσι ο A_1 θα λάμβανε τα $\{x_1, x_1 \oplus x_2\}$ και θα μπορούσε να λύσει αυτό το σύστημα δύο εξισώσεων και να υπολογίσει τα x_1 και x_2. Αντίστοιχα ο A_2 θα λάμβανε το $\{x_2, x_1 \oplus x_2\}$ και θα μπορούσε να λύσει τις εξισώσεις ως προς x_1 και x_2.

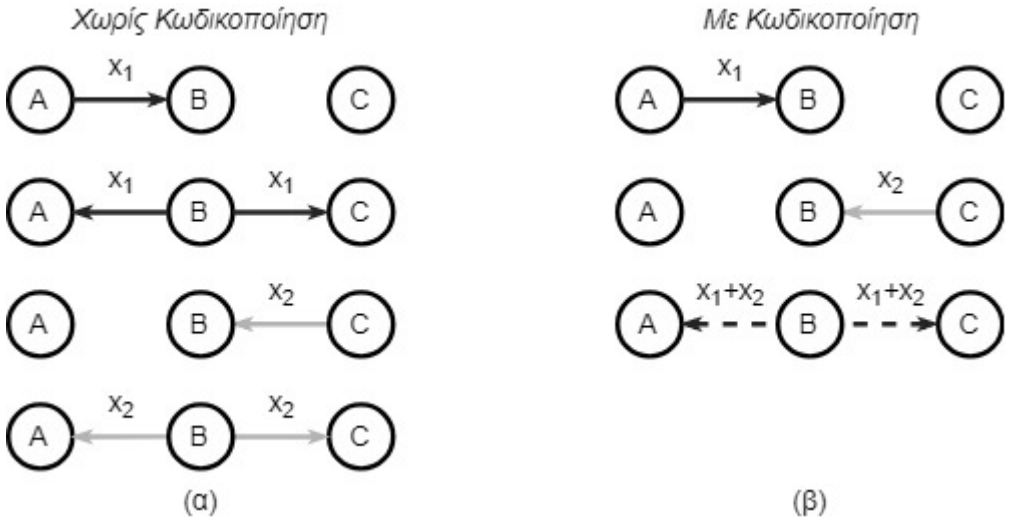
Στο παραπάνω παράδειγμα χρησιμοποιείται το άθροισμα XOR. Ωστόσο, η πράξη κωδικοποίησης θα μπορούσε να είναι πολύ πιο γενική. Για παράδειγμα θα μπορούσαν ομάδες από bit να θεωρηθούν ως στοιχεία ενός πεπερασμένου πεδίου και ένα πακέτο ως ένα διάνυσμα πάνω σε αυτό το πεδίο. Η κωδικοποίηση, τότε, θα μπορούσε να εκτελεί γραμμικούς συνδυασμούς σε αυτά τα διανύσματα, με συντελεστές επιλεγμένους από το ίδιο πεδίο. Για να μπορέσει ο κάθε δέκτης να αποκωδικοποιήσει την πληροφορία, θα πρέπει να τόσους γραμμικούς συνδυασμούς, όσα τα πακέτα που έχουν συνδυαστεί και τότε να λύσει το σύστημα εξισώσεων με την απαλοιφή Gauss-Jordan.

2.5.2. Κωδικοποίηση Δικτύου σε Ασύρματο Δίκτυο

Το Σχήμα 8 περιγράφει ένα ασύρματο δίκτυο όπου οι κόμβοι A και C θέλουν να ανταλλάξουν τα αρχεία τους μέσω του ενδιάμεσου κόμβου B (αναμεταδότης), εξαιτίας της μικρής εμβέλειας του ασύρματου δικτύου. Ακολουθώντας τη συνήθη τεχνική μετάδοσης, χρειάζονται τέσσερις μονάδες χρόνου (χρονοθυρίδες) για την ολοκλήρωση της ανταλλαγής, όπως φαίνεται στο Σχήμα 8(α), όπου ο A εκπέμπει το bit x_1 και στη

συνέχεια ο Β το εκπέμπει (πολυεκπομπή) και στους δύο. Μετά ακολουθεί την ίδια ακριβώς διαδικασία ο C για το bit x_2.

Με τη χρήση της κωδικοποίησης δικτύου, ο κόμβος Β, αφού λάβει τα δύο bit x_1 και x_2, μπορεί να δημιουργήσει το bit $x_3 = x_1 \oplus x_2$ και εκπέμψει αυτό μόνο μια φορά. Έτσι ο κόμβος Α, ο οποίος έχει ήδη το bit x_1, λαμβάνοντας το x_3 μπορεί να υπολογίσει το x_2. Αντίστοιχα ο κόμβος C έχοντας ήδη το bit x_2, λαμβάνοντας το x_3 μπορεί να υπολογίσει το x_1.



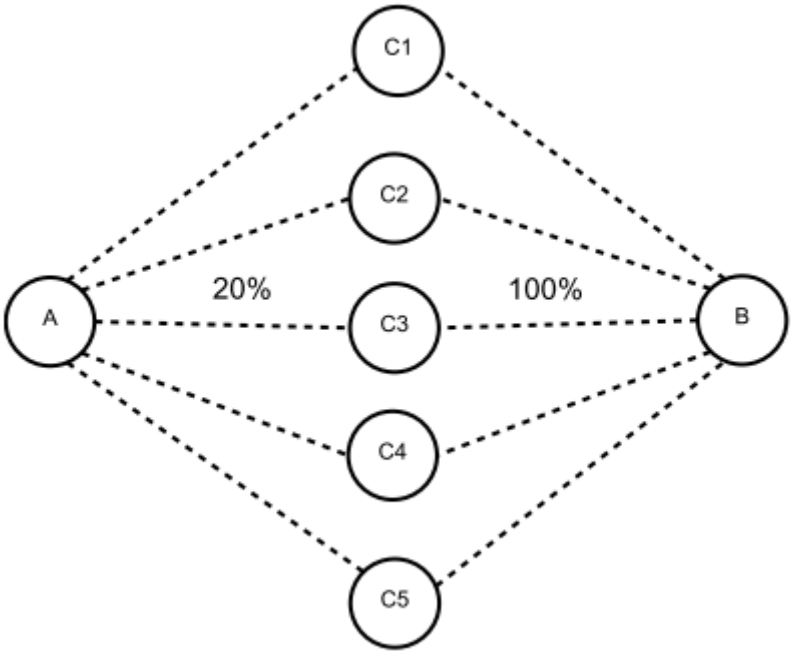
Σχήμα 8 Επικοινωνία σε ασύρματο δίκτυο (Fragouli & Soljanin, 2006)

2.5.3. Δρομολόγηση πλημμυρίδας

Η παραδοσιακή δρομολόγηση επιλέγει τον επόμενο κόμβο για κάθε πακέτο πριν από κάθε μετάδοση. Αν όμως οι σύνδεσμοι έχουν απώλειες, η πιθανότητα μετάδοσης είναι μικρή, με αποτέλεσμα την μείωση της απόδοσης του δικτύου.

Στην δρομολόγηση πλημμυρίδα (flood routing) κάθε κόμβος που λαμβάνει ένα πακέτο μπορεί να συμμετάσχει στην προώθησή του. Για παράδειγμα στο δίκτυο που φαίνεται στο Σχήμα 9, υπάρχουν πέντε ενδιάμεσοι κόμβοι που μπορούν να προωθούν πακέτα. Η πιθανότητα λήψης ενός πακέτου από τον A σε οποιονδήποτε C_i είναι 20%, ενώ από κάθε C_i σε B είναι 100%. Με την παραδοσιακή δρομολόγηση θα φτάνει ένα στα πέντε πακέτα από τον A στον B, ανεξάρτητα από τον ενδιάμεσο κόμβο C_i που επιλέγεται κάθε φορά. Αν όμως χρησιμοποιηθεί η δρομολόγηση πλημμυρίδας, τότε η πιθανότητα επιτυχίας είναι μεγαλύτερη του 67%. Η συγκεκριμένη τεχνική δρομολόγησης μειώνει

την πολυπλοκότητα στην επιλογή μονοπατιού δρομολόγησης αλλά και την ανάγκη συντονισμού των ενεργειών των ενδιάμεσων κόμβων για την προώθηση του πακέτου στον τελικό προορισμό. Αποτελεί δε, με κατάλληλες προσαρμογές, μία ιδανική λύση για τη δρομολόγηση σε έντονα ευκαιριακά δίκτυα, τα οποία έχουν διαρκώς μεταβαλλόμενη τοπολογία, όπως για παράδειγμα επικοινωνία μέσω οχημάτων στις πόλεις ή δίκτυα παρατήρησης άγριας ζωής.



Σχήμα 9 Δρομολόγηση πλημμυρίδας (Vu, 2014, p. 35)

2.6. Πρακτικές Εφαρμογές και Παραδείγματα

Το (Angelopoulos et al., 2017) παρουσιάζει το πρώτο προσαρμοσμένο πολύ-μεγάλης-κλίμακας-ολοκληρωμένο (VLSI) με ενσωματωμένο πομπό 2.4 GHz, ειδικά για τη χρήση σε συσκευές IoT, αναγνωρίζοντας ότι το RLNC είναι μια ανερχόμενη τεχνολογία που μπορεί να παρέχει πολλά πλεονεκτήματα ιδιαιτέρως σε ασύρματα δίκτυα, όπως ρυθμαπόδοση, ευρωστία, καλύτερη εκμετάλλευση των πόρων του δικτύου. Τα δίκτυα οχημάτων (vehicular networks) είναι μία άλλη εφαρμογή της κωδικοποίησης δικτύου για τη βελτίωση της διαθεσιμότητας δεδομένων (Feng et al., 2012).

Τα συστήματα αποθήκευσης (storage systems) είναι ένας τομέας όπου το RLNC μπορεί να προσφέρει σημαντικά πλεονεκτήματα. Ακόμα και σε άστατα (unstable), από άποψη συνδεσιμότητας συστήματα, το RLNC επιτρέπει την αποκωδικοποίηση των δεδομένων

ακόμα και μετά από αρκετές αποτυχίες και επιδιορθώσεις (Abdrashitov & Medard, 2016). Σε ένα μεγάλης κλίμακας κατανεμημένο σύστημα αποθήκευσης δεδομένων με πολλούς ανεξάρτητους κόμβους, η περίσσεια είναι απαραίτητη για την διασφάλιση της διαθεσιμότητας και ανθεκτικότητας των δεδομένων. Πολλά συστήματα στην πράξη δημιουργούν περίσσεια με την αντιγραφή δεδομένων, όπου πολλαπλά αντίγραφα για κάθε μπλοκ δεδομένων αποθηκεύονται σε διάφορους κόμβους. Όμως αυτή η αντιγραφή δημιουργεί επιπλέον φόρτο μετάδοσης και αυξάνει σημαντικά το συνολικό κόστος ανάκτησης. Η κωδικοποίηση εξάλειψης (Erasure Coding) είναι ένας εναλλακτικός τρόπος παροχής περίσσειας με μικρότερο φόρτο (Weatherspoon & Kubiatowicz, 2002). Οι παραδοσιακές τεχνικές εξάλειψης δεν είναι όμως κατάλληλες για μεγάλης κλίμακας συστήματα. Σε ένα ιδιαίτερα ευμετάβλητο περιβάλλον, το RLNC μπορεί να λειτουργήσει αρκετά καλά και επιτρέπει την αποκωδικοποίηση της πληροφορίες ακόμα και μετά από μεγάλο αριθμό αποτυχημένων επικοινωνιών (Abdrashitov & Medard, 2016).

Κεφάλαιο 3
Θεωρητική Μελέτη

3.1. Ερευνητικό Ερώτημα

Το RLNC παρουσιάζεται ως μια καλή μέθοδος, με πολλά πλεονεκτήματα, για ένα δίκτυο. Το ερώτημα λοιπόν που γεννάται είναι αν μπορεί να αποτελέσει ικανοποιητική επιλογή για την προστασία της διαθεσιμότητας, ως πλευρά της ασφάλειας.

Η διαθεσιμότητα κινδυνεύει από πολλά είδη καταστροφών. Μία τέτοια κατηγορία είναι οι ακούσιες καταστροφές, όπως τα φυσικά φαινόμενα, οι διακοπές ρεύματος ή τα μικρά ενεργειακά αποθέματα, στα οποία είναι ιδιαίτερα επιρρεπή τα ασύρματα δίκτυα. Για αυτό έχει αρχίσει να δίνεται ιδιαίτερη βαρύτητα στην ανθεκτικότητά τους σε τέτοιου είδους καταστροφές (Tornatore et al., 2016). Ακόμα, όμως, και στα ενσύρματα δίκτυα αναπτύσσονται τεχνικές βελτίωσης της ανθεκτικότητας. Στο (Chen et al., 2015) μελετάται πως τα Δίκτυα Ανθεκτικά σε Καθυστέρηση (Delay Tolerant Networking, DTN) συνδυάζονται με τεχνικές κωδικοποίησης δικτύου και πώς μπορούν να ωφεληθούν από τα πλεονεκτήματα τους.

Μία άλλη κατηγορία καταστροφών είναι οι εκούσιες, όπως οι επιθέσεις από ανθρώπινα μέσα με σκοπό την μη εξουσιοδοτημένη απόκτηση πρόσβασης ή την διακοπή παροχής μιας υπηρεσίας (Furdek et al., 2016) και η ανθεκτικότητα θα πρέπει να λαμβάνει υπόψη της και αυτές τις δραστηριότητες που επίσης μπορεί να αποτρέπουν τις επικοινωνίες ή να υποβιβάζουν την ποιότητα μιας υπηρεσίας. Τέτοιου είδους απειλές είναι για παράδειγμα ο ηλεκτρομαγνητικός παλμός, επιθέσεις σε οπτικές είναι (κόψιμο ή λύγισμα) ή παρεμβολές με την εισαγωγή επιβλαβών σημάτων σε συνδέσμους οπτικών ινών.

Για το σκοπό αυτό, στη συγκεκριμένη μεταπτυχιακή διατριβή, μελετώνται τα χαρακτηριστικά του RLNC και αυτά πώς μπορούν να χρησιμοποιηθούν, σε επίπεδο

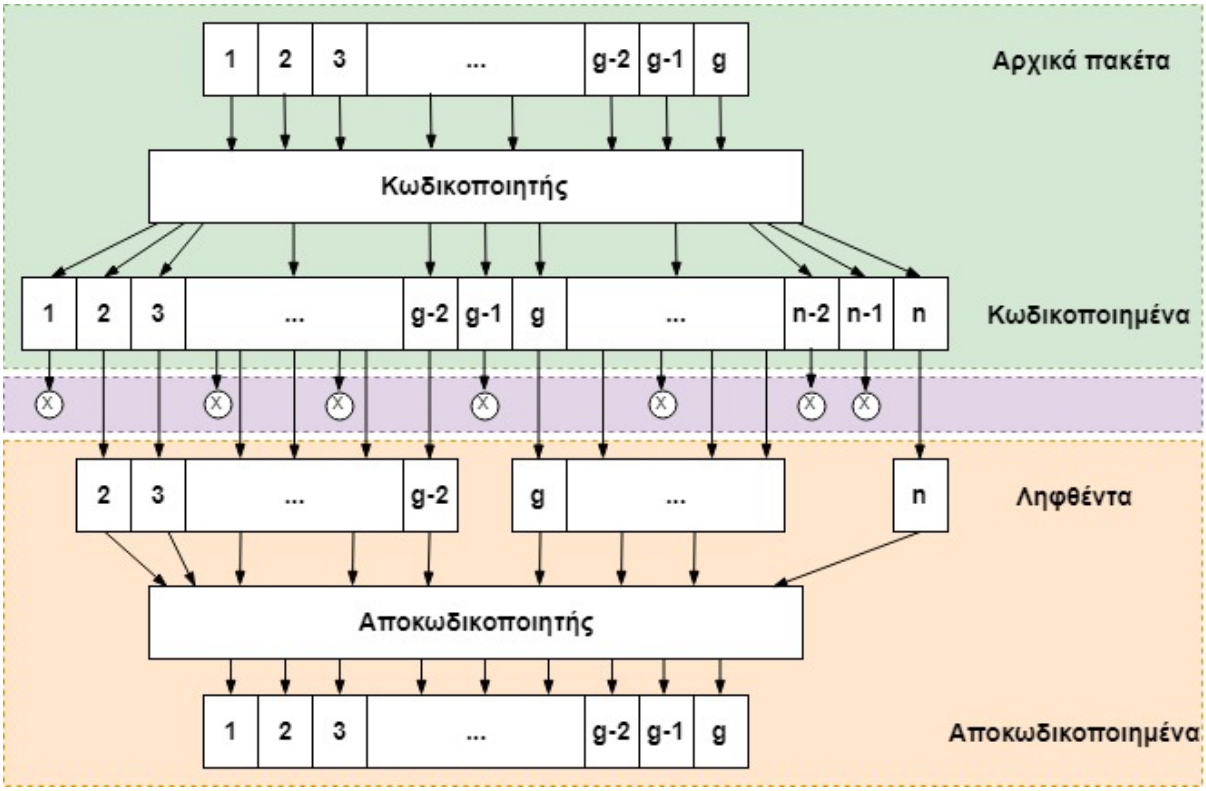
δικτύου, για να βοηθήσουν στην προστασία της διαθεσιμότητας σε διάφορα σενάρια επιθέσεων, σε ενσύρματα ή ασύρματα δίκτυα.

3.2. Πλεονεκτήματα RLNC

Η τυχαία γραμμική κωδικοποίηση δικτύου παρουσιάζει ορισμένα σημαντικά χαρακτηριστικά για βελτίωση της ανθεκτικότητας ενός δικτύου και την παροχή του πλεονεκτήματος, που θα οδηγήσει στα επιθυμητά χαρακτηριστικά ασφάλειας δικτύου, όπως αξιοπιστία, ευρωστία, αύξηση της ρυθμαπόδοσης και ενεργειακή αποδοτικότητα. Αναλύουμε στις επόμενες ενότητες τα χαρακτηριστικά αυτά υπό το πρίσμα της διαθεσιμότητας.

3.2.1. Προσθήκη Περίσσειας

Για την αντιμετώπιση απωλειών, η κωδικοποίηση δικτύου, εισάγει περίσσεια στα πακέτα μιας γενιάς με αποτέλεσμα να αυξάνεται η αξιοπιστία και η ανθεκτικότητα της επικοινωνίας είτε πρόκειται για μονές είτε για πολλαπλές συνδέσεις (Bhatia, Patel & Narmawala, 2011), (Lun, Medard & Koetter, 2006). Έτσι αν για παράδειγμα μια γενιά αποτελείται από g πακέτα, τότε παράγονται και αποστέλλονται από τον κωδικοποιητή $n > g$ κωδικοποιημένα πακέτα, όπως φαίνεται στο Σχήμα 10.



Σχήμα 10 Εισαγωγή περίσσειας σε δίκτυο με απώλειες
(Pedersen, Heide & Fitzek, 2011)

Αν λοιπόν στο κανάλι επικοινωνίας υπάρξουν απώλειες, αρκεί να φτάσουν g σε αριθμό γραμμικά ανεξάρτητα κωδικοποιημένα πακέτα στον παραλήπτη για να μπορέσει να αποκωδικοποιήσει τα αρχικά πακέτα. Η τυχαία επιλογή των συντελεστών κωδικοποίησης αυξάνει αρκετά την πιθανότητα τα παραγόμενα πακέτα να είναι γραμμικά ανεξάρτητα (Ostovari & Wu, 2016), αλλά ακόμα και αν παραχθούν και μη ανεξάρτητα, η εισαγωγή περίσσειας, με την παραγωγή $n > g$ κωδικοποιημένων πακέτων, εξασφαλίζει μεγάλο πλήθος γραμμικά ανεξάρτητων.

3.2.2. Ανεξαρτησία Κόμβων

Ένα ιδιαίτερο χαρακτηριστικό του RLNC είναι ότι κάθε ενδιάμεσος κόμβος επιλέγει τους συντελεστές του, και κατά συνέπεια την κωδικοποίηση του, τυχαία και ανεξάρτητα από τους υπόλοιπους. Οποιαδήποτε θέματα σταθερότητας, όπως αυτά που προκύπτουν από διάδοση (propagation) της πληροφορίας δρομολόγησης, εξαλείφονται με τη χρήση του RNLC (Bhatia, Patel & Narmawala, 2011). Για το λόγο αυτό το RLNC είναι ιδανικό για δυναμικά και κατανεμημένα περιβάλλοντα με δυναμικά μεταβαλλόμενη τοπολογία, όπου οι παραδοσιακοί αιτιοκρατικοί (ντεντερμινιστικοί)

αλγόριθμοι κωδικοποίησης (Deterministic Network Coding) δεν είναι εφαρμόσιμοι καθώς απαιτούν ένα κεντρικοποιημένο (centralized) σχεδιασμό, βασισμένο στην τοπολογία ολόκληρου του (Segovia, 2012).

Η ανεξάρτητη επανα-κωδικοποίηση στους ενδιάμεσους κόμβους του RLNC μπορεί να πραγματοποιείται χωρίς να χρειάζεται να γίνει αποκωδικοποίηση των αρχικών πακέτων (Sundararajan et al., 2011). Ο τελικός παραλήπτης κατά συνέπεια, ανεξάρτητα από το πλήθος των κωδικοποιήσεων που έχουν πραγματοποιηθεί στο δίκτυο από τους ενδιάμεσους κόμβους, χρειάζεται να κάνει μία μόνο αποκωδικοποίηση (Cloud & Medard, 2015).

Η ανεξαρτησία των κόμβων και η δυνατότητα προσαρμογής σε μεταβολές, αυξάνει την ανθεκτικότητα σε επιθέσεις, καθώς δεν υπάρχει ένα μοναδικό (αδύναμο) σημείο στόχευσης της επίθεσης.

3.2.3. Ταυτόχρονα μονοπάτια

Με την κωδικοποίηση δικτύου τα κωδικοποιημένα πακέτα, ίδια ή διαφορετικά, μπορούν να μεταφέρονται *ταυτόχρονα* από διαφορετικές διαδρομές, παρέχοντας ακόμα μεγαλύτερη ευρωστία στην επικοινωνία. Σε περίπτωση επίθεσης, όπου μεμονωμένα κανάλια επικοινωνίας καταστρέφονται ή υπολειτουργούν, μπορούν οι μεταφορές των κωδικοποιημένων πακέτων από εναλλακτικές και παράλληλες διαδρομές να είναι αρκετές για την επιτυχή αποκωδικοποίηση και ολοκλήρωση της επικοινωνίας.

Επιπλέον, η διάσπαση της πληροφορίας σε τμήματα που ταξιδεύουν από διαφορετικά μονοπάτια δυσκολεύει τις όποιες προσπάθειες υποκλοπής, τόσο για τη συλλογή των δεδομένων για την ανακατασκευή των αρχικών πακέτων, όσο και για τον εντοπισμό των κατάλληλων παραμέτρων ανά κανάλι. Προς αυτή την κατεύθυνση, για παράδειγμα, έχει γίνει ανάπτυξη αλγεβρικών κριτηρίων ασφαλείας για την διερεύνηση των εγγενών χαρακτηριστικών ασφάλειας που διαθέτει το RLNC (Lima, Medard & Barros, 2007) και έχει παραχθεί ένα κρυπτογραφικό σχήμα χαμηλής πολυπλοκότητας για την προστασία των συντελεστών κωδικοποίησης (Vilela, Lima & Barros, 2008).

3.2.4. Αύξηση Ρυθμαπόδοσης

Η κωδικοποίηση δικτύου και ιδίως το χαρακτηριστικό της να επιτρέπει στους ενδιάμεσους κόμβους να επανα-κωδικοποιούν τα πακέτα που έχουν λάβει, παρέχει σημαντικό κέρδος στην ρυθμαπόδοση και σε σύγκριση με την κωδικοποίηση από άκρο-σε-άκρο (Cloud & Medard, 2015). Μάλιστα, ειδικά σε σενάρια πολυεκπομπής, όπου όλες οι συνεδρίες πολυεκπομπής έχουν τον ίδιο αποδέκτη, είναι ικανή να πετύχει το βέλτιστο ρυθμό μετάδοσης ελάχιστης τομής (min-cut rate) (Bhatia, Patel & Narmawala, 2011). Είναι έτσι εφικτό ο κάθε ένας από τους αποδέκτες να λαμβάνει την πληροφορία με τον ίδιο ρυθμό, όπως αν είχε αποκλειστική πρόσβαση στους πόρους του δικτύου (Fragouli & Soljanin, 2006). Όμως και σε ενσύρματα δίκτυα, η κωδικοποίηση δικτύου έχει εφαρμοστεί με στόχο την επίλυση των προβλημάτων στενωπού (bottleneck) και τη μεγιστοποίηση της ρυθμαπόδοσης (Ostovari & Wu, 2016).

3.2.5. Ενεργειακή Απόδοση Δικτύου

Η κωδικοποίηση δικτύου τείνει να μειώνει τον αριθμό των επανεκπομπών, αυξάνοντας έτσι την ενεργειακή αποδοτικότητα του δικτύου (Chou & Wu, 2007). Ειδικά σε περιπτώσεις πολύ-εκπομπών όπου όλοι οι παραλήπτες απαιτούν την επανάληψη αποστολής πακέτων που δεν έχουν λάβει (πολλές φορές ένα-προς-ένα), η χρήση των συνδυασμών των πακέτων (NC) είναι ικανή να καλύψει τις ανάγκες αυτές με σημαντικά μικρότερο αριθμό επαναλήψεων. Κατά συνέπεια, μπορεί να συμβάλει στην αύξηση της διάρκειας ζωής κάθε κόμβου αλλά και του δικτύου συνολικά, ειδικά σε σενάρια επιθέσεων εξάντλησης των ενεργειακών τους πόρων (energy depletion).

3.3. Μειονεκτήματα RLNC

Υπάρχουν ορισμένα μειονεκτήματα και εμπόδια, τα οποία, προς το παρόν, δεν έχουν ξεπεραστεί, κυρίως στην εφαρμογή σε πραγματικές συνθήκες. Αναλύουμε στις επόμενες ενότητες τις προκλήσεις που εντοπίζουμε.

3.3.1. Πολυπλοκότητα

Για την υλοποίηση της κωδικοποίησης δικτύου απαιτείται οι ενδιάμεσοι κόμβοι να έχουν επιπλέον δυνατότητες επεξεργασίας, ώστε να εκτελούν πράξεις στα εισερχόμενα πακέτα πάνω σε ένα πεπερασμένο σύνολο. Μία τέτοια αναβάθμιση μπορεί να είναι ιδιαίτερα δύσκολη σε ήδη υλοποιημένα δίκτυα ή υποδομές. Η προσθήκη της λειτουργικότητας ακόμα και σε νέα, υπό σχεδίαση δίκτυα, μπορεί να έχει ως συνέπεια την αύξηση του κόστους κατασκευής, τόσο χρονικά όσο και χρηματικά.

3.3.2. Παραμετροποίηση

Για την επίτευξη του καλύτερου δυνατού αποτελέσματος, η σωστή επιλογή όλων των παραμέτρων λειτουργίας είναι ουσιώδης. Κάποιο σημαντικό λάθος μπορεί να οδηγήσει σε αποτελέσματα αντίθετα του αναμενόμενου. Για παράδειγμα, η υπερβολική αύξηση του μεγέθους της γενιάς μπορεί να σημαίνει αύξηση της καθυστέρησης, καθώς ο κάθε αποδέκτης θα πρέπει να περιμένει να παραληφθούν όλα τα πακέτα της γενιάς για να ολοκληρώσει την αποκωδικοποίηση (Bhatia, Patel & Narmawala, 2011). Επιπλέον, η επιλογή ενός μικρού μεγέθους πεπερασμένου πεδίου θα οδηγήσει σε πολλές γραμμικά εξαρτημένες σχέσεις, ενώ ενός πολύ μεγάλου, σε αύξηση του κόστους υπολογισμού. Απαιτείται συνεπώς ιδιαίτερη προσοχή στη μελέτη και σχεδίαση, ώστε να επιλεχθεί ο καλύτερος συνδυασμός των παραμέτρων.

3.3.3. Καθυστέρηση

Όλοι οι απαραίτητοι υπολογισμοί για την κάλυψη των απαιτήσεων των λειτουργιών του RLNC (ενδεικτικά: επιπλέον υπολογισμοί ανά πακέτο, μνήμη για την ενταμίευση (buffering) των πακέτων και υλοποίηση απαλοιφής Gauss), αυξάνουν το χρόνο επεξεργασίας σε κάθε κόμβο. Αυτό έχει ως αποτέλεσμα την εισαγωγή χρονικής καθυστέρησης για κάθε πακέτο (packet delay). Αυτό ενδέχεται να λειτουργήσει απαγορευτικά για χρήση σε εφαρμογές πραγματικού χρόνου.

3.3.4. Υιοθέτηση – Ενσωμάτωση

Ένα μεγάλο στοίχημα που θα είναι αρκετά δύσκολο να κερδηθεί θα είναι η ενσωμάτωσή της με τις υπάρχουσες τεχνολογίες που έχουν καθιερωθεί σε πολύ μεγάλο φάσμα συσκευών και χρησιμοποιούνται από όλο τον κόσμο. Όπως κάθε νέα τεχνολογία θα χρειαστεί αρκετός χρόνος για την πρακτική υιοθέτησή της.

Επίσης δεν έχουν επιλυθεί πλήρως θέματα στην υλοποίηση της σε πρακτικά πρωτόκολλα δικτύων. Για παράδειγμα οι τρέχουσες προσεγγίσεις της τεχνικής αυτής δεν είναι ακόμα άμεσα συμβατές με επανεκπομπές σε TCP και τον μηχανισμό του κυλιόμενου παραθύρου. Έτσι υπάρχει η ανάγκη για την προσθήκη ενός ενδιάμεσου επιπέδου, όπως συμβαίνει και με το TCP/NC που εισάγει ένα νέο επίπεδο κωδικοποίησης δικτύου ανάμεσα στο επίπεδο μεταφοράς (transport layer) και το επίπεδο δικτύου στο μοντέλο αναφοράς OSI (Sundararajan et al., 2011).

Πειραματική εφαρμογή της τεχνολογίας έχει γίνει σε δίκτυα σε απομακρυσμένα νησιά του Ειρηνικού Ωκεανού, όπου είναι σύνηθες φαινόμενο η απώλεια πακέτων και η αστάθεια των συνδέσεων (Speidel et al., 2015). Σε τόσο ασταθή δίκτυα το TCP μειώνει το ρυθμό μετάδοσης σε περιπτώσεις απώλειας πακέτων και, σε συνδυασμό με το μεγάλο χρόνο υστέρησης που παρατηρείται σε τέτοια δίκτυα, βγαίνει εκτός συγχρονισμού, οδηγώντας σε ένα φαινόμενο ταλάντωσης με αποτέλεσμα να παρατηρούνται στη δορυφορική σύνδεση μεγάλες περίοδοι που είναι ανενεργή. Με την εφαρμογή του TCP/NC, ο κωδικοποιητής μπορεί να ξεκινήσει να παράγει άμεσα περίσσεια, με το που θα έχει στη διάθεση του τουλάχιστον δύο αρχικά πακέτα, βελτιώνοντας κατά πολύ την συνολική ρυθμαπόδοση σε πολύ δύσκολες συνθήκες.

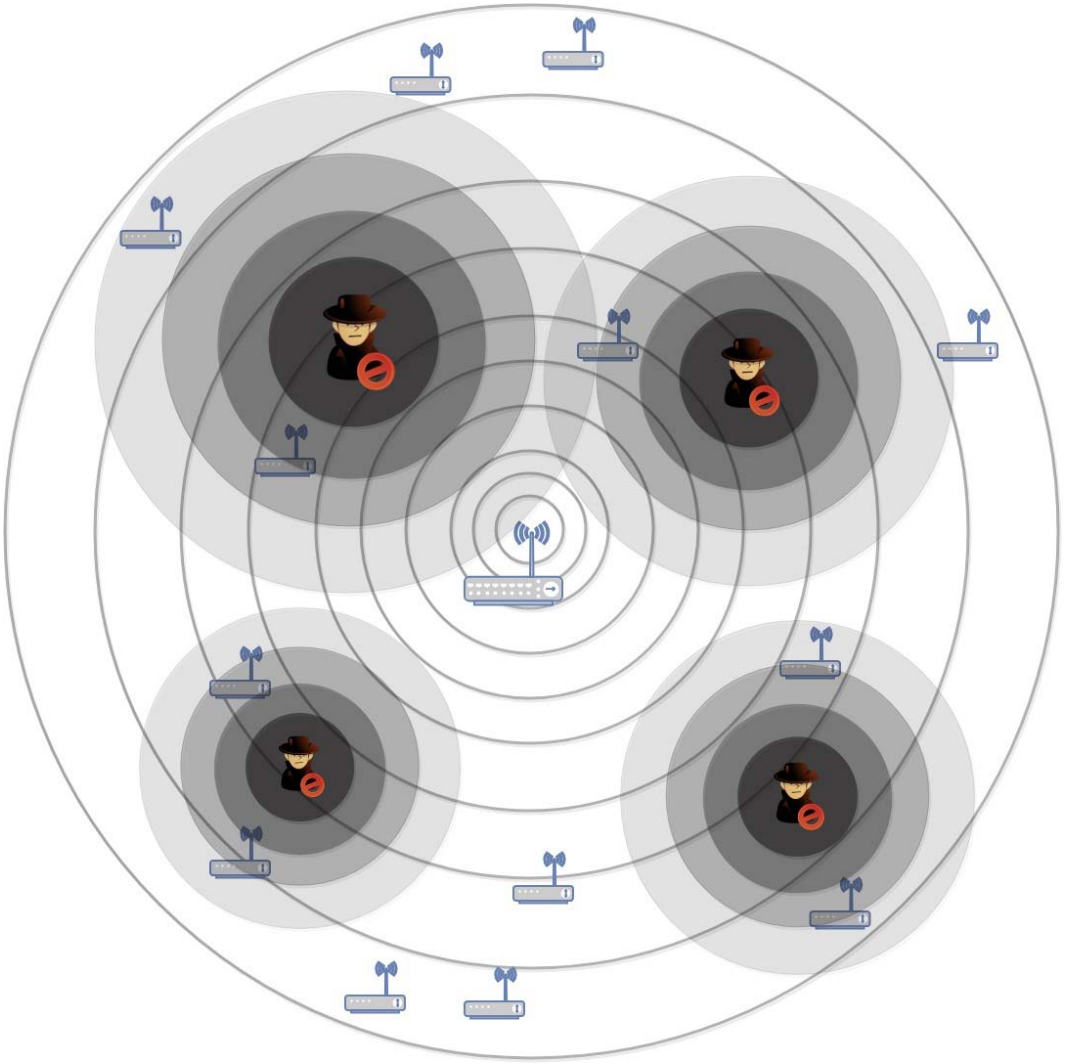
3.4. Πιθανά Σενάρια Χρήσης

Αξιολογώντας τα πλεονεκτήματα και μειονεκτήματα του RLNC που αναλύθηκαν στις προηγούμενες ενότητες, παρουσιάζουμε στις επόμενες ενότητες έξι συνολικά σενάρια χρήσης, όπου τα παραπάνω θετικά χαρακτηριστικών, είτε μεμονωμένα είτε συνδυαστικά, μπορούν να βελτιώσουν τη διαθεσιμότητα και τις άλλες πλευρές ασφάλειας δικτύων.

3.4.1. Ευρυεκπομπή

Η κωδικοποίηση δικτύου είναι, εν γένει, ιδανική για ασύρματα δίκτυα (Bilbao et al., 2016). Είναι από τη φύση τους αναξιόπιστα και η κωδικοποίηση δικτύου επιτρέποντας τον συνδυασμό πολλαπλών παραληφθέντων πακέτων μαζί για την αύξηση του συνόλου της πληροφορίας, σε μια μόνο μετάδοση, πετυχαίνει το στόχο της βελτίωσης της απόδοσης του συνόλου του δικτύου (Zhao & Yao, 2010). Επίσης υπόσχεται σημαντικά οφέλη στην απόδοση του δικτύου, ειδικά σε περιβάλλοντα με απώλειες και πολυεκπομπή (Sundararajan et al., 2011).

Ένα πιθανό σενάριο περιλαμβάνει μια πηγή που εκπέμπει ασύρματα σε πολλούς αποδέκτες, όπως περιγράφεται στο Σχήμα 11, με κακόβουλους χρήστες να επιτίθενται, δημιουργώντας παρεμβολές και υποβιβάζοντας την ποιότητα του δικτύου.

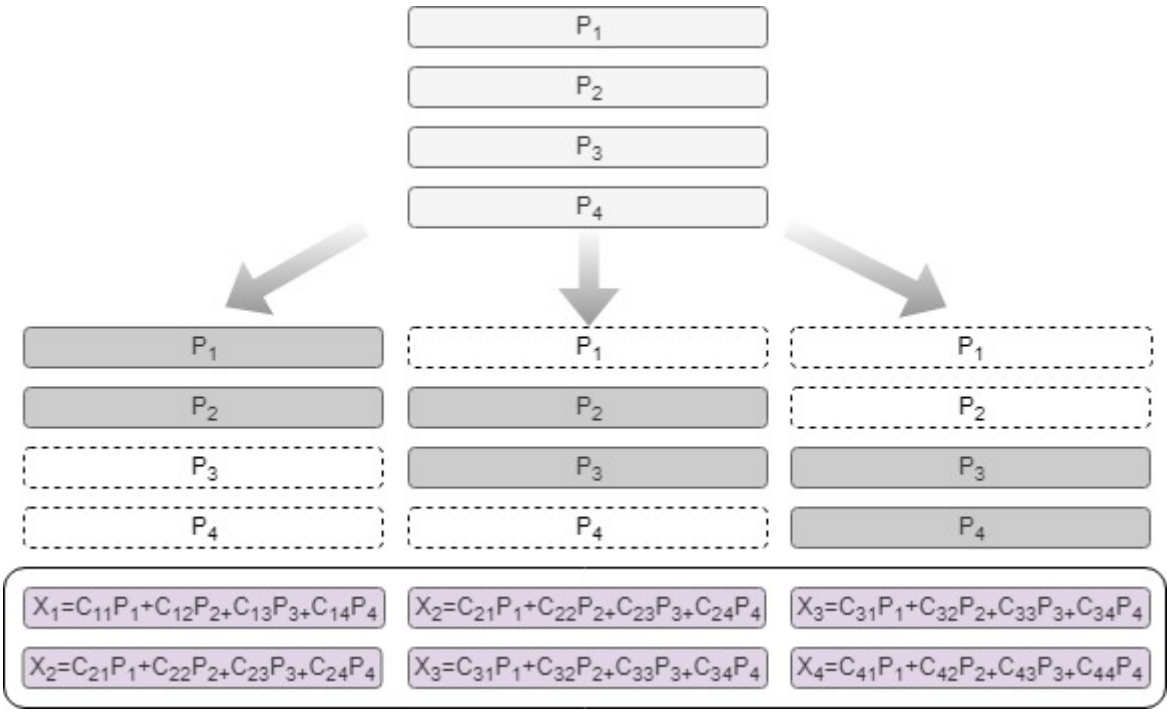


Σχήμα 11 Σενάριο ασύρματης ευρυεκπομπής

Σε ιδανικές συνθήκες, χωρίς την ύπαρξη επίθεσης και άλλες απώλειες, όλα τα πακέτα θα έφταναν ταυτόχρονα σε όλους του παραλήπτες. Σε συνθήκες επίθεσης θα χρειαστούν αρκετές επαναποστολές. Μία απλοϊκή λύση θα ήταν κάθε παραλήπτης να ζητήσει την επαναποστολή από την πηγή όλων των πακέτων που δεν έχει λάβει. Αυτό σημαίνει ότι κάθε χαμένο πακέτο κάθε παραλήπτη θα ξανα-αποσταλλεί, ενώ πολλοί παραλήπτες μπορεί να το έχουν ήδη λάβει. Το αποτέλεσμα της προσέγγισης αυτής είναι ότι ωφελούνται μόνο λίγοι παραλήπτες από κάθε επαναποστολή. Με τη χρήση της κωδικοποίησης δικτύου όλοι οι παραλήπτες μπορούν να ωφεληθούν ταυτόχρονα από μια επαναποστολή, καθώς κάθε αποστολή περιέχει ένα *κωδικοποιημένο* πακέτο, δηλαδή ένα συνδυασμό πακέτων, αντί για ένα μόνο αρχικό πακέτο.

Ας θεωρήσουμε, για παράδειγμα και για την ευκολία υπολογισμών, ότι μία επίθεση έχει ως αποτέλεσμα την *ομοιογενή* υποβάθμιση του δικτύου σε ένα ποσοστό 50%. Δηλαδή μία απλοποιημένη παραδοχή ότι η πιθανότητα λήψης ενός πακέτου από οποιονδήποτε παραλήπτη είναι 50%. Αν σταλούν τα τέσσερα πακέτα, όπως απεικονίζεται στο Σχήμα 12, τότε σε κάθε παραλήπτη θα φτάσουν δύο από αυτά (σκούρο γκρίζο χρώμα).

Αν χρησιμοποιηθεί το RLNC, με την ίδια λογική θα φτάσουν σε κάθε παραλήπτη δύο (κατά πάσα πιθανότητα) γραμμικώς ανεξάρτητες σχέσεις (συνδυασμοί) των αρχικών πακέτων (μωβ χρώμα). Στην πρώτη περίπτωση (χωρίς χρήση RLNC) θα πρέπει να σταλούν και τα τέσσερα πακέτα ξανά, καθώς σε κάθε παραλήπτη λείπει τουλάχιστον ένα διαφορετικό και, αφού το ποσοστό λήψης είναι 50%, τελικά θα πρέπει να γίνουν οκτώ επανεκπομπές συνολικά. Στη δεύτερη περίπτωση (με χρήση RLNC) οι παραλήπτες δε χρειάζεται να λάβουν όλα τα πακέτα. Αρκεί να φτάσουν σε κάθε παραλήπτη ακόμα δύο οποιοιδήποτε γραμμικώς ανεξάρτητοι συνδυασμοί τους, δηλαδή χρειάζονται μόνο άλλες τέσσερις επανεκπομπές.



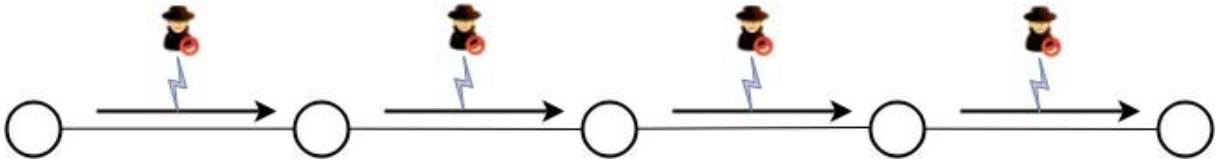
Σχήμα 12 Κατανομή πακέτων σε ευρυεκπομπή

Μία απλοποιημένη παραλλαγή της συγκεκριμένης τεχνικής είναι η εξής. Τα πρώτα πακέτα που αποστέλλονται δεν είναι κωδικοποιημένα. Τα υπόλοιπα της γενιάς, τα οποία προσθέτουν περίσσεια, είναι κωδικοποιημένα. Μία άλλη εναλλακτική, όπως στο (Krigslund et al., 2015), είναι ο κωδικοποιητής να λειτουργεί on-the-fly, κωδικοποιώντας πακέτα καθώς αυτά καταφτάνουν και αντίστοιχα εξάγονται από αυτόν, χωρίς να χρειάζεται να έχουν φτάσει όλα τα πακέτα της γενιάς. Ένα από τα πλεονεκτήματα αυτής της παραλλαγής είναι ότι τα κωδικοποιημένα πακέτα μπορούν να αρχίσουν να αποστέλλονται πριν ακόμα τροφοδοτηθεί όλη η γενιά στον κωδικοποιητή. Επιτυγχάνεται έτσι μείωση της καθυστέρησης, αλλά με την αρνητική συνέπεια τη μείωση της πιθανότητας αποκωδικοποίησης, καθώς τα κωδικοποιημένα πακέτα έχουν μεγαλύτερη πιθανότητα να βελτιώσουν μια απώλεια όταν περισσότερα από τα αρχικά πακέτα συμπεριλαμβάνονται στους γραμμικούς συνδυασμούς.

Το ίδιο ακριβώς σενάριο, μπορεί να εφαρμοστεί και σε ένα ενσύρματο δίκτυο, χωρίς να αλλάζει η λογική της εφαρμογής της κωδικοποίησης δικτύου.

3.4.2. Multi-hop με επανεκπομπή

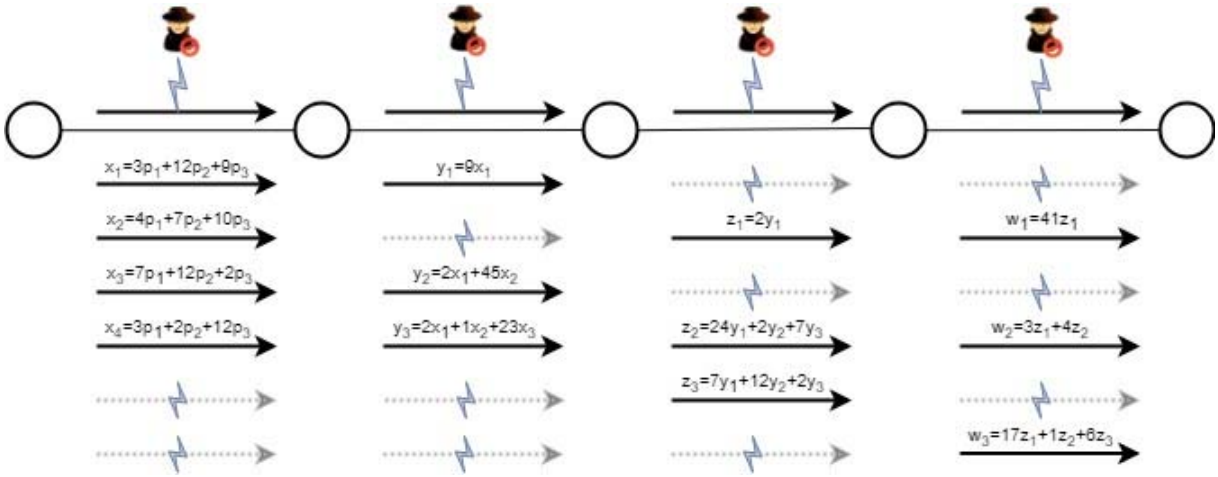
Το επόμενο σενάριο περιλαμβάνει την επικοινωνία από μια πηγή σε ένα μόνο παραλήπτη, μέσω από πολλούς ενδιάμεσους κόμβους, είτε εξαιτίας της δομής του ενσύρματου δικτύου είτε εξαιτίας της θέσης και της εμβέλειας των κόμβων του ασύρματου δικτύου, όπως φαίνεται στο Σχήμα 13.



Σχήμα 13 Multi-hop με επανεκπομπή

Η ιδιαιτερότητα σε αυτό το δίκτυο είναι ότι οι αναμεταδότες δεν προωθούν απλά τα εισερχόμενα πακέτα τους, αλλά τα επανα-κωδικοποιούν. Στην περίπτωση των ασύρματων δικτύων κάθε κόμβος μπορεί εύκολα να συμμετέχει και ως κωδικοποιητής (Lun, Medard & Koetter, 2006).

Το δίκτυο στο συγκεκριμένο σενάριο, θεωρείται ότι δέχεται επίθεση από έναν κακόβουλο χρήστη με αποτέλεσμα οι πιθανότητες για κάθε κόμβο να λάβει ένα πακέτο να είναι πολύ μικρή. Η χρήση της κωδικοποίησης δικτύου σε συνδυασμό με την επανα-κωδικοποίηση σε κάθε ενδιάμεσο κόμβο, είναι αυτά που θα αυξήσουν την πιθανότητα τα πακέτα να φτάσουν στον τελικό παραλήπτη.



Σχήμα 14 Multi-hop με επανεκπομπή

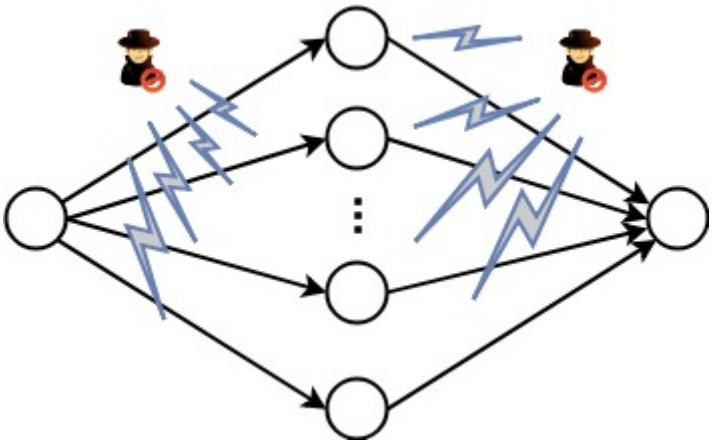
Αν για παράδειγμα ο πρώτος ενδιάμεσος κόμβος λάβει ένα κωδικοποιημένο πακέτο x_1, τότε μπορεί να στείλει ένα επανα-κωδικοποιημένο πακέτο y_1και να τηρήσει το x_1 στη μνήμη του (buffer). Έτσι την επόμενη φορά, λαμβάνοντας και ένα δεύτερο

κωδικοποιημένο πακέτο x_2, μπορεί να παράξει ένα νέο κωδικοποιημένο πακέτο y_2 ως συνδυασμό και των δύο (x_1 και x_2). Ο δεύτερος ενδιάμεσος κόμβος λαμβάνει το y_1 και παράγει ένα κωδικοποιημένο πακέτο, το οποίο όμως χάνεται. Την επόμενη φορά, αν και δεν έχει λάβει νέα πληροφορία, μπορεί να παράξει ένα νέο κωδικοποιημένο πακέτο z_1 και να το στείλει. Έτσι κάθε ενδιάμεσος κόμβος, τηρώντας τα εισερχόμενά του πακέτα, μπορεί να παράγει συνδυασμούς τους, ακόμα και όταν δεν λαμβάνει νέα από τον προηγούμενό του. Έτσι προωθεί νέους συνδυασμούς, οι οποίοι μπορεί τελικά να είναι χρήσιμοι στον τελικό παραλήπτη για την αποκωδικοποίηση των αρχικών πακέτων.

Στην αντίστοιχη περίπτωση που δεν εφαρμόζεται η κωδικοποίηση δικτύου, η πηγή θα στείλει διαδοχικά τα p_1, p_2, p_3, p_2 και αντίστοιχα ο παραλήπτης λαμβάνει, για παράδειγμα, τελικά τα p_1, p_2, p_2. Δηλαδή λαμβάνει πακέτα που ήδη έχει και δεν προσθέτουν καμία επιπλέον πληροφορία.

3.4.3. Multi-hop με παράλληλα μονοπάτια

Σε αυτό το σενάριο τα κωδικοποιημένα πακέτα ταξιδεύουν από πολλαπλούς παράλληλους δρόμους με αποδέκτη ένα μόνο παραλήπτη, όπως απεικονίζεται στο Σχήμα 15.

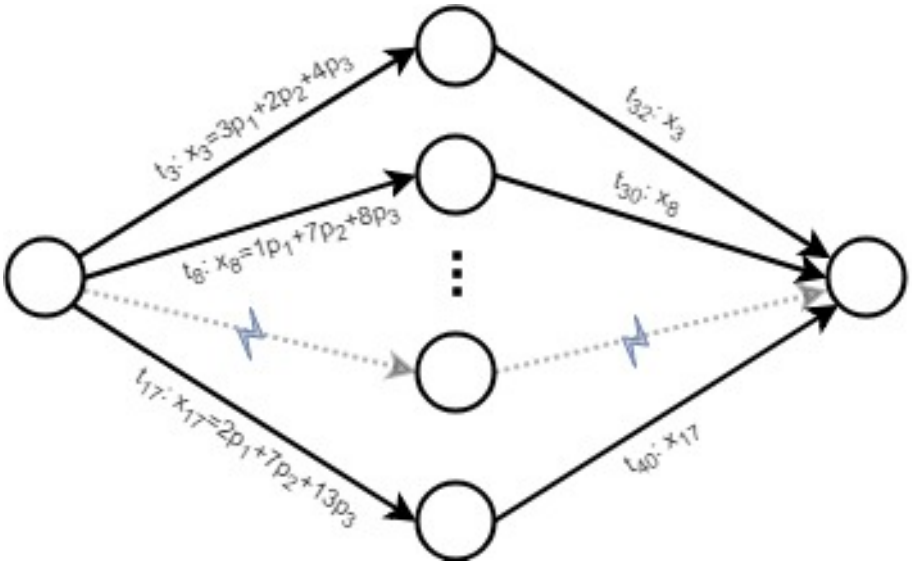


Σχήμα 15 Παράλληλα μονοπάτια

Η πηγή κάνει ευρεκπομπή των πακέτων στους ενδιάμεσους κόμβους και αυτοί με τη σειρά τους στέλνουν ένας-ένας την πληροφορία στον τελικό παραλήπτη. Θεωρείται ότι το δίκτυο δέχεται συνολικά επίθεση, με αποτέλεσμα τόσο η επικοινωνία από την πηγή στους ενδιάμεσους κόμβους, όσο και η επικοινωνία από τους ενδιάμεσους στον τελικό παραλήπτη, να είναι σημαντικά υποβιβασμένη και η πιθανότητα επιτυχούς λήψης

πακέτου αρκετά μικρή. Η εφαρμογή του RLNC και ειδικά η προσθήκη της δυνατότητας στους ενδιάμεσους κόμβους να συμμετέχουν στην κωδικοποίηση, παράγοντας νέα κωδικοποιημένα πακέτα κάθε φορά, μπορούν να συντελέσουν στη βελτίωση της διαθεσιμότητας του δικτύου.

Στην περίπτωση που οι ενδιάμεσοι κόμβοι δεν επανα-κωδικοποιούν τα πακέτα και οι δυνατότητες επικοινωνίες είναι περιορισμένες, μπορούμε να θεωρήσουμε ότι κάποια στιγμή t_3 κάποιος ή κάποιοι ενδιάμεσοι κόμβοι θα λάβουν ένα κωδικοποιημένο πακέτο x_3, το οποίο θα προσπαθήσουν να στείλουν στον παραλήπτη. Αν αποτύχουν, τότε θα επαναλάβουν την αποστολή, τηρώντας το ληφθέν πακέτο στη μνήμη τους (buffer).



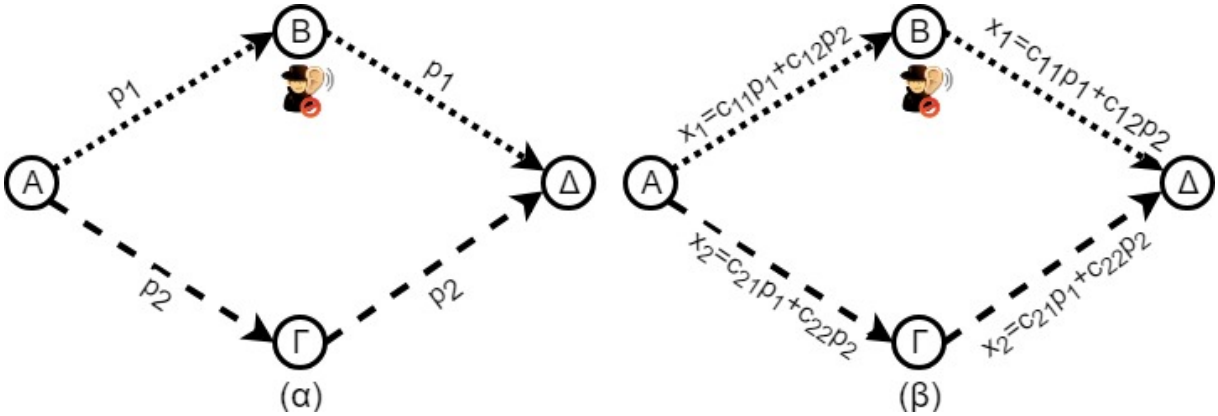
Σχήμα 16 Παράλληλα μονοπάτια

Κάποια χρονική στιγμή t_{32}, ένας ή περισσότεροι κόμβοι καταφέρνουν να το στείλουν στον τελικό παραλήπτη. Αντίστοιχα και άλλοι ενδιάμεσοι κόμβοι θα λάβουν κάποιες χρονικές στιγμές (t_8, t_{17}) πακέτα και θα καταφέρουν να τα παραδώσουν (t_{30}, t_{40}). Τελικά ο παραλήπτης θα έχει στη διάθεση του τρία κωδικοποιημένα πακέτα, τα οποία θα μπορέσει να αποκωδικοποιήσει στα αρχικά τους p_1, p_2 και p_3. Αν τύχει όμως και οι επιτυχημένες επικοινωνίες είναι για παράδειγμα (α) την ίδια χρονική στιγμή από δύο ενδιάμεσους κόμβους που έχουν το ίδιο κωδικοποιημένο πακέτο ή (β) από τον ίδιο ενδιάμεσο κόμβο, ο οποίος μπορεί να έχει στη διάθεση του περισσότερα από ένα κωδικοποιημένα πακέτα, αλλά αποφασίζει να στείλει το ίδιο (είτε για παράδειγμα γιατί λειτουργεί τυχαία ή στέλνει το τελευταίο), τότε ο τελικός παραλήπτης δε θα καταφέρει να αποκτήσει τρεις γραμμικά ανεξάρτητους συνδυασμούς και δε θα είναι εφικτή η αποκωδικοποίηση. Σε αυτό το σενάριο μπορεί να αξιοποιηθεί η δυνατότητας επανα-

κωδικοποίησης στους ενδιάμεσους κόμβους, όπου θα μπορούσε (α) οι δύο ενδιάμεσοι κόμβοι ή (β) ο ίδιος κόμβος, θεωρώντας ότι κατέχει και άλλα x_i κωδικοποιημένα πακέτα, να στείλουν διαφορετικούς συνδυασμούς τους με αποτέλεσμα να φτάσουν τελικά στον παραλήπτη οι ανεξάρτητοι συνδυασμοί που χρειάζονται.

3.4.4. Προστασία από Υποκλοπές

Ένα άλλο σενάριο που δείχνει τα εγγενή χαρακτηριστικά ασφαλείας της τεχνικής αυτής, φαίνεται στο Σχήμα 17.



Σχήμα 17 Αποστολή δεδομένων από ανεξάρτητες διαδρομές

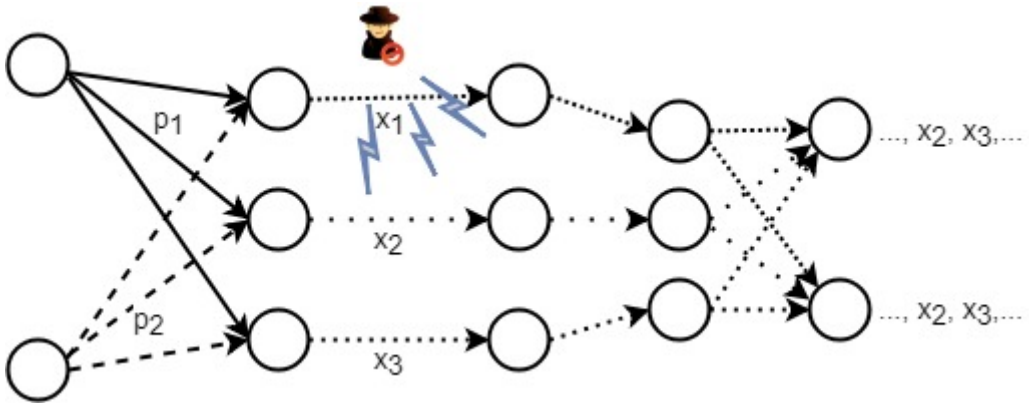
Εδώ ο κόμβος Α στέλνει τα πακέτα p_1 και p_2 στον κόμβο Δ από δύο ανεξάρτητες διαδρομές (Σχήμα 17). Αν κάποιο κακόβουλος μπορούσε να υποκλέψει την επικοινωνία από ένα κανάλι, τότε θα μπορούσε να διαβάσει το ένα από τα δύο. Αν όμως ο Α έστελνε γραμμικούς συνδυασμούς των p_1 και p_2, τότε ο υποκλοπέας δε θα μπορούσε να γνωρίζει κανένα από τα δύο πακέτα.

Για το συγκεκριμένο σκοπό, δε χρησιμοποιείται η περίσσεια ως χαρακτηριστικό, καθώς δε παρέχει κάποιο πλεονέκτημα, αλλά γίνεται αξιοποίηση της ανάγκης λήψης μεγάλου ποσοστού των πακέτων μιας γενιάς για να μπορεί να ξεκινήσει και να ολοκληρωθεί η αποκωδικοποίηση των αρχικών πακέτων, ως χαρακτηριστικό ασφάλειας. Επιπλέον θα μπορούσε η πληροφορία, για να είναι πιο ασφαλής, να συνδυάζεται με εντελώς τυχαία πληροφορία, ώστε να μειώσει ακόμα περισσότερο την πιθανότητα μη εξουσιοδοτημένης ανάκτησης. Τέλος, αν τα πιθανά μονοπάτια δρομολόγησης είναι γνωστά στον κόμβο Α, τότε θα μπορούσε να τεμαχίζει τα πακέτα με τέτοιο τρόπο ώστε να μη γίνεται αποστολή όλων των τμημάτων τους από ένα μονοπάτι. Έτσι, μόνο ο

παραλήπτης Δ, ο οποίος λαμβάνει όλα τα τμήματα μέσα από τα διαφορετικά μονοπάτια, θα μπορούσε να ανακτήσει τα αρχικά πακέτα, ενώ ένας υποκλοπέας στον κόμβο Β θα μπορούσε να επιτύχει μερική μόνο ανάκτηση του κάθε πακέτου.

3.4.5. Inter-flow Κωδικοποίηση Δικτύου

Ένα ακόμα σενάριο είναι η inter-flow κωδικοποίηση, όπου διαφορετικές ροές συνδυάζονται για να χρησιμοποιήσουν ταυτόχρονα τους ίδιους πόρους του δικτύου και να μεγιστοποιήσουν την πιθανότητα μετάδοσης της πληροφορίας, ακόμα και όταν κάποιες από τις διαδρομές δεν είναι πλέον διαθέσιμες, λόγω επιθέσεων.



Σχήμα 18 Inter-flow κωδικοποίηση

Σε ένα τέτοιο σενάριο τα πακέτα από διαφορετικές ροές συνδυάζονται μεταξύ τους και αποστέλλονται από διαφορετικά μονοπάτια για την επίτευξη ευρωστίας στο δίκτυο.

3.4.6. Πολύ-εκπομπή Βέλτιστης Προσπάθειας (Best-Effort Multicast)

Σε αυτό το σενάριο, τα αρχικά πακέτα μιας γενιάς στέλνονται μη κωδικοποιημένα και συνοδεύονται από έναν αριθμό πλεοναζόντων κωδικοποιημένων πακέτων. Έτσι, ακόμα και σε ένα εχθρικό περιβάλλον, τα κωδικοποιημένα πακέτα που θα μπορέσουν να παραληφθούν, θα παράσχουν επιπλέον βαθμούς αξιοπιστίας. Σε συνδυασμό με όσα αρχικά πακέτα έχουν παραληφθεί, ένα μεγάλο πλήθος παραληπτών θα μπορέσει να ανακτήσει σε ικανοποιητικό βαθμό, αν και όχι πλήρως, το αρχικό περιεχόμενο. Αυτό το σενάριο έχει κοινά χαρακτηριστικά με τις τεχνικές Forward Error Correction (FEC), καθώς τα κωδικοποιημένα πακέτα παράγονται προκαταβολικά για την διόρθωση τυχόν σφαλμάτων στο εχθρικό περιβάλλον λειτουργίας, χωρίς να αναμένεται κάποια

ανάδραση από τους αποδέκτες, ούτε να επιδιώκεται η πλήρης ανάκτηση του περιεχομένου.

Κεφάλαιο 4
Πειραματική Μελέτη

Το προηγούμενο κεφάλαιο κατέδειξε σε θεωρητικό επίπεδο ότι η κωδικοποίηση δικτύου και ιδιαίτερα η τεχνική RLNC μπορεί να συνεισφέρει στην ασφάλεια δικτύων βελτιώνοντας σημαντικά τη διαθεσιμότητά τους σε εχθρικά περιβάλλοντα. Το κεφάλαιο αυτό θα ελέγξει και επαληθεύσει τα πορίσματα της θεωρητικής προσέγγισης μέσα από μία πειραματική μελέτη βασισμένη σε διαθέσιμες υλοποιήσεις του RLNC.

4.1. Πλατφόρμα Προσομοίωσης

Το πρώτο βήμα της πειραματικής μελέτης είναι η επιλογή μίας πλατφόρμας προσομοίωσης δικτύων. Η προσομοίωση είναι η ενδεδειγμένη προσέγγιση, δεδομένης της καινοτομίας της προσέγγισης, της πολυπλοκότητας των προς εξέταση σεναρίων αλλά και της αδυναμίας υλοποίησης επιθέσεων σε δίκτυα που βρίσκονται σε λειτουργία, είτε παραγωγικά είτε πειραματικά. Επιλέξαμε ως πλατφόρμα προσομοίωσης το Network Simulator 3 [5], καθώς είναι μία από τις πιο διαδεδομένες και δημοφιλείς πλατφόρμες προσομοίωσης δικτύων στον ερευνητικό και ακαδημαϊκό χώρο. Είναι ένας προσομοιωτής δικτύου των επιπέδων του OSI γραμμένος στη γλώσσα προγραμματισμού C++ και διατίθεται ελεύθερα για ερευνητικούς και εκπαιδευτικούς σκοπούς με την άδεια χρήσης GPLv2.

4.2. Αξιολόγηση Υλοποιήσεων Network Coding

Το επόμενο βήμα είναι η αναζήτηση, αξιολόγηση, αποτίμηση και επιλογή κατάλληλων εργαλείων και βιβλιοθηκών υλοποίησης και υποστήριξης του network coding και

[5] https://www.nsnam.org/

ειδικότερα του RLNC, τα οποία να συνεργάζονται με την πλατφόρμα προσομοίωσης ns-3. Η αναζήτησή μας εντόπισε τρία συνολικά εργαλεία, τα οποία αναλύονται στη συνέχεια:

- Network coding implementation on ns-3 (David Gómez Fernández, Eduardo Rodríguez Maza & Ramón Agüero Calvo, 2014)
- Yet Another Network Coding Implementation (ns3-yanci)
- kodo

4.2.1. Network coding implementation on ns-3

Το Network coding implementation on ns-3 (David Gómez Fernández, Eduardo Rodríguez Maza & Ramón Agüero Calvo, 2014) είναι ένα άρθρωμα (module) για το ns-3. Δημιουργήθηκε το 2014 για ακαδημαϊκούς σκοπούς. Τα κύρια χαρακτηριστικά του με βάση τον επίσημο ιστότοπο είναι:

- Κωδικοποίηση Δικτύου: παρέχει ένα επιπλέον επίπεδο ανάμεσο στο επίπεδο δικτύου (network layer) και το επίπεδο μεταφοράς (transport layer) με δύο είδη κωδικοποίησης: ένα Inter-Flow Network Coding και ένα Intra-Flow Network Coding.
- Εργαλείο δημιουργίας σεναρίων: ένα βολικό τρόπο για την κατασκευή σεναρίων ασύρματων δικτύων προς προσομοίωση.

Η ανάπτυξη του εργαλείου σταμάτησε το 2014. Η εγκατάσταση του εργαλείου σε ένα σύγχρονο υπολογιστή και διανομή του λειτουργικού συστήματος Linux αποδείχθηκε μία ιδιαίτερα δύσκολη και επίπονη διαδικασία, ώστε να λειτουργήσει σωστά. Η λειτουργία σε μία σύγχρονη διανομή Linux (Ubuntu 18.04) ήταν αδύνατη παρά τις εκτεταμένες προσπάθειές μας. Απαιτήθηκε να εντοπιστούν μέσα από δοκιμές και λάθη τα προ-απαιτούμενα εργαλεία, βιβλιοθήκες και αρθρώματα (module) λογισμικού, τα οποία κυκλοφορούσαν την εποχή που δημιουργήθηκε, μία ιδιαίτερα χρονοβόρα διαδικασία. Στον Πίνακας 1 παρατίθενται οι συνδυασμοί των προ-απαιτούμενων πακέτων λογισμικού (είδη και εκδόσεις) που δούλεψαν στη δικιά μας περίπτωση. Ακόμα και η αλλαγή της έκδοσης του λειτουργικού μπορεί να δημιουργήσει

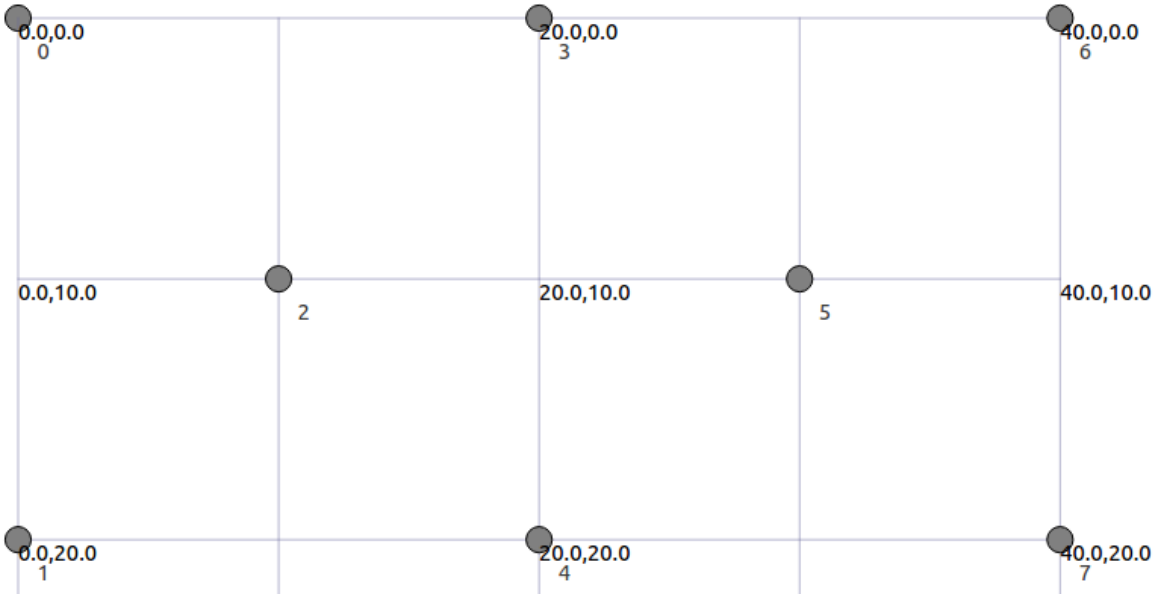
προβλήματα, γιατί συνοδεύεται από εκδόσεις βασικών εργαλείων που δεν είναι συμβατές με το εργαλείο (όπως μεταγλωττιστές και βιβλιοθήκες).

Προ-απαιτούμενο	Έκδοση	Σχόλιο
Ubuntu	14.04	*Λειτουργικό σύστημα*
Ns-3	3.13	*Network Simulator 3*
g++	4.4.7	*Compiler*
OpenSSL	1.0.2 (τελευταία)	*Toolkit για SSL, TLS*
IT++	4.3.1	*Βιβλιοθήκη με μεθόδους μαθηματικών, επεξεργασίας σήματος και επικοινωνιών*
FFLAS/FFPACK	1.5.0	*Βιβλιοθήκη με βασικές μεθόδους γραμμικής άλγεβρας σε πεπερασμένο πεδίο*
GMP	5.0.1	*Project Γραφικής Μοντελοποίησης*
Givaro	3.6.0	*Βιβλιοθήκη αριθμητικών και αλγεβρικών υπολογισμών*
OpenBLAS	0.2.20	*Βιβλιοθήκη βασικής γραμμικής άλγεβρας*
Lapack	τελευταία έκδοση	*Βιβλιοθήκη γραμμικής άλγεβρας*
Libxml2-dev	τελευταία έκδοση	*Toolkit για xml*
gtk	2.0	*Toolkit για GUI*
gsl	Libgsl10-dev	*Βιβλιοθήκη για αριθμητική σε C, C++*
doxygen		*Εργαλείο για παραγωγή documentation*
NetAnim	τελευταία έκδοση	*Πρόγραμμα οπτικοποίησης της κίνησης ενός δικτύου βάσει της προσομοίωσης στο ns-3*

Πίνακας 1 Προ-απαιτούμενα «Network coding implementation on ns-3»

Η εκτέλεση προσομοιώσεων στο συγκεκριμένο ns-3 module γίνεται υποχρεωτικά με τον ορισμό σεναρίων από το "scenario-creator". Για παράδειγμα, η δημιουργία του ασύρματου δικτύου[6], το οποίο απεικονίζεται στο Σχήμα 19 γίνεται ορίζοντας τον παρακάτω πίνακα περιγραφής σεναρίου.

[6] Να σημειωθεί ότι για το συγκεκριμένου και όπου είναι εφικτό, χρησιμοποιείται το NetAnim, ένα λογισμικό για την οπτικοποίηση των αποτελεσμάτων προσομοίωσης του ns-3. Αυτό μας δείχνει τις θέσεις των κόμβων στον χώρο, καθώς και την κίνηση των κόμβων του δικτύου στο χρόνο.



Σχήμα 19 Παράδειγμα ασύρματου δικτύου

#No.	X	Y	Z	TX	RX	CR	FWD
0	0	0	0	7	0	0	0
1	0	20	0	6	0	0	0
2	10	10	0	0	0	1	1
3	20	0	0	0	0	0	1
4	20	20	0	0	0	0	1
5	30	10	0	0	0	0	1
6	40	0	0	0	1	0	0
7	40	20	0	0	1	0	0

Πίνακας 2 Παράδειγμα πίνακα περιγραφής σεναρίου

Δηλώνονται οι θέσεις των κόμβων, ποιοί κόμβοι είναι οι αποστολείς (TX) με τους αντίστοιχους παραλήπτες (RX), ποιοί κόμβοι πραγματοποιούν κωδικοποίηση δικτύου (CR) και ποιοί απλά προωθούν τα πακέτα (FWD). Στον επόμενο Πίνακας 3 καταγράφονται τα κανάλια επικοινωνίας , όπου 0 σημαίνει ότι περνάνε όλα τα πακέτα, ενώ 1 ότι κανένα πακέτο δεν περνάει.

	#0	#1	#2	#3	#4	#5	#6	#7
#0	1	1	0	1	1	1	1	1
#1	1	1	0	1	1	1	1	1
#2	0	0	1	0	0	1	1	1
#3	1	1	0	1	1	0	1	1
#4	1	1	0	1	1	0	1	1
#5	1	1	1	0	0	1	0	0

#6	1	1	1	1	1	0	1	1
#7	1	1	1	1	1	0	1	1

Πίνακας 3 Παράδειγμα καναλιών επικοινωνίας

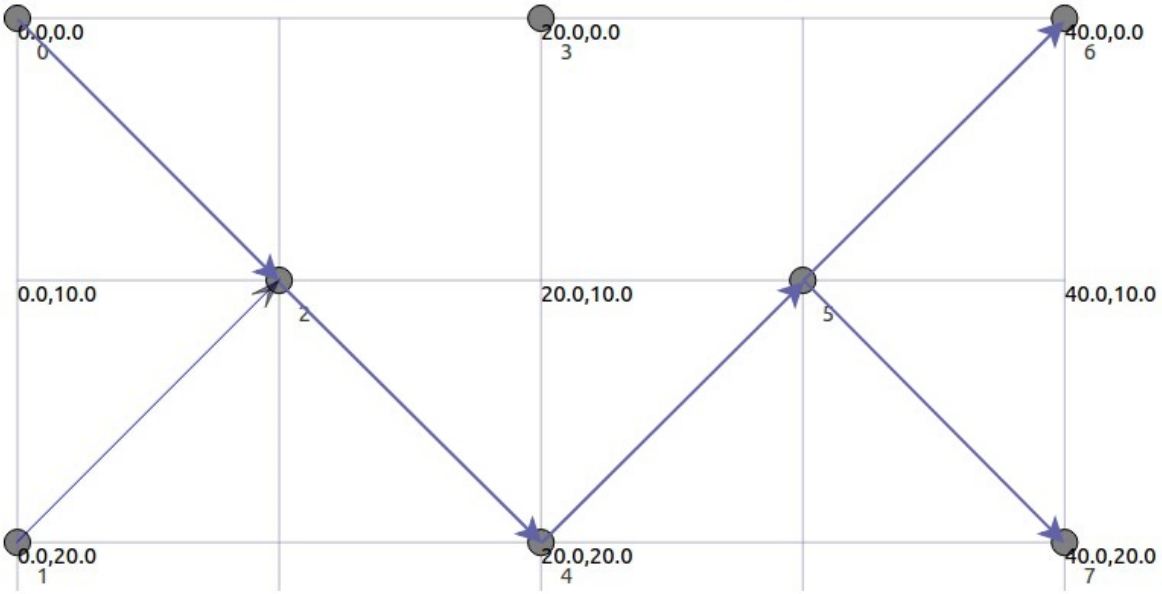
Τέλος, ορίζεται ο πίνακας δρομολόγησης (Πίνακας 4), όπου, σύμφωνα με τις προδιαγραφές, αν για ένα προορισμό θέλουμε να δηλώσουμε δύο πιθανές διαδρομές, τότε δημιουργούνται δύο ξεχωριστές γραμμές.

#Node ID	Destination	Next hop	#Node ID	Destination	Next hop
0	1	2	4	0	2
0	2	2	4	1	2
0	3	2	4	2	2
0	4	2	4	3	2
0	5	2	4	3	5
0	6	2	4	5	5
0	7	2	4	6	5
1	0	2	4	7	5
1	2	2	5	0	3
1	3	2	5	0	4
1	4	2	5	1	3
1	5	2	5	1	4
1	6	2	5	2	3
1	7	2	5	2	4
2	0	0	5	3	3
2	1	1	5	4	4
2	3	3	5	6	6
2	4	4	5	7	7
2	5	3	6	0	5
2	5	4	6	1	5
2	6	3	6	2	5
2	6	4	6	3	5
2	7	3	6	4	5
2	7	4	6	5	5
3	0	2	6	7	5
3	1	2	7	0	5
3	2	2	7	1	5
3	4	2	7	2	5
3	4	5	7	3	5
3	5	5	7	4	5
3	6	5	7	5	5
3	7	5	7	6	5

Πίνακας 4 Πίνακας δρομολόγησης

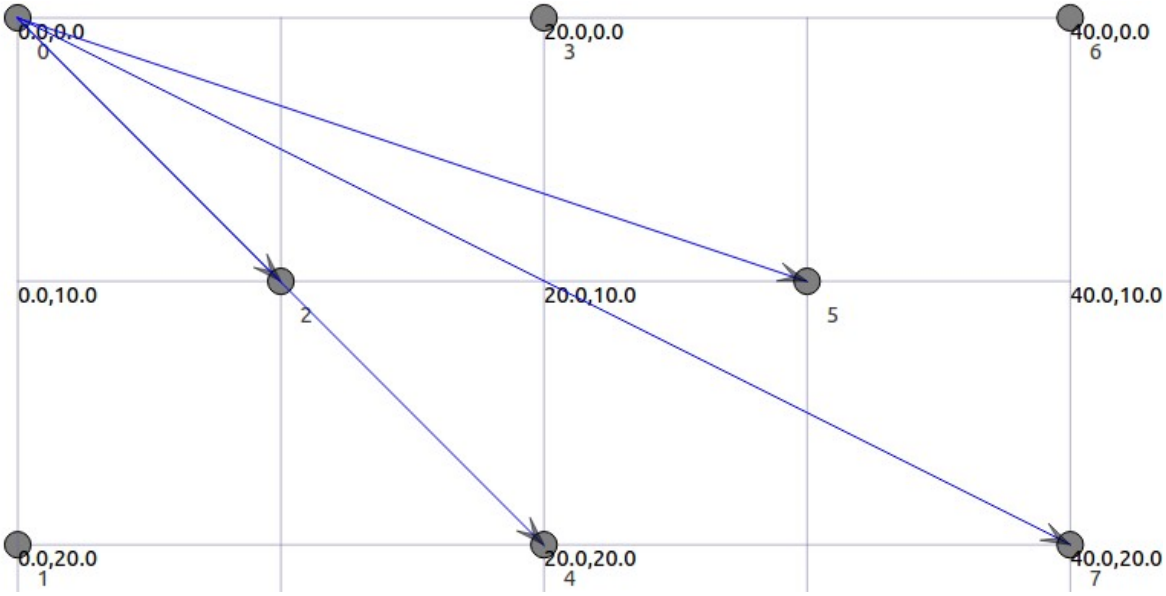
Όπως αναφέρθηκε παραπάνω, η ανάπτυξη του εργαλείου ξεκίνησε και σταμάτησε το 2014. Μέσα από τις εκτεταμένες δοκιμές μας, διαπιστώθηκε ότι παρά τις επίσημες περιγραφές, πολλά από τα χαρακτηριστικά του δεν υλοποιήθηκαν ποτέ ή παρέμειναν ημιτελή και λειτουργούσαν αναξιόπιστα. Αναφέρουμε στη συνέχεια ορισμένες χαρακτηριστικές περιπτώσεις.

Κατά την εκτέλεση της προσομοίωσης στο παραπάνω δίκτυο, αν υπερθέσουμε όλες τις κινήσεις των πακέτων, μετά την αρχικοποίηση του δικτύου με την αποστολή αιτημάτων ARP από όλους τους κόμβους για τη συμπλήρωση της αντίστοιχης ARP cache, παρατηρούμε όπως φαίνεται και στο Σχήμα 20, ότι όλες οι κινήσεις περνάνε από τον κόμβο 4 και καμία από τον 3. Αν αλλάξει η θέση τους στον πίνακα δρομολόγησης, αλλάζει και το αποτέλεσμα. Επίσης η επιλογή στο αρχείο ρυθμίσεων MULTIPATH αναφέρεται στο αρχείο οδηγιών (Readme) ότι δεν έχει ακόμα υλοποιηθεί και όντως δεν ανακτάται πουθενά στον κώδικα. Επομένως δεν υπάρχει τρόπος να ακολουθηθούν πολλαπλές διαδρομές ταυτόχρονα.

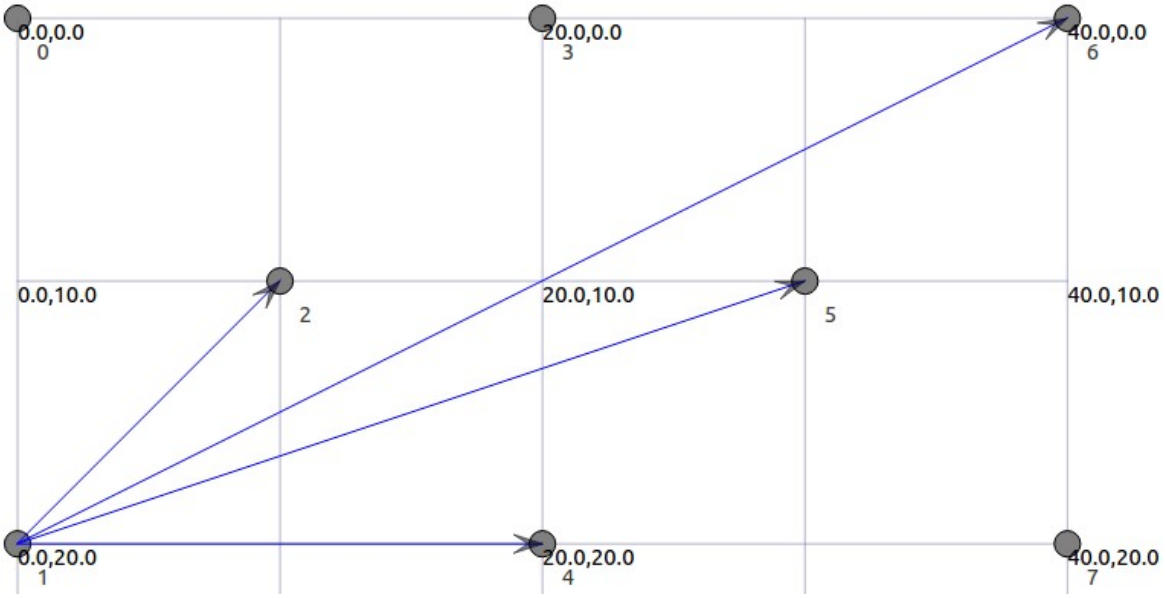


Σχήμα 20 Συνολική κίνηση δικτύου

Αν κάποιος επιλέξει την απενεργοποίηση της κωδικοποίησης δικτύου, ώστε να αποκτήσει συγκρίσιμα αποτελέσματα, τότε καταλήγει σε μία κίνηση που δεν ακολουθεί καθόλου τον πίνακα δρομολόγησης, όπως φαίνεται και στα παρακάτω δύο σχήματα (Σχήμα 21 και Σχήμα 22), τα οποία έχουν αποτυπωμένη όλη την κίνηση.



Σχήμα 21 Παράδειγμα χωρίς κωδικοποίηση δικτύου



Σχήμα 22 Παράδειγμα χωρίς κωδικοποίηση δικτύου

Στην τεκμηρίωση του εργαλείου αναφέρεται ότι δεν έχει υλοποιηθεί ακόμα η inter-flow λύση, παρά μόνο η intra-flow, η οποία υποστηρίζει μόνο το πρωτόκολλο UDP και όχι το TCP. Τέλος, στην προσπάθεια καθορισμού του ρυθμού διαγραφής πλαισίων (Frame Erasure Rate, FER) και ακολουθώντας τις οδηγίες (Readme) σχετικά με το νέο μοντέλο διάδοσης απωλειών (propagation loss model) SIMPLE, εντοπίσαμε την επεξήγηση:

«5- SIMPLE --> Make use of the SimplePropagationLossModel created by us

*(NEW)*5- MANUAL --> The scenario description file (i.e. x-channel-sides.conf) will hold the information related to the FER values that will be set throughout the links»*

Αναλύοντας τον πηγαίο κώδικα, δε βρέθηκε στο αντίστοιχο switch statement κάποια υλοποίηση, παρά μόνο το σχόλιο «*//TO BE IMPLEMENTED*».

Με βάση τα παραπάνω ευρήματα και παρά τη μεγάλη επένδυση χρόνου για την εκμάθηση του συγκεκριμένου εργαλείου, αποφασίστηκε να απορριφθεί η χρήση του για τους σκοπούς της συγκεκριμένης μεταπτυχιακής διατριβής, ως ακατάλληλο και αναξιόπιστο.

4.2.2. Ns3-yanci

Το Yet Another Network Coding Implementation[7] διατίθεται επίσης ως ένα άρθρωμα του ns-3. Περιλαμβάνει μια απλοποιημένη υλοποίηση κωδικοποίησης ασύρματου δικτύου σε σενάριο μονού πομπού, βασιζόμενο στο COPE (Coding Opportunistically). Το COPE είναι ένας αλγόριθμος κωδικοποίησης inter-flow, ο οποίος συνθέτει με XOR πολλά πακέτα από διαφορετικές ροές και τα εκπέμπει όλα μαζί ως ένα προς όλους τους αποδέκτες.

Παρά τις εκτεταμένες προσπάθειές μας, το yanci δε λειτούργησε στο περιβάλλον μας καθώς δεν καλύπτονταν όλα τα προ-απαιτούμενα για την εγκατάστασή του. Στις εκδόσεις του ns-3 και διανομές του Linux που είχαμε στη διάθεσή μας, δεν μπορούσε να γίνει μεταγλώττιση (compilation) χωρίς σφάλματα. Επίσης, διαπιστώθηκε σημαντική έλλειψη τεκμηρίωσης (documentation) και σχετικών οδηγιών χρήσης.

Τα παραπάνω προβλήματα σε συνδυασμό με την πρότερη αρνητική εμπειρία με το εργαλείο Network coding implementation on ns-3 λειτούργησε αποτρεπτικά ώστε να επενδυθούν περισσότεροι πόροι για τη διαμόρφωση ενός λειτουργικού περιβάλλοντος για το yanci.

[7] https://github.com/yangchi/ns3-yanci

4.2.3. Kodo ns-3

Το kodo[8] (Pedersen, Heide & Fitzek, 2011) είναι μια βιβλιοθήκη ανοικτού κώδικα (open source) γραμμένη στη γλώσσα προγραμματισμού C++. Παρέχεται από την εταιρεία Steinwurf. Υλοποιεί Erasure Correcting Codes και πιο συγκεκριμένα το Random Linear Network Coding και παραλλαγές του καθώς και άλλους αλγορίθμους όπως το Reed-Solomon. Διατίθεται με άδεια για χρήση σε ερευνητικούς και εκπαιδευτικούς σκοπούς. Επιτρέπει στους ερευνητές την υλοποίηση νέων αλγορίθμων, την προσομοίωση και έλεγχο λειτουργιών κώδικα.

Η υλοποίηση του RLNC στο kodo δίνει τη δυνατότητα δημιουργίας κόμβων, τόσο σε ασύρματα όσο και σε ενσύρματα δίκτυα, που να μπορούν να κωδικοποιούν ή να επανα-κωδικοποιούν πακέτα. Στα δίκτυα αυτά, μια πηγή στέλνει τα πακέτα μίας μόνο γενιάς έως ότου όλοι οι παραλήπτες λάβουν τον αριθμό των κωδικοποιημένων πακέτων που είναι ικανός για την αποκωδικοποίηση της αρχικής πληροφορίας.

Η διαδικασία εγκατάστασης ήταν απλή καθώς υπήρχαν σαφείς οδηγίες εγκατάστασης, οι οποίες συνοδεύονταν και με την αντίστοιχη λίστα των προ-απαιτούμενων εργαλείων και βιβλιοθηκών και πώς μπορούν αυτά να εγκατασταθούν. Επίσης, η διαδικασία απόκτησης της ειδικής άδειας χρήσης ήταν εύκολη και γρήγορη. Τέλος η τεκμηρίωση συμπεριλάμβανε και μερικά παραδείγματα και επεξηγήσεις για το τρόπο εκτέλεσης των προσομοιώσεων, αλλά και τη χρήση των νέων στοιχείων, σε επίπεδο κώδικα, που περιέχονται σε αυτό το νέο άρθρωμα του ns-3.

4.3. Επιλογή Υλοποίησης Network Coding

Για την επιλογή της υλοποίησης και με βάση τα στοιχεία που αναλύθηκαν παραπάνω, δημιουργήθηκε ο συγκεντρωτικός πίνακας των χαρακτηριστικών των παραπάνω υλοποιήσεων.

[8] kodo, 2011, http://steinwurf.com/products/kodo.html

Κριτήρια	NC impl.	yanci	kodo
Εγκατάσταση	Δύσκολη	Αδύνατη	Εύκολη
Τεκμηρίωση	Μέτρια	Σχεδόν μηδαμινή	Πλήρης τόσο για την εγκατάσταση όσο και για τη χρήση
Λοιπά	Αναξιόπιστο, ημιτελές και μη συντηρημένο	Περιορισμένο εύρος χρήσης όχι RLNC	Συνεχής συντήρηση και εμπορική διάθεση

Πίνακας 5 Χαρακτηριστικά εργαλείων

Κανένα από τα παραπάνω εργαλεία δεν έχει σχεδιαστεί με στόχο την ασφάλεια δικτύων και την προώθηση της σχετικής έρευνας. Το kodo είναι πιο κοντά στα κριτήρια που θέσαμε. Επομένως από τις τρεις διαθέσιμες υλοποιήσεις, επιλέξαμε το kodo, καθώς είναι το πιο ολοκληρωμένο, με αρκετή τεκμηρίωση και παρουσία σε αρκετές ερευνητικές μελέτες.

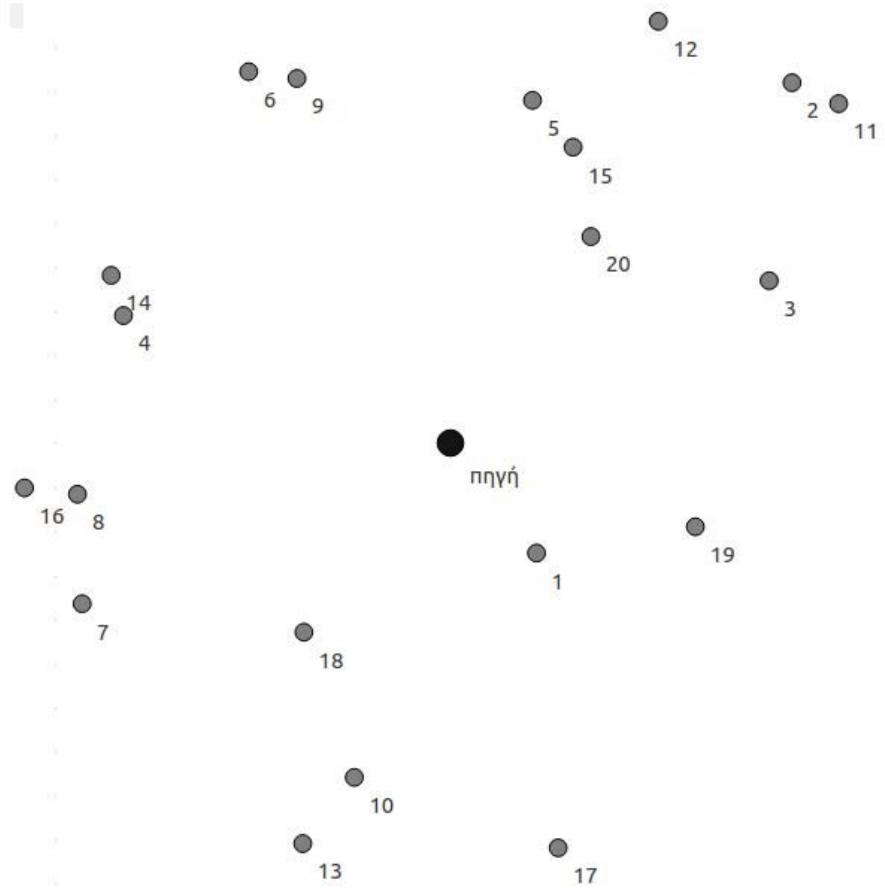
4.4. Σενάρια

Αξιολογήσαμε τα σενάρια επιθέσεων που αναλύθηκαν στο προηγούμενο κεφάλαιο, ως προς τη δυνατότητα προσομοίωσης στην πλατφόρμα και υλοποίηση RLNC που επιλέχθηκε. Τα ιδιαίτερα χαρακτηριστικά των επιθέσεων, ως προς την πολυπλοκότητα του σεναρίου εφαρμογής και επίδειξης, σε συνδυασμό με τα διαθέσιμα χαρακτηριστικά της υλοποίησης του RLNC, οδήγησαν στην επιλογή τεσσάρων σεναρίων, τα οποία μελετήθηκαν εκτενέστερα στο πλαίσιο της παρούσας μεταπτυχιακής διατριβής και παρουσιάζονται στις επόμενες ενότητες.

4.4.1. Ασύρματη Ευρυεκπομπή

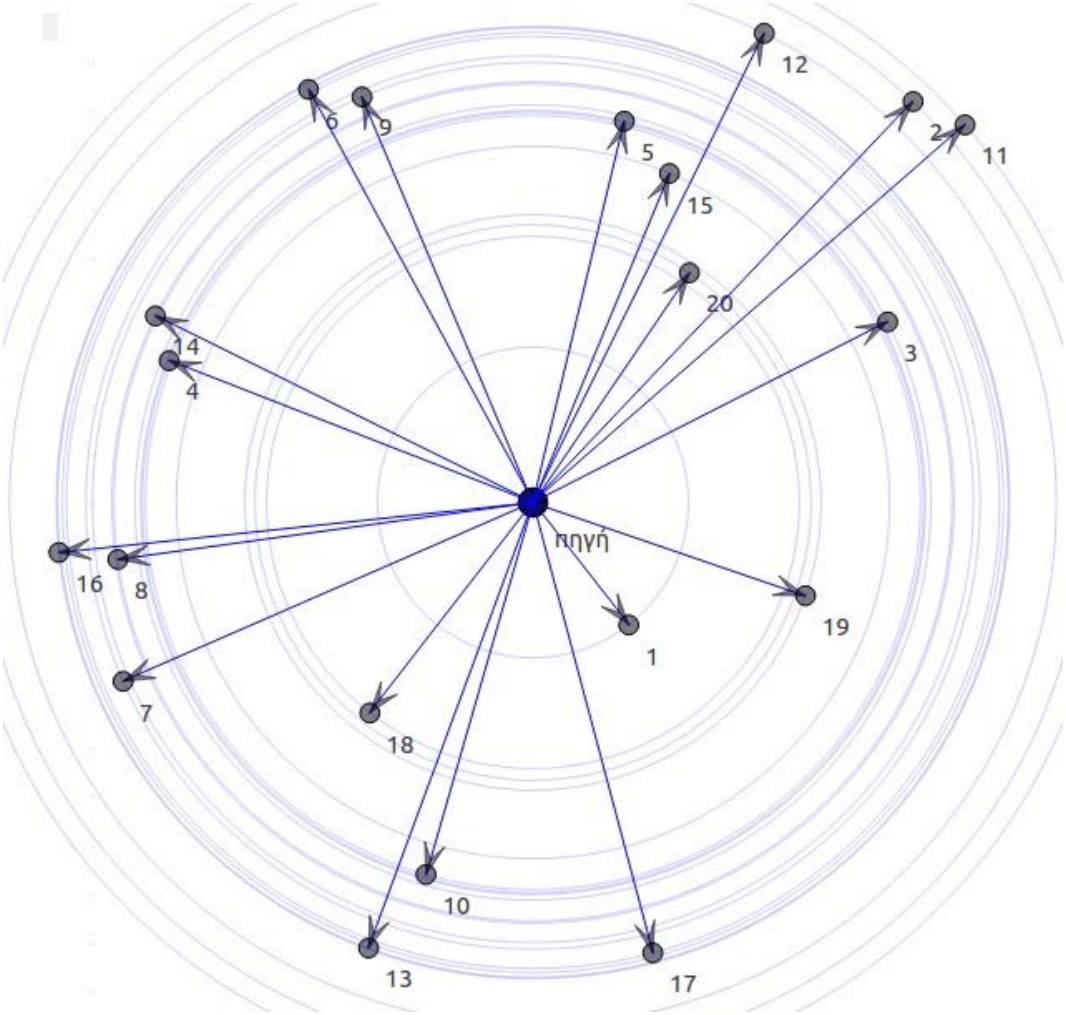
Μια πηγή στέλνει πακέτα μέσω ενός ασύρματου καναλιού IEEE 802.11b σε N παραλήπτες εντός της εμβέλειάς της. Όλοι οι παραλήπτες πρέπει να λάβουν το κάθε πακέτο σε αυτό το σενάριο λειτουργίας. Το δίκτυο δέχεται επίθεση τύπου jamming από κακόβουλους χρήστες με αποτέλεσμα τη σημαντική υποβάθμιση της ποιότητας του καναλιού και τη μείωση της πιθανότητας λήψης κάθε πακέτου από όλους τους

παραλήπτες του, δυσχεραίνοντας την περαιτέρω επικοινωνία και εισάγοντας μεγάλες καθυστερήσεις.



Σχήμα 23 Ενδεικτική τοπολογία δικτύου

Τα πακέτα που στέλνονται είναι κωδικοποιημένα με RLNC σε ένα πεπερασμένο πεδίο F_q μεγέθους q και το μέγεθος της κάθε γενιάς είναι g πακέτα. Η θέση των κόμβων είναι τυχαία και δε λαμβάνεται υπόψη, θεωρείται ότι όλοι οι κόμβοι είναι εντός της εμβέλειας της πηγής.



Σχήμα 24 Ασύρματη ευρυεκπομπή

Το μέγεθος του πεπερασμένου πεδίου μπορεί να πάρει τις τιμές $q = 2^1$ ή 2^4 ή 2^8 , επομένως τα σύμβολα μπορούν να αποτελούνται από $s = 1$ ή 4 ή 8 bit αντίστοιχα. Κάθε πακέτο, για το οποίο μπορεί να καθοριστεί ο αριθμός των bit (για παράδειγμα 1.000) που περιέχει, αποτελείται από L σύμβολα. Η πηγή, για μία συγκεκριμένη γενιά, η οποία αποτελείται από g πακέτα, παράγει και στέλνει μέχρι και n κωδικοποιημένα πακέτα, όπου $n \geq g$ κάθε ένα δευτερόλεπτο.

Μερικά πακέτα δε θα φτάσουν στους παραλήπτες τους, αλλά για να μπορέσει ο κάθε ένας από αυτούς να αποκωδικοποιήσει τα αρχικά πακέτα, θα πρέπει να παραλάβει τουλάχιστον g κωδικοποιημένα πακέτα (διατηρούνται στο buffer του κάθε κόμβου), τα οποία να είναι και γραμμικά ανεξάρτητοι συνδυασμοί των αρχικών. Η πηγή συνεχίζει να στέλνει κωδικοποιημένα πακέτα, μέχρι και οι N παραλήπτες να μπορέσουν να αποκωδικοποιήσουν όλα τα αρχικά πακέτα.

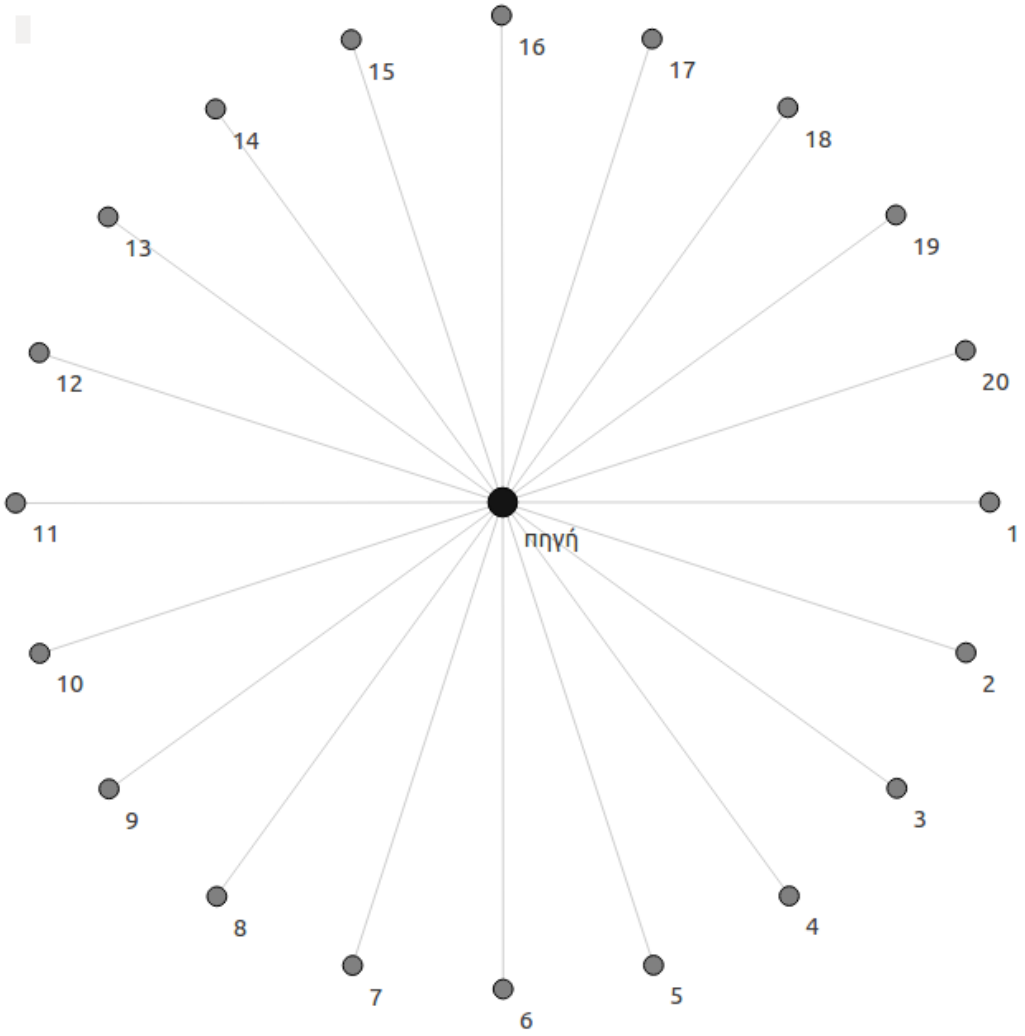
Στο φυσικό επίπεδο (physical layer), το Wi-Fi κανάλι του δικτύου έχει σταθερή ταχύτητα διάδοσης καθυστέρησης (propagation delay speed) και η ισχύς λήψης των παραληπτών (receiver signal strength) είναι επίσης σταθερή. Για το λόγο αυτό δεν επηρεάζεται από την απόστασή τους.

Η προσομοίωση της επίθεσης στο kodo γίνεται εισάγοντας θόρυβο στην επικοινωνία (μείωση του SNR) ή με ένα μοντέλο διάδοσης απωλειών (propagation loss model). Στο επίπεδο ζεύξης (datalink layer) χρησιμοποιήθηκαν οι προκαθορισμένες παράμετροι ad hoc MAC για ασύρματο (Wi-Fi) δίκτυο. Στο επίπεδο δικτύου (network layer) ορίστηκε το πρωτόκολλο IPv4 και στο επίπεδο μεταφοράς (transport layer) το πρωτόκολλο UDP. Η δρομολόγηση καθορίστηκε ως στατική (static routing), η απλούστερη επιλογή με προϋπολογισμό των πινάκων δρομολόγησης. Τέλος η πληροφόρηση για τον αριθμό των καινοτόμων πακέτων που έχει παραλάβει η πηγή δεν υλοποιείται, αλλά για λόγους απλότητας θεωρείται ότι είναι αυτόματα διαθέσιμη στην πηγή.

Για τη σύγκριση των αποτελεσμάτων υλοποιήθηκε το ίδιο δίκτυο χωρίς κωδικοποίηση δικτύου, αλλά με την ίδια λογική. Πιο συγκεκριμένα κάθε πακέτο, από τα g μοναδικά που αποστέλλονται (στο σύνολο $n \geq g$), αριθμείται και κάθε παραλήπτης καταγράφει ποιά πακέτα έχει παραλάβει. Για την ολοκλήρωση της προσομοίωσης πρέπει κάθε παραλήπτης να έχει να λάβει κάθε αριθμημένο πακέτο τουλάχιστον μία φορά. Έτσι μετά την αποστολή του i-οστού πακέτου, αν έστω και ένας παραλήπτης δεν το έχει παραλάβει, η αποστολή του επαναλαμβάνεται όσες φορές χρειαστεί, ώστε τελικά να το έχουν λάβει και οι N παραλήπτες τουλάχιστον μία φορά. Ο αριθμός των αποστολών που απαιτήθηκαν είναι το συγκριτικό χαρακτηριστικό ανάμεσα στις προσομοιώσεις.

4.4.2. Ενσύρματη Ευρυεκπομπή

Μια πηγή στέλνει σε N παραλήπτες μέσω ενός ενσύρματου δικτύου αστέρα (star network), που δέχεται επίθεση από κακόβουλους χρήστες με αποτέλεσμα τη σημαντική υποβάθμισή του και τη μείωση της πιθανότητας λήψης πακέτων από τους παραλήπτες. Η προσομοίωση της επίθεσης γίνεται με την αύξηση του ρυθμού διαγραφής (erasure rate), που καταδεικνύει τις απώλειες πακέτων.

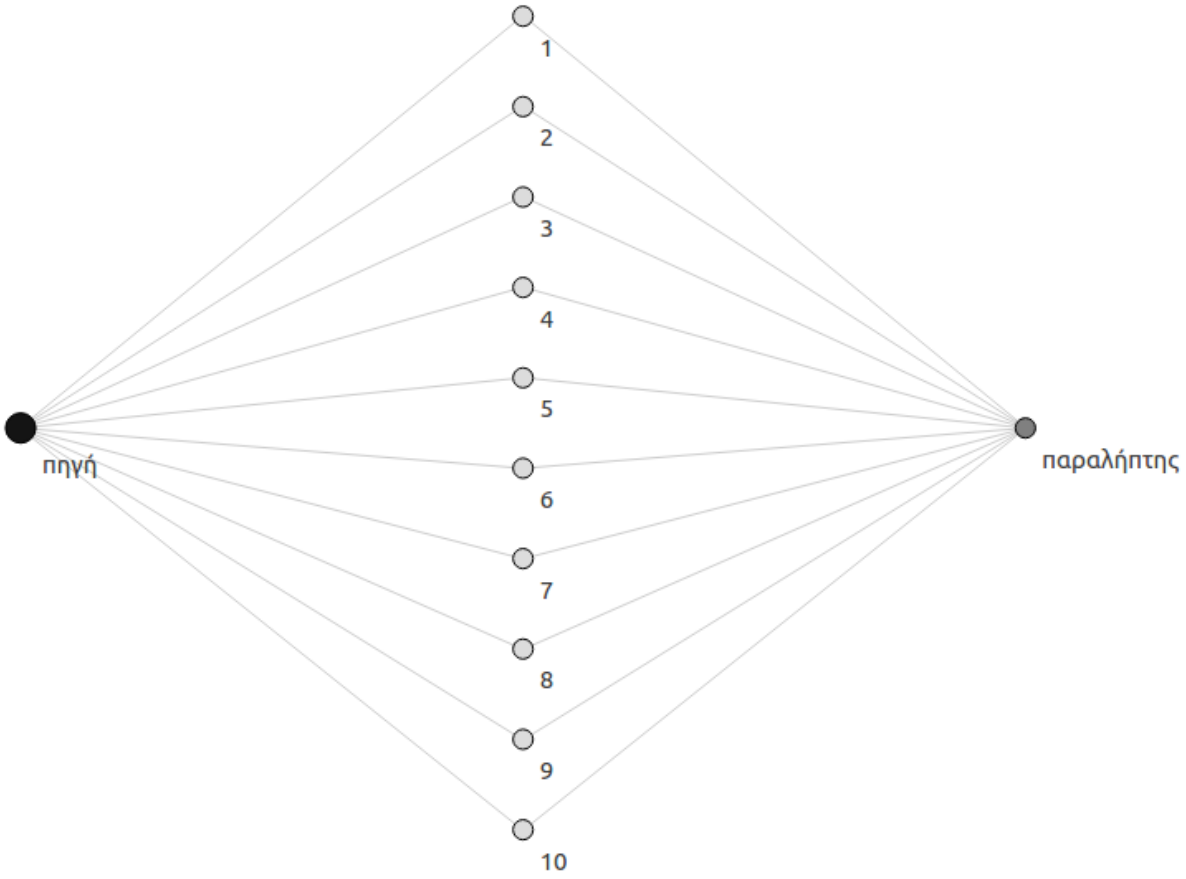


Σχήμα 25 Ενσύρματη ευρυεκπομπή

Στο φυσικό επίπεδο ορίστηκε ένα δίκτυο αστέρα με την πηγή στο κέντρο, που στέλνει πακέτα κάθε ένα δευτερόλεπτο και ένα καθορισμένο ρυθμό διαγραφής πακέτων. Στο επίπεδο δικτύου (network layer) έχει οριστεί το πρωτόκολλο IPv4, στο επίπεδο μεταφοράς (transport layer) το πρωτόκολλο UDP και η δρομολόγηση έχει καθοριστεί ως στατική (static routing). Τα χαρακτηριστικά της κωδικοποίησης παραμένουν τα ίδια με το προηγούμενο σενάριο, δηλαδή πεπερασμένο πεδίο μεγέθους $q = 2^1$ ή 2^4 ή 2^8 και κάθε πακέτο αποτελείται από 1.000 bit.

4.4.3. Two-hop με Παράλληλα Μονοπάτια

Σε αυτό το σενάριο μια πηγή στέλνει κωδικοποιημένα πακέτα ταυτόχρονα σε N αναμεταδότες οι οποίοι με τη σειρά τους στέλνουν τα πακέτα (με επανακωδικοποίηση ή όχι) σε έναν τελικό παραλήπτη.



Σχήμα 26 Two-hop με παράλληλα μονοπάτια

Η πηγή στέλνει τη γενιά έως ότου όλοι οι αναμεταδότες να έχουν g γραμμικώς ανεξάρτητα κωδικοποιημένα πακέτα. Πακέτα μπορεί να χαθούν λόγω της επίθεσης που δέχεται το δίκτυο. Η επίθεση προσομοιώνεται με τον ορισμό ενός ρυθμού απώλειας των πακέτων, ο οποίος είναι ο ίδιος παντού. Στη συνέχεια οι αναμεταδότες στέλνουν, με την καθυστέρηση ενός δευτερολέπτου, τυχαία ένα από τα πακέτα που έχουν καταχωρισμένα στη μνήμη τους στον τελικό παραλήπτη ή στην περίπτωση επανα-κωδικοποίησης, παράγουν και στέλνουν κάθε φορά ένα νέο κωδικοποιημένο συνδυασμό των διαθέσιμων πακέτων.

Το πρώτο τμήμα του δικτύου είναι ένα δίκτυο αστέρα, όπου γίνεται ευρυεκπομπή του ίδιου, για όλους τους ενδιάμεσους κόμβους, κωδικοποιημένο πακέτου (παρόμοια με τα προηγούμενα δύο σενάρια). Το δεύτερο τμήμα είναι ζεύγη σημείο-προς-σημείο (point-to-point) συνδέσεων του κάθε κόμβου με τον παραλήπτη. Το πρωτόκολλο που χρησιμοποιείται είναι το UDP/IPv4 με την προφανή από το Σχήμα 26 στατική δρομολόγηση.

4.4.4. Multi-hop με Επανεκπομπή

Σε αυτό το σενάριο μια πηγή στέλνει κωδικοποιημένα πακέτα στον παραλήπτη μέσα από N κόμβους στη σειρά. Κάθε ενδιάμεσος κόμβος στέλνει τα πακέτα που λαμβάνει με επανα-κωδικοποίηση ή χωρίς, στον επόμενο κόμβο, μέχρι να φτάσουν στον τελικό παραλήπτη.

Σχήμα 27 Multi-hop

Η πηγή στέλνει τα κωδικοποιημένα πακέτα της γενιάς, κάθε ένα δευτερόλεπτο, όπως και οι αναμεταδότες (με μια καθυστέρηση μισού δευτερολέπτου) έως ότου ο παραλήπτης να έχει g γραμμικώς ανεξάρτητα κωδικοποιημένα πακέτα και να μπορέσει να αποκωδικοποιήσει τα αρχικά πακέτα.

Πακέτα μπορεί να χαθούν λόγω της επίθεσης που δέχεται το δίκτυο. Η επίθεση προσομοιώνεται στο kodo με τον ορισμό ενός ρυθμού απώλειας των πακέτων, ο οποίος είναι ο ίδιος παντού. Οι συνδέσεις μεταξύ των κόμβων είναι σημείο-προς-σημείο (point-to-point) και οι ενδιάμεσοι κόμβοι είτε στέλνουν τυχαία ένα από τα πακέτα που έχουν καταχωρισμένα στη μνήμη τους ή, στην περίπτωση επανα-κωδικοποίησης, παράγουν και στέλνουν κάθε φορά ένα νέο κωδικοποιημένο συνδυασμό των πακέτων αυτών. Και εδώ χρησιμοποιείται UDP/IPv4.

Κεφάλαιο 5
Ανάλυση Αποτελεσμάτων

5.1. Αποτελέσματα Προσομοιώσεων

Σε όλες τις προσομοιώσεις που πραγματοποιήθηκαν για τη μελέτη των σεναρίων που αναφέρονται στο προηγούμενο κεφάλαιο, έγινε συλλογή αποτελεσμάτων για την κατάδειξη της επίδρασης των διαφορετικών παραμέτρων σε κάθε περίπτωση. Για κάθε τέτοιο σύνολο παραμέτρων πραγματοποιήθηκαν 50 επαναλήψεις, ώστε να εξαλειφθούν τυχαία φαινόμενα ή απλά να δοθεί μία πιο ολοκληρωμένη εικόνα. Τα στοιχεία που εισάγουν τυχαιότητα είναι:

- η τυχαία επιλογή των συντελεστών στο RLNC
- οι απώλειες των πακέτων, οι οποίες καθορίζονται από ένα ρυθμό σφαλμάτων ή την προσθήκη θορύβου, αλλά σε κάθε εκτέλεση είναι διαφορετικές για διαφορετικό "run" (ή και "seed").

Στη συνέχεια ακολουθούν τα αποτελέσματα για κάθε σενάριο.

5.2. Σενάρια Ευρυεκπομπής

Υλοποιήθηκαν δύο διαφορετικά δίκτυα, ένα ασύρματο και ένα ενσύρματο, όπως αυτά αναλύθηκαν στο προηγούμενο κεφάλαιο.

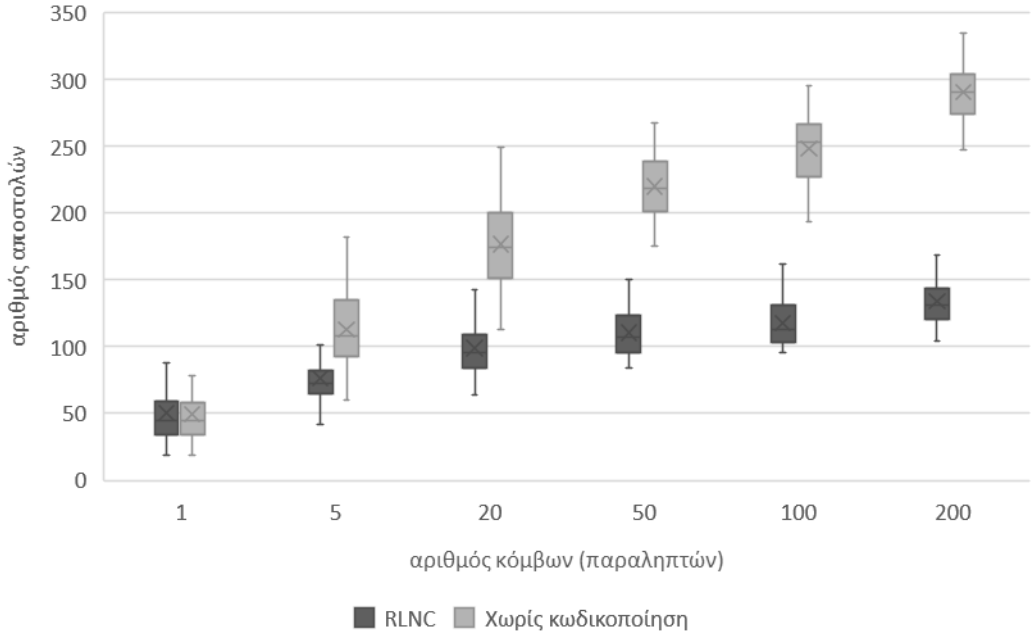
5.2.1. Σενάριο Ασύρματης Ευρυεκπομπής

Για το ασύρματο δίκτυο έγιναν αρχικά δοκιμές για μεταβλητό αριθμό παραληπτών. Ο Πίνακας 6 συνοψίζει τις παραμέτρους που χρησιμοποιήθηκαν.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός κόμβων (παραληπτών)	1, 5, 20, 50, 100, 200
Ποσοστό απωλειών	90%

Πίνακας 6 Παράμετροι για διαφορετικό πλήθος παραληπτών

Τα αποτελέσματα συνοψίζονται στο Διάγραμμα 1 (Box and Whisker). Στον οριζόντιο άξονα αποτυπώνεται ο αριθμός των παραληπτών. Για κάθε τιμή του (1,5,20,…) καταγράφεται ο συνολικός αριθμός αποστολών που χρειάστηκαν, για κάθε ένα από τα είδη της προσομοίωσης: με RLNC και χωρίς καμία κωδικοποίηση.



Διάγραμμα 1 Ασύρματη ευρυεκπομπή για διαφορετικό πλήθος παραληπτών

Όσο μεγαλώνει το πλήθος των παραληπτών τόσο πιο δύσκολο είναι να φτάσουν όλα τα πακέτα της γενιάς (πέντε στη συγκεκριμένη περίπτωση) σε όλους τους παραλήπτες, με αποτέλεσμα να μεγαλώνει πολύ ο αριθμός των αποστολών που χρειάζονται. Με τη χρήση του RLNC αρκεί οποιαδήποτε πέντε γραμμικά ανεξάρτητα κωδικοποιημένα πακέτα να φτάσουν σε όλους τους παραλήπτες. Έτσι ο αριθμός των αποστολών που χρειάζονται διατηρείται σε χαμηλότερα επίπεδα. Συνεπώς, ακόμη και σε ένα ιδιαίτερα εχθρικό περιβάλλον λειτουργίας, το RLNC επιτυγχάνει μικρότερες καθυστερήσεις στην επικοινωνία, επιτρέποντας σε μεγαλύτερο πλήθος πακέτων να φτάσουν σε όλους τους παραλήπτες, με σημαντικά λιγότερες εκπομπές. Το τελευταίο σημείο μπορεί να βελτιώσει σημαντικά τη διάρκεια ζωής του ασύρματου δικτύου και την ανθεκτικότητά

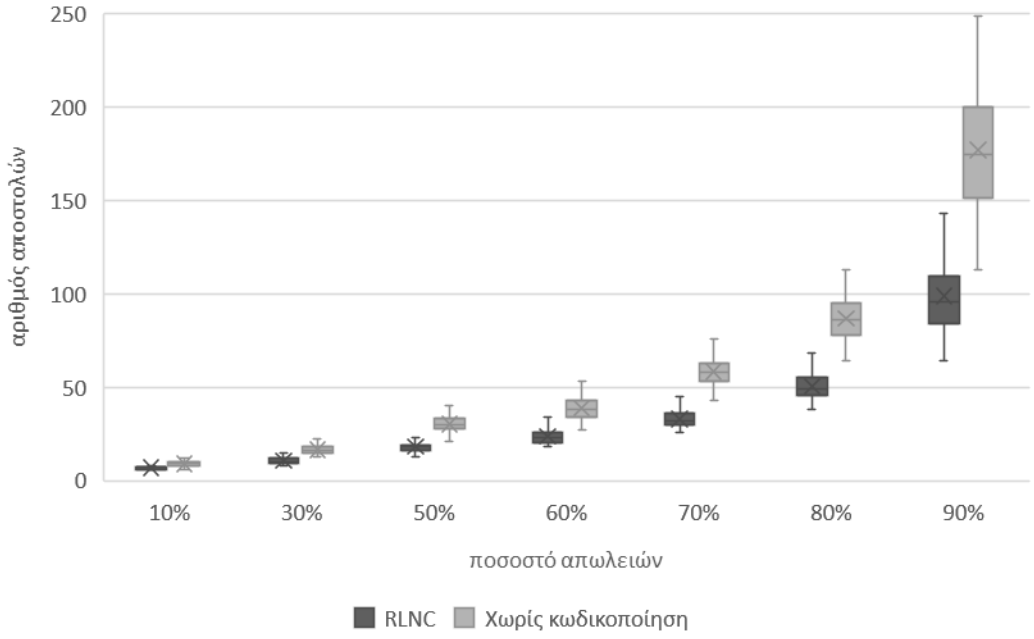
του, ειδικά έναντι επιθέσεων εξάντλησης των ενεργειακών του πόρων (battery depletion attacks).

Στη συνέχεια ακολουθούν δοκιμές όπου μεταβάλλεται το ποσοστό των απωλειών, με τα χαρακτηριστικά που καταγράφονται στον Πίνακας 7.

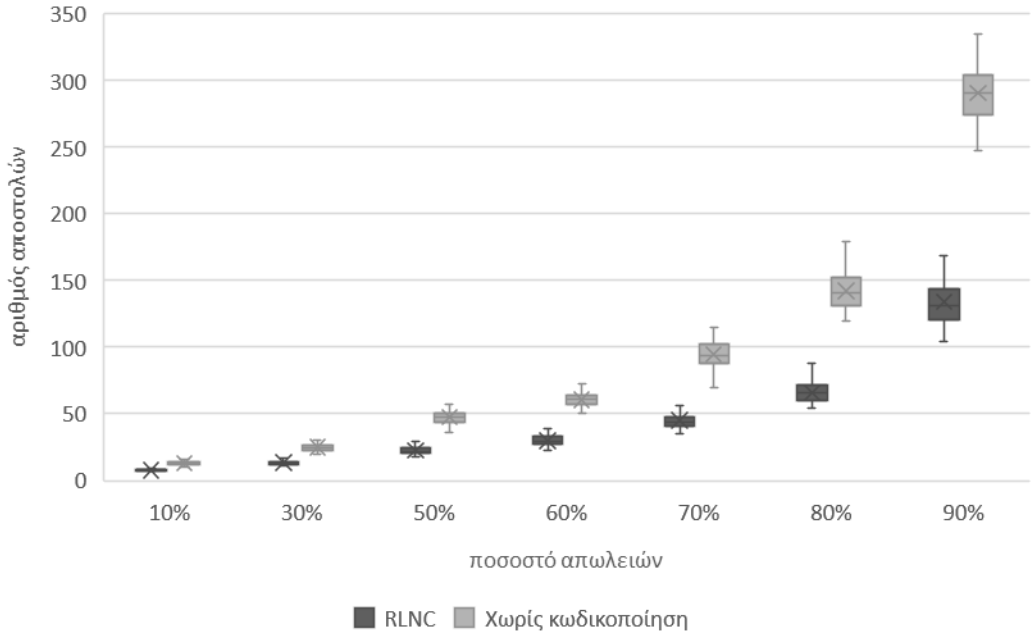
Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός κόμβων (παραληπτών)	20 ή 200
Ποσοστό απωλειών	10%, 30%, 50%, 60%, 70%, 80%, 90%

Πίνακας 7 Παράμετροι για διαφορετικά ποσοστά απωλειών

Τα αποτελέσματα συνοψίζονται στο Διάγραμμα 2 και Διάγραμμα 3 για τις δύο περιπτώσεις 20 και 200 παραληπτών.



Διάγραμμα 2 Ασύρματη ευρυεκπομπή για διαφορετικά ποσοστά απωλειών (N=20)



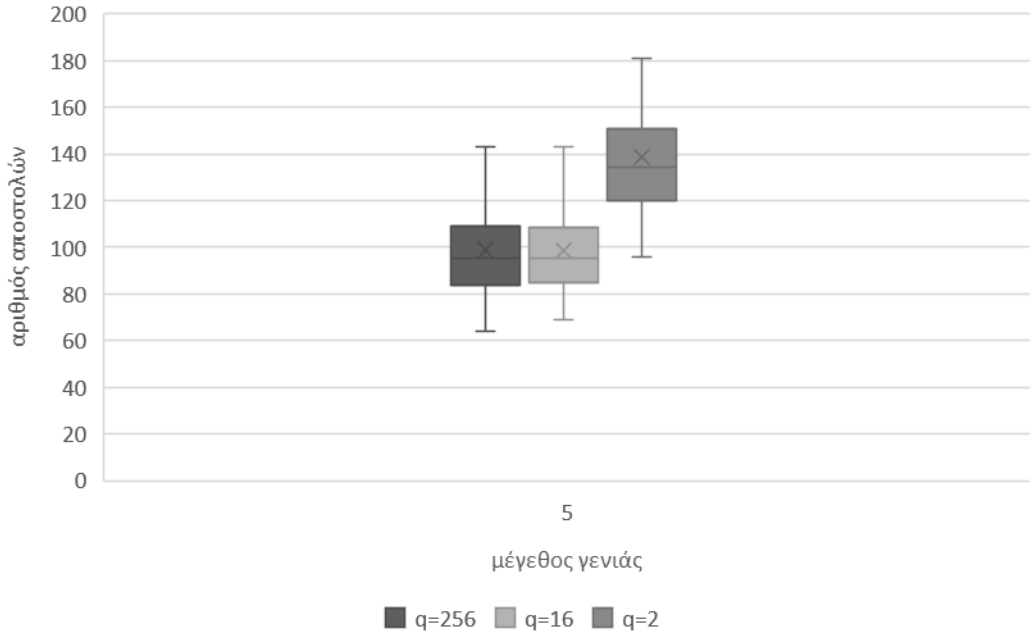
Διάγραμμα 3 Ασύρματη ευρυεκπομπή για διαφορετικά ποσοστά απωλειών (N=200)

Παρατηρούμε ότι η διαφορά στη χρήση ή μη του RLNC είναι υπαρκτή αλλά μικρή όσο το ποσοστό απωλειών είναι μικρό. Τα οφέλη του RLNC γίνονται αισθητά όσο αυξάνει το ποσοστό απωλειών και μάλιστα συνδυαστικά με την αύξηση του πλήθους των παραληπτών.

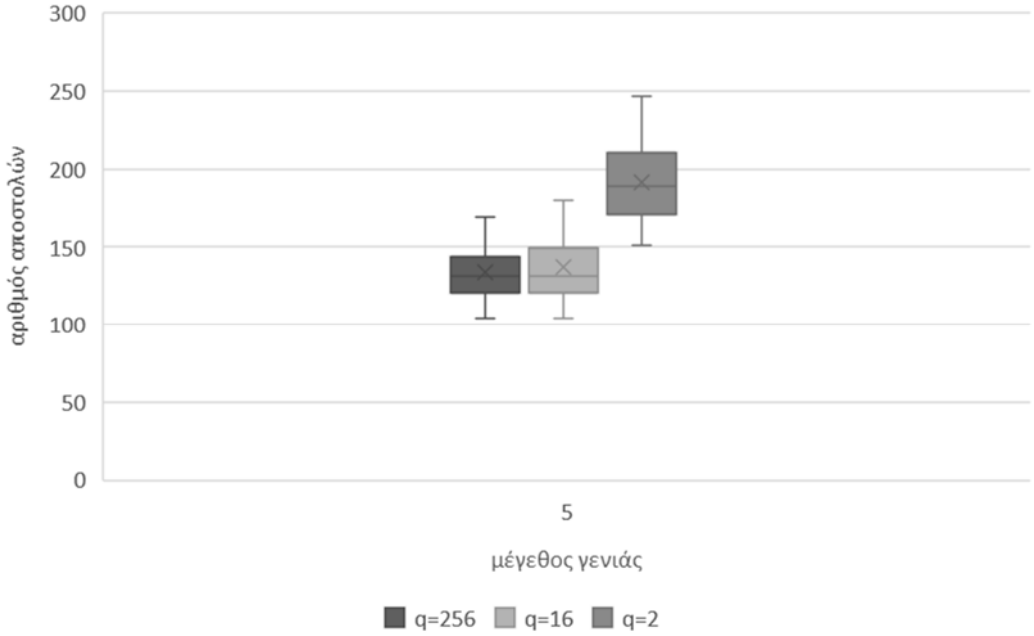
Ένα άλλο σημείο ενδιαφέροντος είναι η επίδραση του μεγέθους του πεπερασμένου πεδίου q. Οι παράμετροι των σχετικών πειραμάτων συνοψίζονται στον Πίνακας 8.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός κόμβων (παραληπτών)	20 ή 200
Ποσοστό απωλειών	90%
Μέγεθος πεδίου	$q = 2^1$ (2) ή 2^4 (16) ή 2^8 (256)

Πίνακας 8 Παράμετροι για διαφορετικά μεγέθη πεδίου



Διάγραμμα 4 Ασύρματη ευρυεκπομπή για διαφορετικά μεγέθη πεδίου (N=20)



Διάγραμμα 5 Ασύρματη ευρυεκπομπή για διαφορετικά μεγέθη πεδίου (N=200)

Το Διάγραμμα 4 και το Διάγραμμα 5 συνοψίζουν τα αποτελέσματα των προσομοιώσεων. Δεν υπάρχει ουσιαστική διαφορά ανάμεσα στα μεγέθη $q = 2^8$ (256) και $q = 2^4$ (16) , καθώς τα 8 και 4 bit αντίστοιχα είναι ικανά να παράξουν το ίδιο πλήθος γραμμικά ανεξάρτητων συνδυασμών. Το μέγεθος όμως πεδίου των 2 bit δεν μπορεί να δώσει την ίδια ποικιλία στους συνδυασμούς, με αποτέλεσμα να υπάρχουν

περισσότερα γραμμικά εξαρτημένα κωδικοποιημένα πακέτα και να χρειάζονται περισσότερες αποστολές καινούργιων.

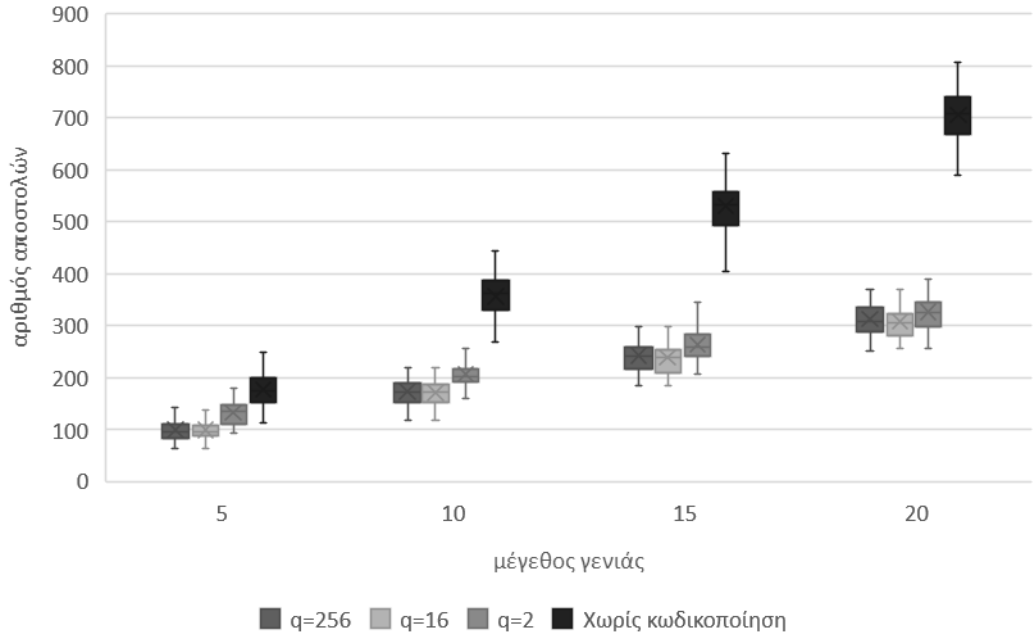
Ως συνέπεια του παραπάνω ευρήματος, στις προσομοιώσεις που ακολουθούν και όπου δεν αναφέρεται ρητώς, θα χρησιμοποιείται το μέγεθος πεπερασμένου πεδίου $q = 2^8$ (256).

Τέλος για το συγκεκριμένο δίκτυο έγινε και συλλογή αποτελεσμάτων για τη μελέτη της επίδρασης του μεγέθους της γενιάς g, όπου συνδυαστικά μεταβάλλεται και το μέγεθος του πεδίου, με σκοπό τη δημιουργία μιας πληρέστερης εικόνας. Οι παράμετροι συνοψίζονται στον Πίνακας 9.

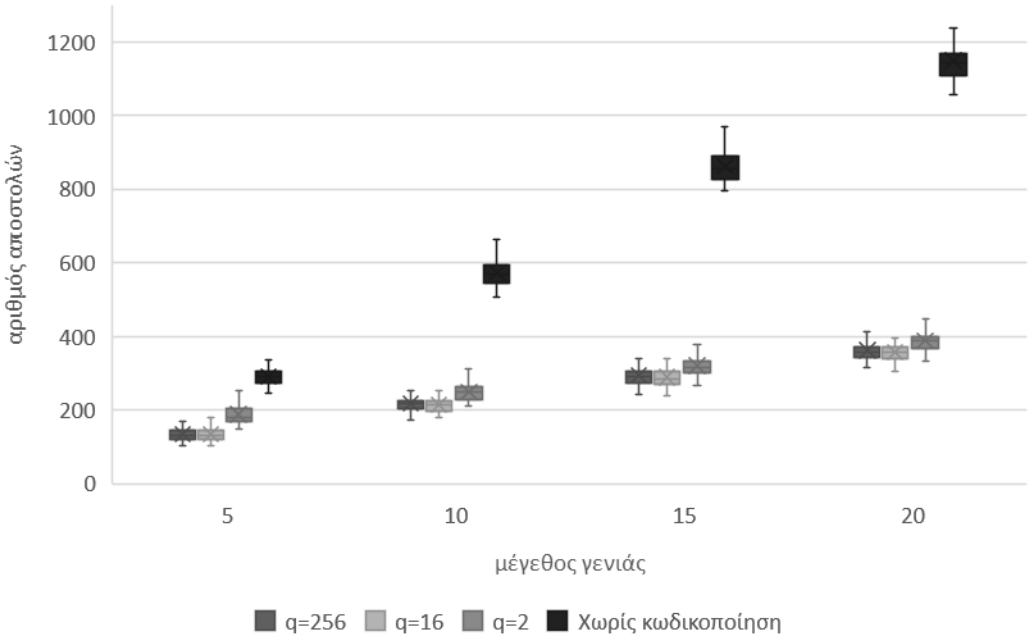
Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5, 10, 15, 20
Αριθμός κόμβων (παραληπτών)	20 ή 200
Ποσοστό απωλειών	90%
Μέγεθος πεδίου	$q = 2^1$ (2) ή 2^4 (16) ή 2^8 (256)

Πίνακας 9 Παράμετροι για διαφορετικά μεγέθη γενιάς και πεδίου

Τα αποτελέσματα για *N*=20 παραλήπτες συνοψίζονται στο Διάγραμμα 6 και ακολούθως για *N*=200 παραλήπτες στο Διάγραμμα 7.



Διάγραμμα 6 Ασύρματη ευρυεκπομπή για διαφορετικά μεγέθη γενιάς (N=20)



Διάγραμμα 7 Ασύρματη ευρυεκπομπή για διαφορετικά μεγέθη γενιάς (N=200)

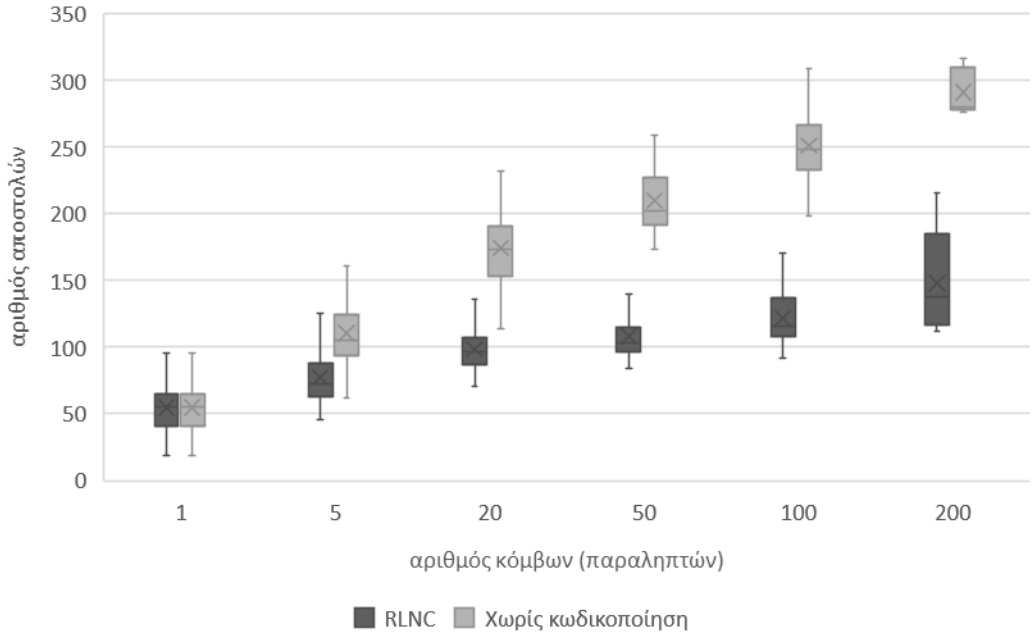
Η επίδραση της μεταβολής του μεγέθους του πεπερασμένου πεδίου είναι όπως έχει αναφερθεί και προηγουμένως. Επιπλέον, ο ρυθμός αύξησης των συνολικών αποστολών που χρειάζονται, ειδικά όσο αυξάνει ο αριθμός των παραληπτών, είναι σημαντικά διαφορετικός με τη μεταβολή του μεγέθους της γενιάς.

5.2.2. Σενάριο Ενσύρματης Ευρυεκπομπής

Ομοίως για το ενσύρματο δίκτυο επαναλαμβάνονται οι ίδιες δοκιμές, με την πρώτη να αφορά στο μεταβλητό αριθμό παραληπτών. Ο Πίνακας 10 συνοψίζει τις παραμέτρους που χρησιμοποιήθηκαν και το Διάγραμμα 8 τα αποτελέσματα των προσομοιώσεων.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός κόμβων (παραληπτών)	1, 5, 20, 50, 100, 200
Ποσοστό απωλειών	90%

Πίνακας 10 Παράμετροι για διαφορετικό πλήθος παραληπτών

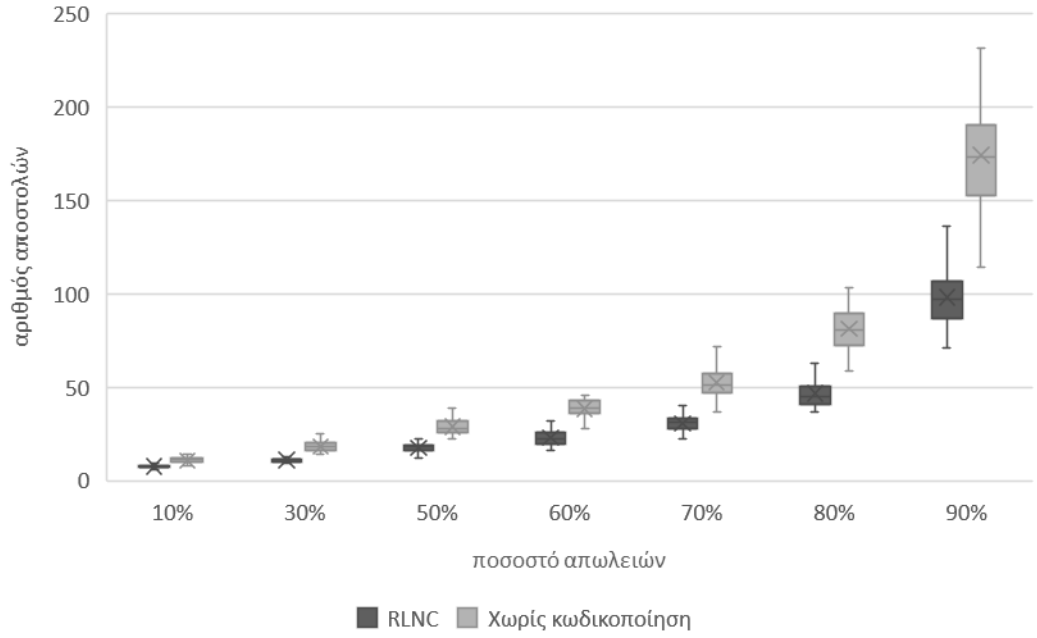


Διάγραμμα 8 Ενσύρματη ευρυεκπομπή για διαφορετικό πλήθος παραληπτών

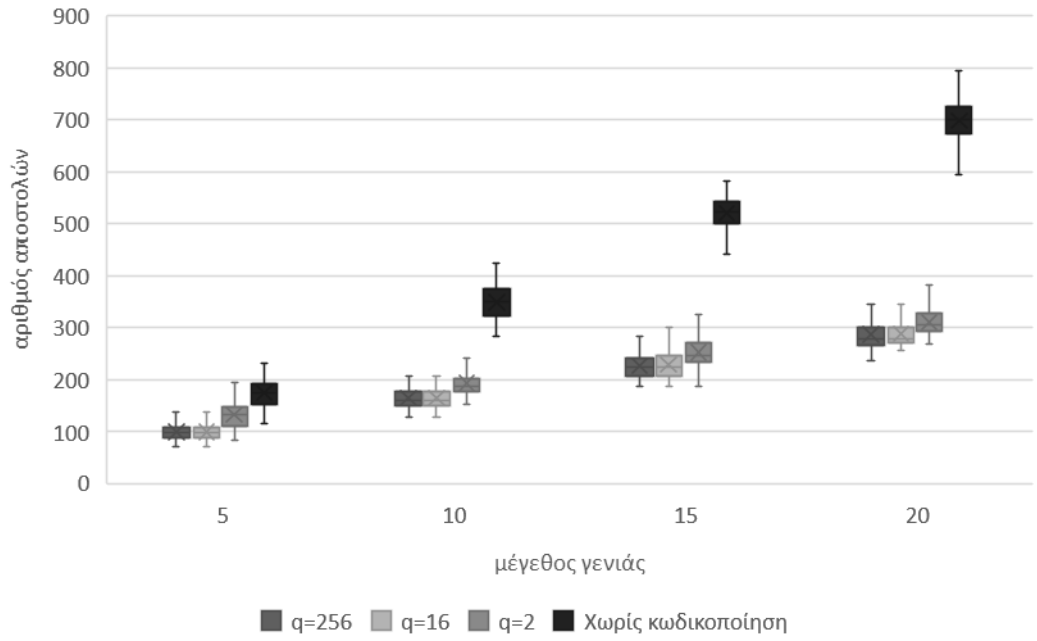
Ακολουθούν τα αποτελέσματα για μεταβλητό αριθμό ποσοστού απωλειών, με βάση τις παραμέτρους που συνοψίζονται στον Πίνακας 11. Το Διάγραμμα 9 συνοψίζει τα αποτελέσματα των προσομοιώσεων για διαφορετικά ποσοστά απωλειών, το Διάγραμμα 10 για συνδυαστικά διαφορετικά μεγέθη πεδίου και γενιάς και το Διάγραμμα 11 για διαφορετικά μεγέθη γενιάς.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός κόμβων (παραληπτών)	20
Ποσοστό απωλειών	10%, 30%, 50%, 60%, 70%, 80%, 90%

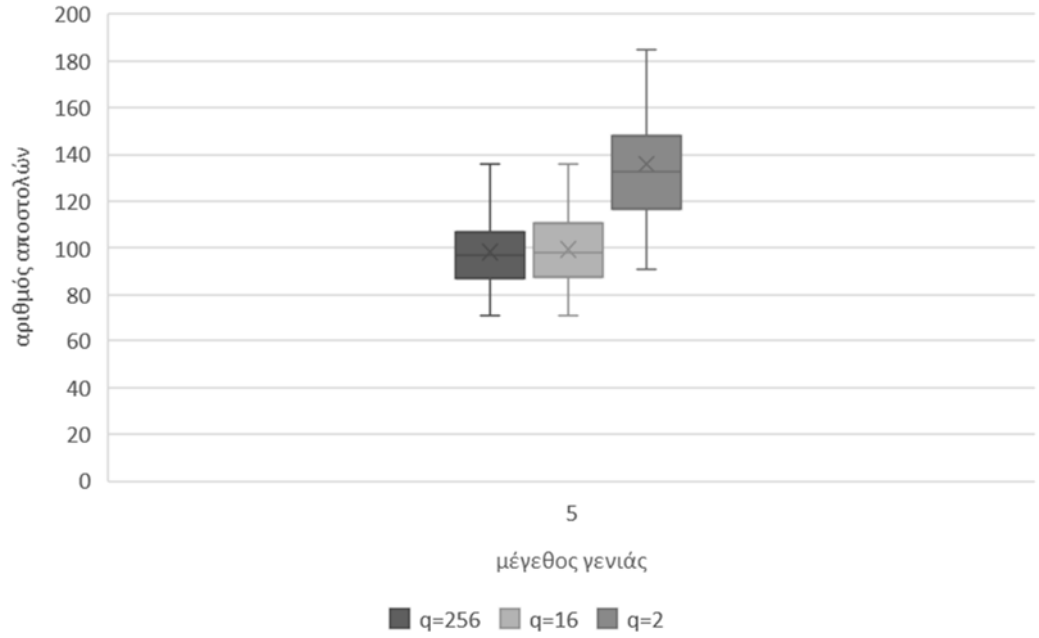
Πίνακας 11 Παράμετροι για διαφορετικά ποσοστά απωλειών



Διάγραμμα 9 Ενσύρματη ευρυεκπομπή για διαφορετικά ποσοστά απωλειών



Διάγραμμα 10 Ενσύρματη ευρυεκπομπή για διαφορετικά μεγέθη πεδίου & γενιάς



Διάγραμμα 11 Ενσύρματη ευρυεκπομπή για διαφορετικά μεγέθη πεδίου

Τα αποτελέσματα είναι παρόμοια με τα αντίστοιχα των προσομοιώσεων για ασύρματο δίκτυο. Συνεπώς, η φύση του δικτύου, ασύρματη ή ενσύρματη, δεν επηρεάζει τα αποτελέσματα των προσομοιώσεων στο kodo.

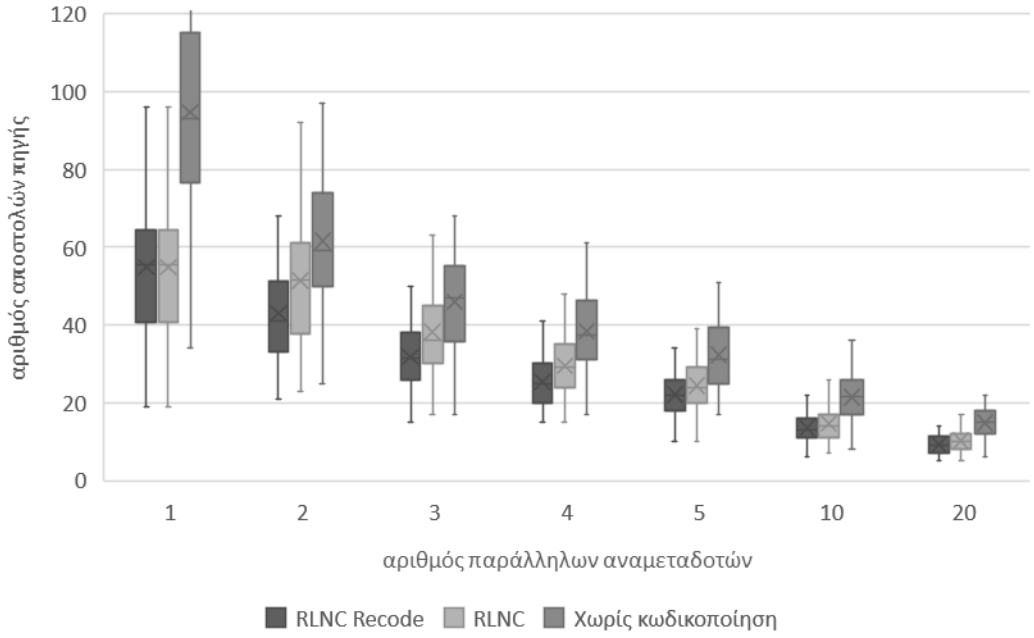
5.3. Σενάριο Two-hop με Παράλληλα Μονοπάτια

Για το σενάριο του δικτύου, όπου η πηγή στέλνει στον έναν και μοναδικό παραλήπτη πακέτα μέσω πολλαπλών παράλληλων μονοπατιών, έγιναν αρχικά δοκιμές και συλλογή αποτελεσμάτων για διαφορετικό πλήθος διαθέσιμων μονοπατιών, δηλαδή των κόμβων που μπορούν ταυτόχρονα και παράλληλα να λαμβάνουν πακέτα από την πηγή και να τα στέλνουν στον παραλήπτη.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός παράλληλων αναμεταδοτών	1, 2, 3, 4, 5, 10, 20
Ποσοστό απωλειών	90%

Πίνακας 12 Παράμετροι για διαφορετικό αριθμό αναμεταδοτών

Εδώ καταγράφονται δύο στοιχεία. Το πρώτο είναι ο αριθμός των αποστολών που χρειάστηκε να κάνει η πηγή.



Διάγραμμα 12 Two-hop, αριθμός αποστολών πηγής για διαφορετικό πλήθος παράλληλων αναμεταδοτών

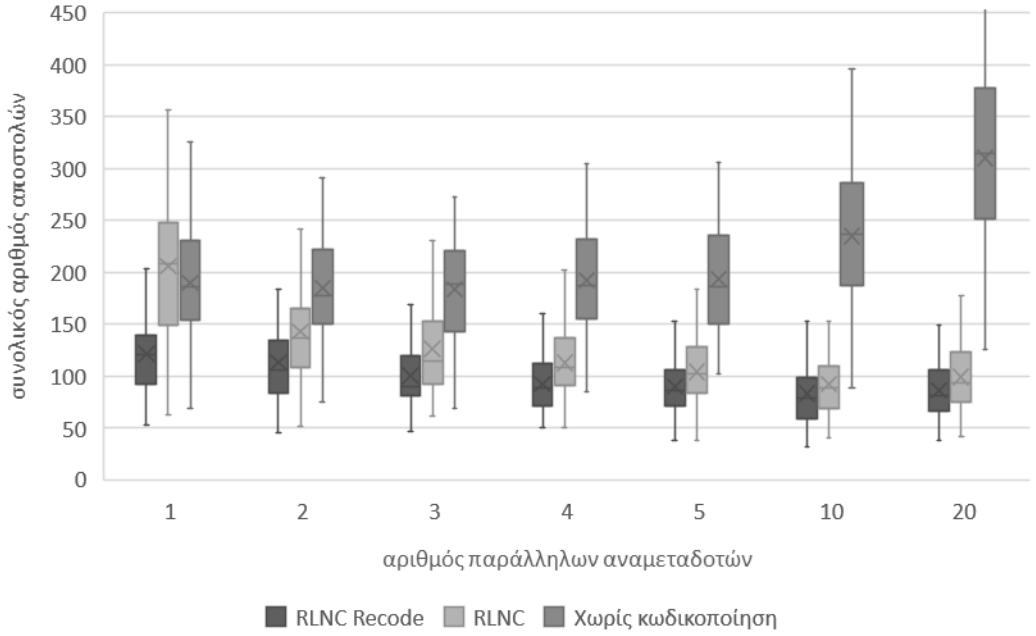
Σε αυτό το σενάριο υπάρχουν τρεις περιπτώσεις: (α) χωρίς κωδικοποίηση, (β) χρήση RLNC από την πηγή και οι υπόλοιποι είναι απλοί αναμεταδότες και (γ) χρήση RLNC αλλά οι υπόλοιποι συμμετέχουν στην κωδικοποίηση, παράγοντας νέα κωδικοποιημένα πακέτα ως γραμμικούς συνδυασμούς όσων έχουν ήδη παραλάβει και διατηρούν στη μνήμη τους.

Όσο αυξάνεται το πλήθος των παράλληλων αναμεταδοτών, τόσο αυξάνεται η πιθανότητα κάποιος από αυτούς που έχει καταφέρει, κάποια στιγμή, να λάβει ένα πακέτο από την πηγή, να μπορέσει επίσης να το στείλει στον παραλήπτη, σε κάποια άλλη ίσως χρονική στιγμή.

Καθώς αυξάνεται το πλήθος αναμεταδοτών, μειώνεται ο αριθμός αποστολών της πηγής που χρειάζεται να πραγματοποιηθούν για την ολοκλήρωση της επικοινωνίας. Μάλιστα με την αύξηση αυτή, μειώνεται η διαφορά ανάμεσα στις περιπτώσεις χρήσης του RLNC και χωρίς κωδικοποίηση. Όμως πάντοτε η χρήση του RLNC και ιδιαίτερα με επανα-κωδικοποίηση δίνει σημαντικά καλύτερα αποτελέσματα. Ακόμα και αν οι αναμεταδότες δε λαμβάνουν κανένα νέο πακέτο, μπορούν να παράξουν νέο κωδικοποιημένο από αυτά που ήδη έχουν, το οποίο μπορεί να είναι καινοτόμο για τον παραλήπτη. Στην περίπτωση του RLNC χωρίς επανα-κωδικοποίηση, είναι καλύτερο οι αναμεταδότες να λαμβάνουν

πακέτα που κατά μεγάλη πιθανότητα είναι καινοτόμα για τον παραλήπτη και να προσπαθούν να τα στείλουν στον παραλήπτη, όποτε αυτό καταστεί δυνατό.

Το δεύτερο στοιχείο που καταγράφεται είναι ο αριθμός του συνόλου των αποστολών που πραγματοποιήθηκαν στο δίκτυο, ώστε ο παραλήπτης να καταφέρει να παραλάβει όλα τα πακέτα, δηλαδή το άθροισμα των αποστολών της πηγής και του κάθε αναμεταδότη.



Διάγραμμα 13 Two-hop, συνολικό αριθμός αποστολών για διαφορετικό πλήθος παράλληλων αναμεταδοτών

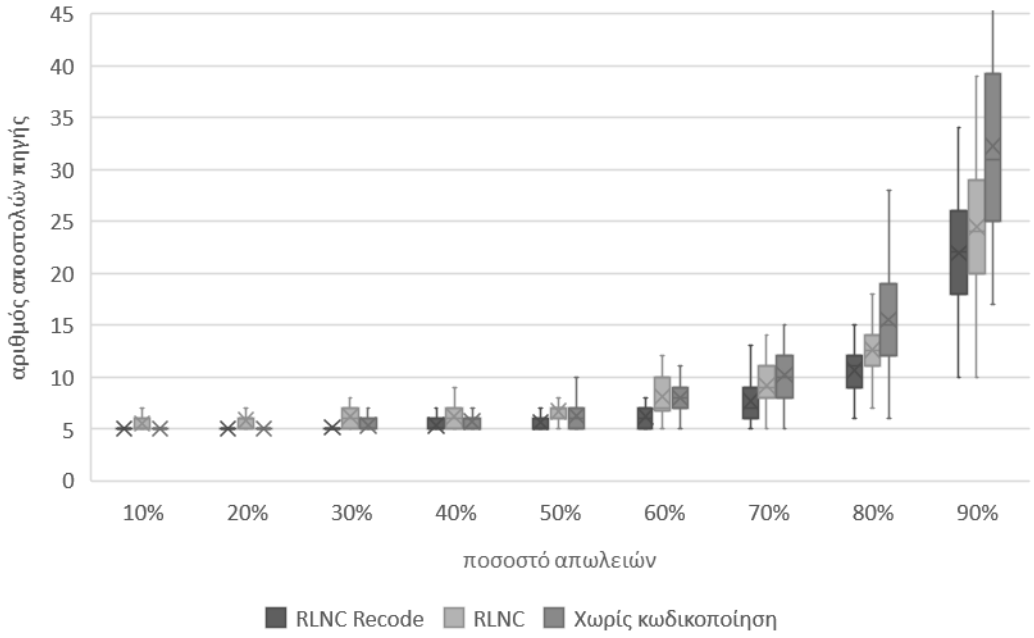
Εδώ είναι αρκετά μεγάλη η διαφορά και μάλιστα όσο αυξάνεται ο αριθμός των αναμεταδοτών, αυξάνεται και το σύνολο των αποστολών για την περίπτωση της μη χρήσης κωδικοποίησης. Αυτό δε συμβαίνει όμως όταν χρησιμοποιείται RLNC. Στην περίπτωση αυτή, με αρκετά μεγάλη πιθανότητα, όποιο πακέτο καταφέρει να σταλεί από αναμεταδότη στον παραλήπτη, είναι και καινοτόμο (ειδικά στην περίπτωση επανα-κωδικοποίησης). Συνεπώς, δεν υπάρχει «σπατάλη» και «φλυαρία» στην επικοινωνία, χωρίς δηλαδή κάποιο όφελος.

Αντίστοιχα πραγματοποιήθηκαν δοκιμές και για διαφορετικά ποσοστά απωλειών. Οι παράμετροι συνοψίζονται στον Πίνακας 13.

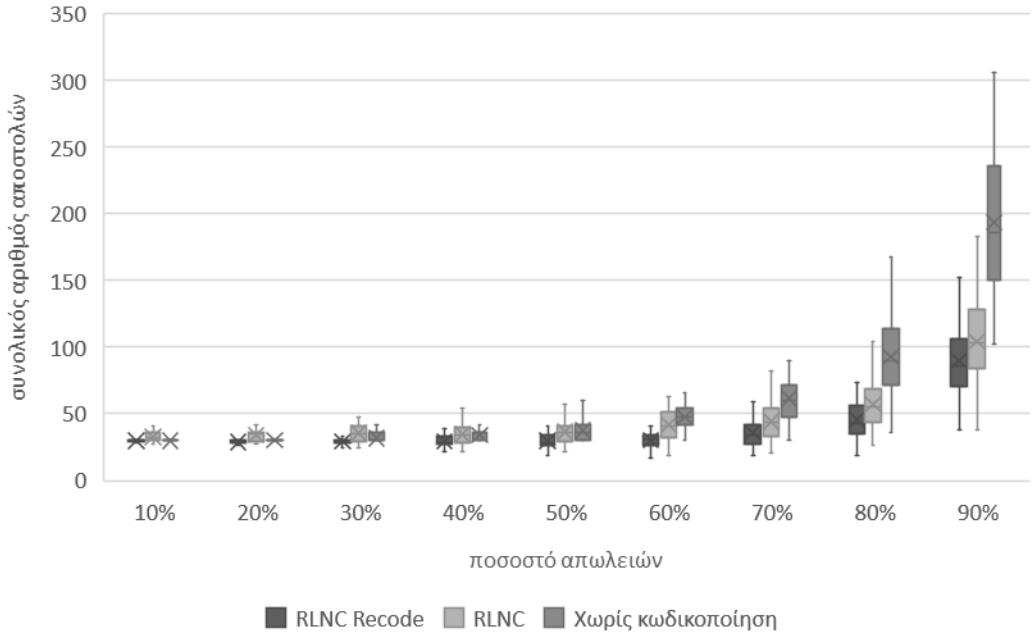
Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός παράλληλων αναμεταδοτών	5
Ποσοστό απωλειών	10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%

Πίνακας 13 Παράμετροι για διαφορετικά ποσοστά απωλειών

Τα αποτελέσματα για την καταγραφή του αριθμού των αποστολών μόνο της πηγής συνοψίζονται στο Διάγραμμα 14 και για το σύνολο των αποστολών στο Διάγραμμα 15.



Διάγραμμα 14 Two-hop, αριθμός αποστολών πηγής για διαφορετικά ποσοστά απωλειών



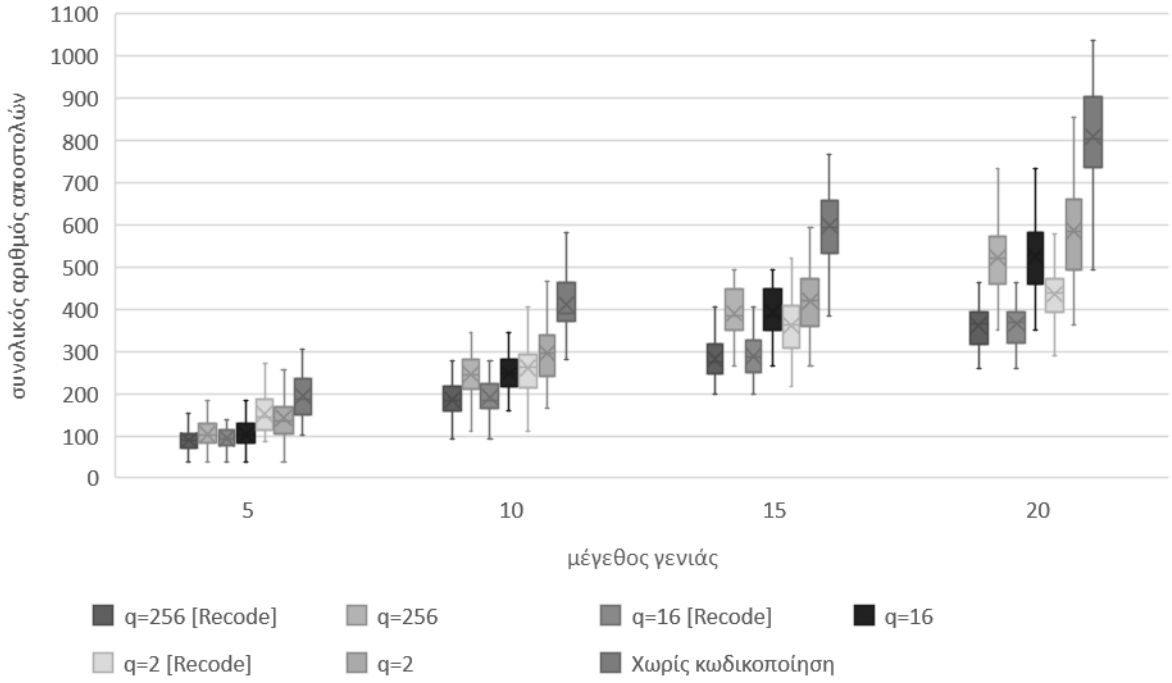
Διάγραμμα 15 Two-hop, αριθμός συνολικών αποστολών για διαφορετικά ποσοστά απωλειών

Δεν υπάρχουν μεγάλες διαφορές όταν οι απώλειες είναι μικρές, καθώς οι πέντε αναμεταδότες είναι ικανοί να παραλάβουν και να στείλουν τα πακέτα στον παραλήπτη. Όταν όμως αυξάνονται οι απώλειες, σε ένα δίκτυο που δέχεται επίθεση, η εφαρμογή του RLNC κρατάει σε χαμηλό επίπεδο τον αριθμό των απαραίτητων αποστολών, παρέχοντας την απαραίτητη ευρωστία και αυξάνοντας τη διάρκεια ζωής του δικτύου.

Η επίδραση του μεγέθους της γενιάς σε συνδυασμό με το μέγεθος του πεδίου συνοψίζεται στο Διάγραμμα 16 με βάση τις παραμέτρους που συνοψίζονται στον Πίνακας 14.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5, 10, 15, 20
Αριθμός παράλληλων αναμεταδοτών	5
Ποσοστό απωλειών	90%
Μέγεθος πεδίου	$q = 2^1$ (2) ή 2^4 (16) ή 2^8 (256)

Πίνακας 14 Παράμετροι για διαφορετικά μεγέθη γενιάς και πεδίου



Διάγραμμα 16 Two-hop για διαφορετικά μεγέθη πεδίου & γενιάς

Η επιλογή μεγέθους πεδίου 2 οδηγεί σε παρόμοια αποτελέσματα, αν και καλύτερα, με αυτά από τη χρήση του RLNC χωρίς επανα-κωδικοποίηση. Μια εξήγηση για αυτό είναι ότι το πλήθος των πακέτων που φτάνουν στους αναμεταδότες είναι πολύ μικρό και οι συνδυασμοί τους, πάνω σε ένα τόσο μικρό πεδίο, δε μπορούν να παράξουν τόσα καινοτόμα πακέτα, όπως αν υπήρχε διαθέσιμο μεγαλύτερο πλήθος πακέτων, το οποίο συμβαίνει στην πηγή. Από την άλλη πλευρά, η εφαρμογή του RLNC χωρίς επανα-κωδικοποίηση αλλά με επιλογή μεγαλύτερου πεδίου, παράγει στην πηγή, σχεδόν πάντα, καινοτόμα πακέτα, που όποτε καταφέρουν να προωθηθούν από τους αναμεταδότες στον παραλήπτη θα αποκωδικοποιηθούν.

Γενικά, με τη χρήση του RLNC χρειάζονται σημαντικά λιγότερες αποστολές, με την περίπτωση της επανα-κωδικοποίησης να είναι η καλύτερη και να ακολουθεί το RLNC χωρίς επανα-κωδικοποίηση.

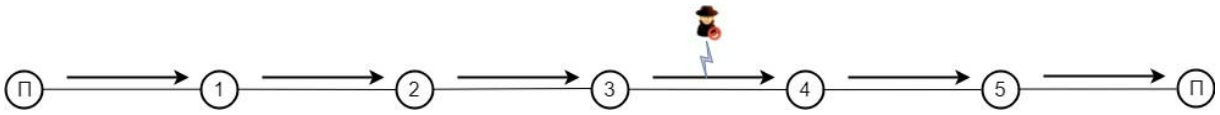
5.4. Σενάριο Multi-hop με Επανεκπομπή

Σε αυτό το σενάριο δικτύου μια πηγή προσπαθεί να επικοινωνήσει με έναν παραλήπτη με τη μεσολάβηση ενδιάμεσων κόμβων που μπορούν να λειτουργούν απλά ως

αναμεταδότες ή να συμμετάσχουν ως επανα-κωδικοποιητές. Διακρίνουμε τρεις περιπτώσεις επίθεσης.

5.4.1. Σενάριο Επίθεσης σε Ένα Σύνδεσμο

Θεωρούμε πέντε ενδιάμεσους κόμβους, όπου ο σύνδεσμος ανάμεσα στον τρίτο και τον τέταρτο δέχεται επίθεση (βλ. Σχήμα 28) με αποτέλεσμα το ποσοστό απωλειών να είναι 90% στο συγκεκριμένο σημείο. Σε όλους τους υπόλοιπους συνδέσμους δεν παρουσιάζεται κανένα πρόβλημα και το ποσοστό απωλειών είναι 0,1%.

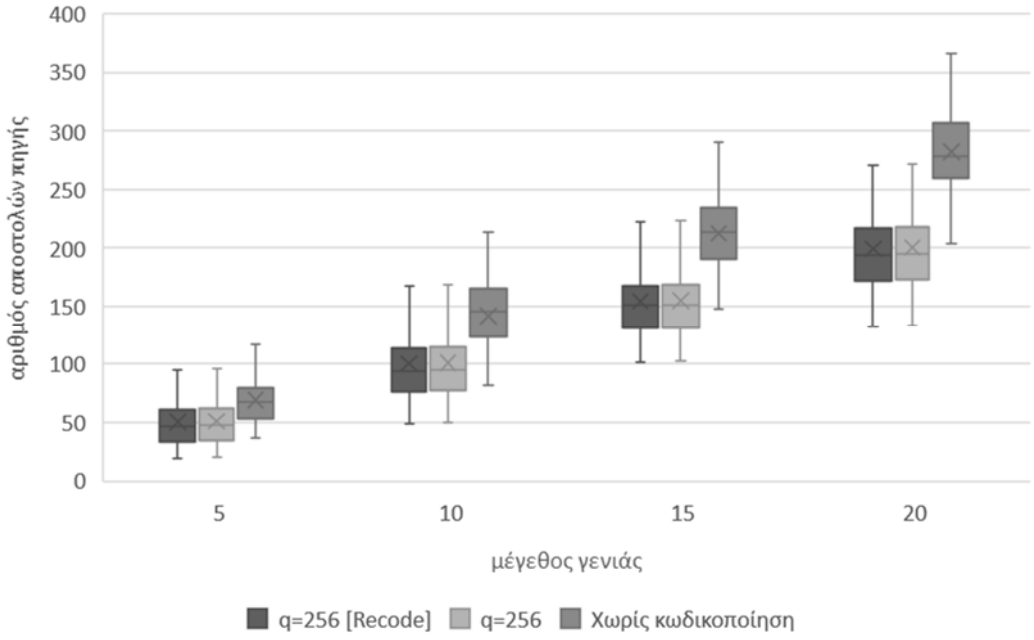


Σχήμα 28 Multi-hop με επίθεση σε ένα σύνδεσμο

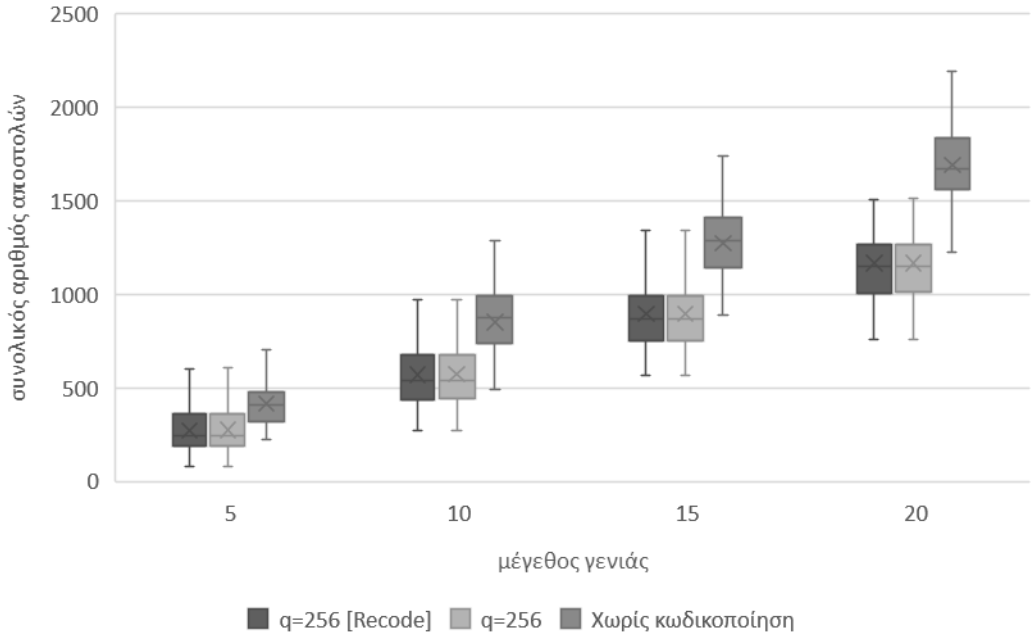
Τα αποτελέσματα της προσομοίωσης για τις παραμέτρους του Πίνακας 15 συνοψίζονται στο Διάγραμμα 17 για τον αριθμό των αποστολών της πηγής και στο Διάγραμμα 18 για το σύνολο της επικοινωνίας.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5, 10, 15, 20
Αριθμός ενδιάμεσων κόμβων	5
Ποσοστό απωλειών	90% σε ένα σημείο και 0.1% στα υπόλοιπα
Μέγεθος πεδίου	$q = 2^8$ (256)

Πίνακας 15 Multi-hop για διαφορετικά μεγέθη γενιάς



Διάγραμμα 17 Multi-hop, αριθμός αποστολών πηγής για διαφορετικά μεγέθη γενιάς



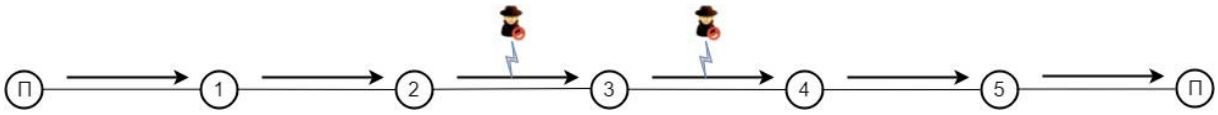
Διάγραμμα 18 Multi-hop, συνολικός αριθμός αποστολών για διαφορετικά μεγέθη γενιάς

Με την κωδικοποίηση δικτύου οποιοδήποτε πακέτο καταφέρει να περάσει από το μοναδικό σημείο επίθεσης, είναι (σχεδόν σίγουρα) καινοτόμο για τον παραλήπτη, καθώς όλα τα κωδικοποιημένα πακέτα που παράγονται από την πηγή κινούνται ελεύθερα στο υπόλοιπο δίκτυο. Για αυτό ακριβώς το λόγο δεν υπάρχει και καμία διαφορά ανάμεσα στη χρήση ή μη των ενδιάμεσων κόμβων ως επανα-κωδικοποιητών.

Αντίθετα, στην περίπτωση της μη χρήσης της κωδικοποίησης δικτύου, ο τρίτος κόμβος προσπαθεί κάθε φορά να προωθήσει το τελευταίο πακέτο που έχει διατηρήσει στη μνήμη του, το οποίο μπορεί να το έχει ξαναστείλει σε αμέσως προηγούμενη στιγμή ή μέχρι και δύο χρονικές περιόδους πίσω.

5.4.2. Σενάριο Επίθεσης σε Δύο Συνδέσμους

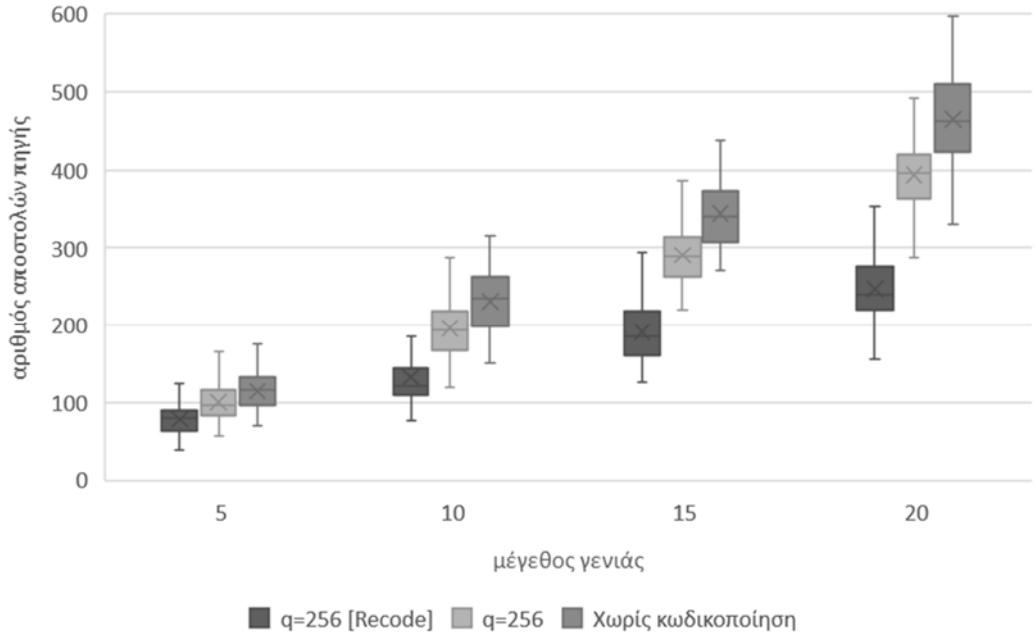
Διευρύνουμε το σενάριο της προηγούμενης επίθεσης, ώστε να συμπεριλάβει και το σύνδεσμο ανάμεσα στο δεύτερο και τρίτο ενδιάμεσο κόμβο. Οι παράμετροι των προσομοιώσεων συνοψίζονται στον Πίνακας 16 και τα αποτελέσματα στο Διάγραμμα 19 και στο Διάγραμμα 20.



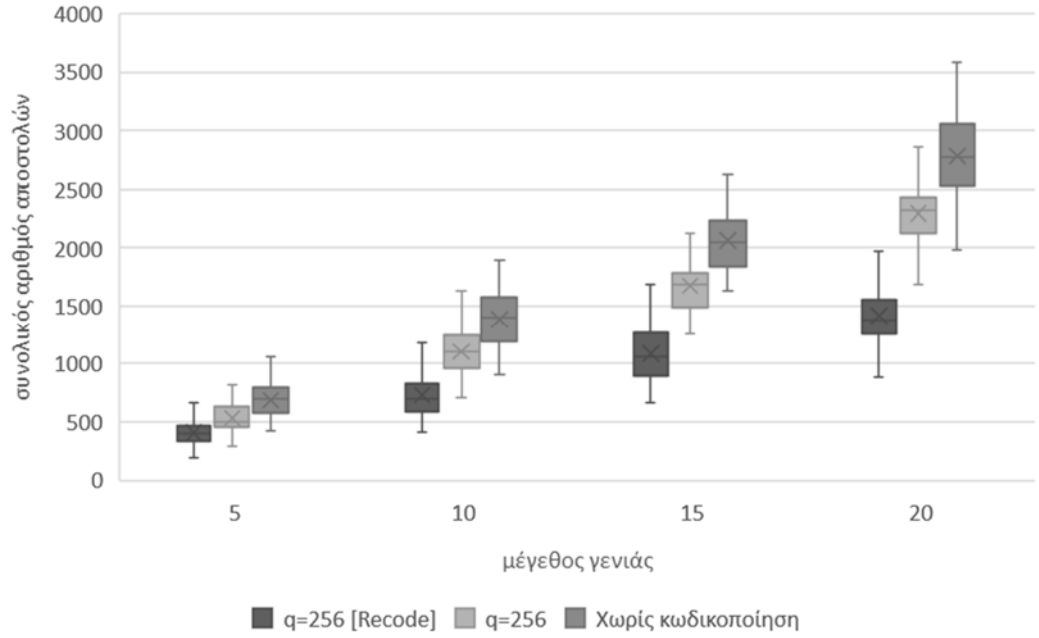
Σχήμα 29 Multi-hop με επίθεση σε δύο συνδέσμους

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5, 10, 15, 20
Αριθμός ενδιάμεσων κόμβων	5
Ποσοστό απωλειών	90% σε δύο σημεία και 0.1% στα υπόλοιπα
Μέγεθος πεδίου	$q = 2^8$ (256)

Πίνακας 16 Multi-hop για διαφορετικά μεγέθη γενιάς



Διάγραμμα 19 Multi-hop, αριθμός αποστολών πηγής για διαφορετικά μεγέθη γενιάς



Διάγραμμα 20 Multi-hop, συνολικός αριθμός αποστολών για διαφορετικά μεγέθη γενιάς

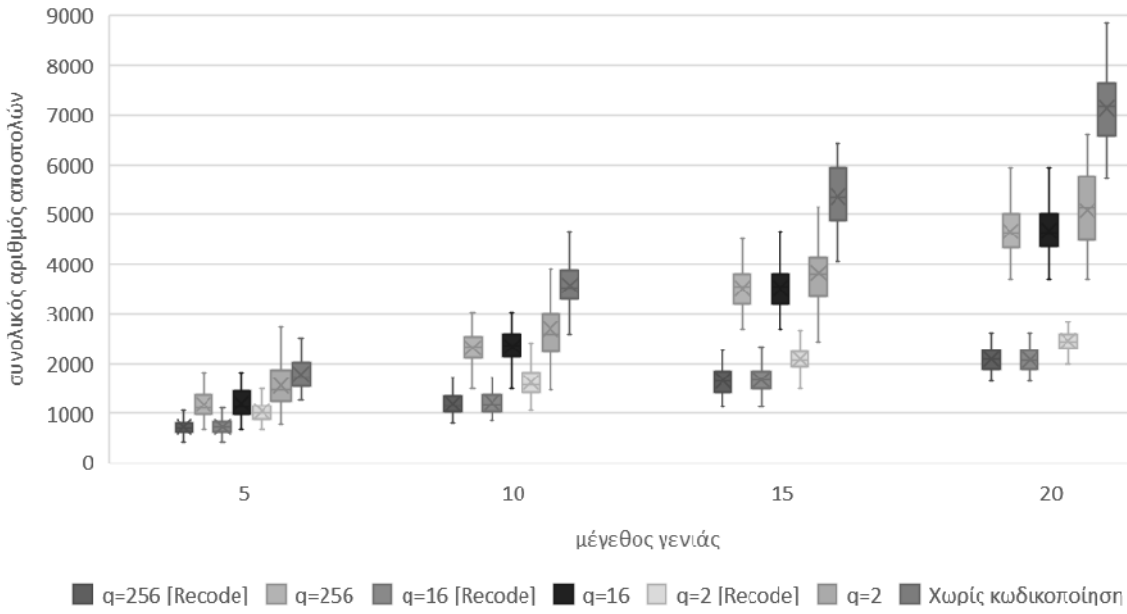
Είναι σαφής και ευδιάκριτη η διαφορά της χρήσης της επανα-κωδικοποίησης, ακόμα και σε σύγκριση με το απλό RLNC. Τα πακέτα που μπορεί να εγκλωβίζονται στον τρίτο ενδιάμεσο κόμβο, μπορούν να παράγουν καινοτόμα κωδικοποιημένα πακέτα, που αρκεί κάποια στιγμή να περάσουν στον τέταρτο και άρα να φτάσουν στον τελικό παραλήπτη. Αυτή ακριβώς η απομόνωση του τρίτου κόμβου είναι που κάνει τόσο αποδοτική την ικανότητά του να παράγει μόνος του νέα, πιθανά καινοτόμα, κωδικοποιημένα πακέτα. Αναδεικνύει έτσι την ανωτερότητα του RLNC έναντι των συμβατικών μεθόδων αποστολής.

5.4.3. Σενάριο Γενικευμένης Επίθεσης

Τέλος, θεωρούμε ότι το δίκτυο δέχεται επίθεση σε όλο το εύρος του, με αποτέλεσμα σε κάθε σύνδεσμο το ποσοστό απωλειών να είναι 90%. Οι παράμετροι των προσομοιώσεων συνοψίζονται στον Πίνακας 17.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5, 10, 15, 20
Αριθμός ενδιάμεσων κόμβων	5
Ποσοστό απωλειών	90%
Μέγεθος πεδίου	$q = 2^8$ (256)

Πίνακας 17 Multi-hop για διαφορετικά μεγέθη πεδίου και γενιάς



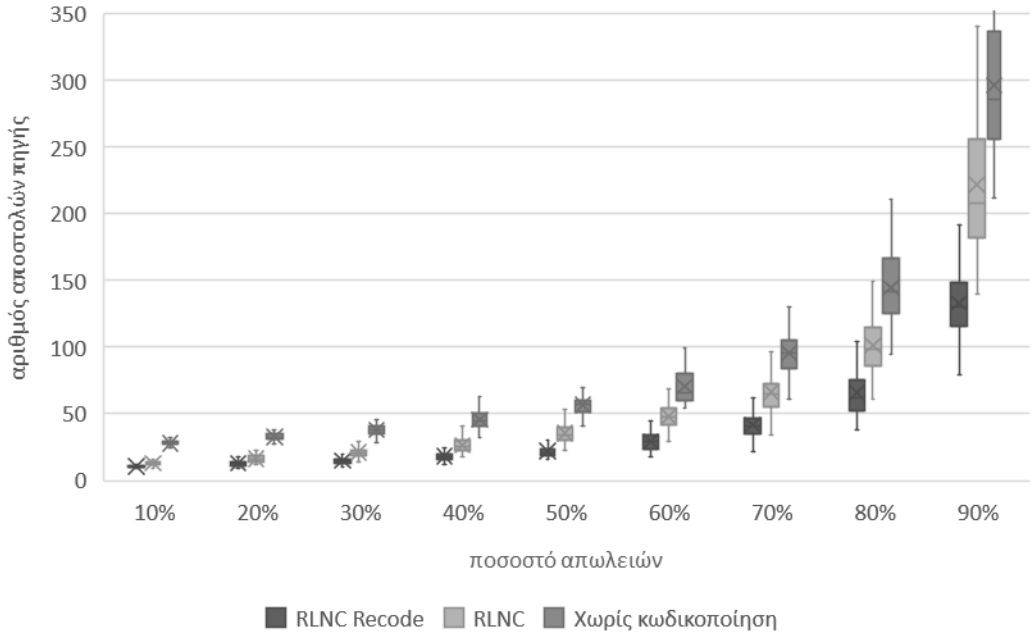
Διάγραμμα 21 Multi-hop, συνολικός αριθμός αποστολών για διαφορετικά μεγέθη γενιάς

Τα αποτελέσματα, που συνοψίζονται στο Διάγραμμα 21, δείχνουν, ειδικά στην περίπτωση του RLNC με επανα-κωδικοποίηση, ότι η αύξηση του μεγέθους της γενιάς (για παράδειγμα διπλασιασμός ή τριπλασιασμός), δε συνεπάγεται αναγκαστικά και διπλασιασμό ή τριπλασιασμό του συνολικού αριθμού αποστολών. Αυτό όμως συμβαίνει στην περίπτωση χωρίς κωδικοποίηση.

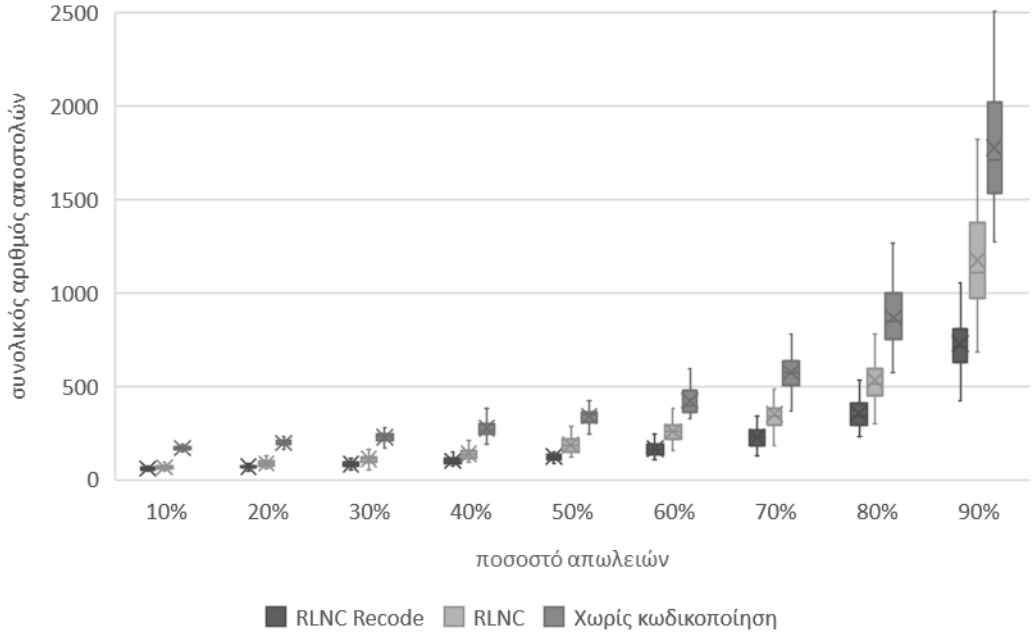
Ενδιαφέρον έχει και η επίδραση του ποσοστού απωλειών στο ίδιο δίκτυο. Οι παράμετροι συνοψίζονται στον Πίνακας 18, ενώ τα αποτελέσματα στο Διάγραμμα 22 και στο Διάγραμμα 23.

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός ενδιάμεσων κόμβων	5
Ποσοστό απωλειών	10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%
Μέγεθος πεδίου	$q = 2^8$ (256)

Πίνακας 18 Multi-hop για διαφορετικά ποσοστά απωλειών



Διάγραμμα 22 Multi-hop, αριθμός αποστολών πηγής για διαφορετικά ποσοστά απωλειών



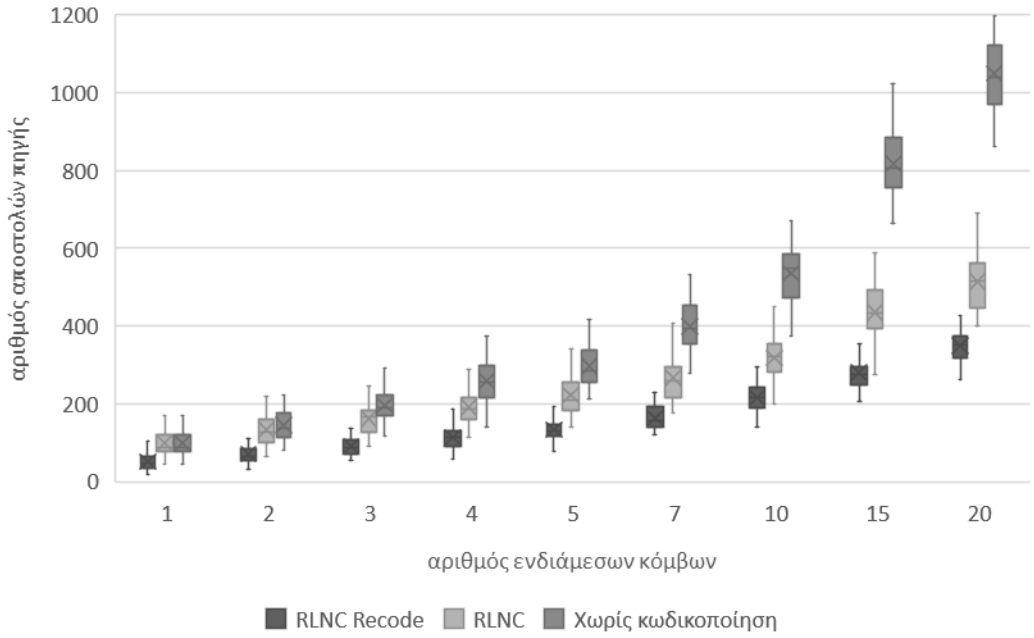
Διάγραμμα 23 Multi-hop, συνολικός αριθμός αποστολών για διαφορετικά ποσοστά απωλειών

Η διαφορά στη χρήση των τριών τεχνικών αυξάνει όσο αυξάνουν και τα ποσοστά απωλειών και τα χαρακτηριστικά ευρωστίας του RLNC είναι ιδιαίτερα εμφανή.

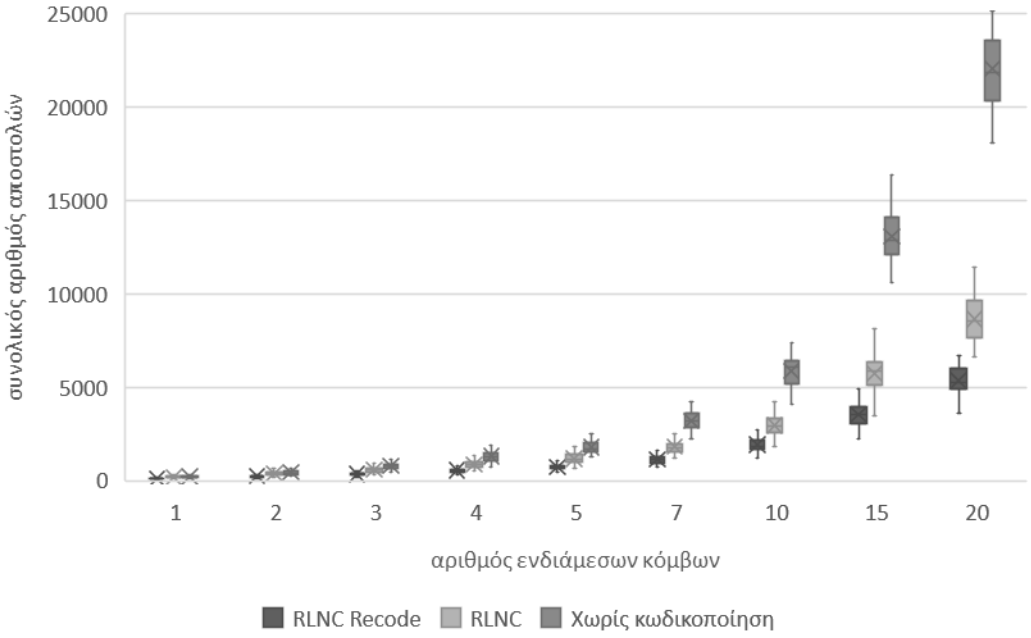
Τέλος αν δοκιμαστεί διαφορετικό πλήθος ενδιάμεσων κόμβων (πβ. Πίνακας 19), τότε το σύνολο των αποστολών μπορεί να φτάσει έως και τις 25.000 σε περίπτωση μη κωδικοποίησης (πβ. Διάγραμμα 24), ενώ με κωδικοποίηση και επανα-κωδικοποίηση μπορεί να διατηρηθεί στο 20% της τιμής αυτής (πβ. Διάγραμμα 25).

Παράμετρος	Τιμή
Αριθμός επαναλήψεων	50
Μέγεθος γενιάς	5
Αριθμός ενδιάμεσων κόμβων	1, 2, 3, 4, 5, 7, 10, 15, 20
Ποσοστό απωλειών	90%
Μέγεθος πεδίου	$q = 2^8$ (256)

Πίνακας 19 Multi-hop για διαφορετικό πλήθος ενδιάμεσων κόμβων



Διάγραμμα 24 Multi-hop, αριθμός αποστολών πηγής για διαφορετικό πλήθος ενδιάμεσων κόμβων



Διάγραμμα 25 Multi-hop, συνολικός αριθμός αποστολών για διαφορετικό πλήθος ενδιάμεσων κόμβων

Κεφάλαιο 6
Συμπεράσματα

Στο πλαίσιο της συγκεκριμένης μεταπτυχιακής διατριβής αναδείχτηκε η σημαντικότητα της διαθεσιμότητας ως απαίτηση της ασφάλειας των δικτύων. Προς την κατεύθυνση αυτή εξετάστηκε η δυνατότητα εφαρμογής της Κωδικοποίησης Δικτύου (network coding) για την επίτευξη αυξημένης διαθεσιμότητας. Από τις διάφορες παραλλαγές που εξετάστηκαν, προκρίθηκε η Τυχαία Γραμμική Κωδικοποίηση Δικτύου (Random Linear Network Coding, RLNC), ως αυτή με τα πιο ισχυρά χαρακτηριστικά προστασίας.

Μελετήθηκαν ποικίλα σενάρια επιθέσεων δικτύου και αναλύθηκε ο τρόπος που μπορεί το RLNC να συνεισφέρει στη βελτίωση των χαρακτηριστικών ασφάλειας του δικτύου.

Τα ευρήματα της θεωρητικής μελέτης επαληθεύτηκαν και πειραματικά, μέσα από μία σειρά προσομοιώσεων των επιθέσεων. Οι προσομοιώσεις έγιναν στην πλατφόρμα ns-3 χρησιμοποιώντας την υλοποίηση kodo για το RLNC. Διαπιστώθηκε ότι υλοποιήσεις του RLNC που έχουν χρησιμοποιηθεί σε προηγούμενες εργασίες και έρευνες έχουν εγκαταλειφθεί, χωρίς καν να έχει ολοκληρωθεί η ανάπτυξη των χαρακτηριστικών που αναφέρονται ως λειτουργικά. Αυτό δυσχεραίνει την πρωτογενή έρευνα αλλά και τις δυνατότητες αναπαραγωγής και επαλήθευσης (reproducibility) των ήδη δημοσιευμένων ερευνών. Το εύρημα αυτό, αν και παράπλευρο των αρχικών στόχων της διατριβής, κρίνεται ιδιαίτερα σημαντικό και μπορεί να αποτελέσει εφαλτήριο περαιτέρω επιστημονικής μελέτης στο πεδίο των δικτύων και της ασφάλειας αυτών.

Η πειραματική μελέτη κατέδειξε ότι το RLNC είναι ιδιαίτερα σημαντικό για την επίτευξη διαθεσιμότητας σε περιπτώσεις όπου ένα δίκτυο δέχεται σφοδρές επιθέσεις. Η διαπίστωση αυτή επιβεβαιώθηκε σε πολλαπλά σενάρια επίθεσης στην επικοινωνία ενός κόμβου με ένα ή περισσότερους παραλήπτες, με μονο-εκπομπή, πολύ-εκπομπή και ευρυ-εκπομπή, σε ασύρματα και ενσύρματα δίκτυα, με δυναμική ή στατική δρομολόγηση και μοναδικά ή πολλαπλά μονοπάτια δικτύου διαθέσιμα. Τα πακέτα που εισάγονται στο δίκτυο κωδικοποιημένα, είτε από την πηγή είτε από ενδιάμεσους

κόμβους, αφού συνδυάσουν πληροφορίες από τα αρχικά πακέτα, μπορεί να είναι χρήσιμα για πολλαπλούς παραλήπτες και για την ανάκτηση των αρχικών πληροφοριών από τον παραλήπτη μέσα από κατακερματισμένες πληροφορίες που περιέχονται στα κωδικοποιημένα πακέτα.

Η ύπαρξη κόμβων εντός του δικτύου με δυνατότητα επανα-κωδικοποίησης πακέτων βελτιώνει σημαντικά τη διαθεσιμότητα αλλά και τη διάρκεια ζωής του δικτύου, ιδιαίτερα σε σενάρια σφοδρών επιθέσεων, όπου μόνο το 10% των πακέτων μεταδίδονται επιτυχώς σε οποιοδήποτε σύνδεσμο. Ακόμη και όταν κάποιος κόμβος είναι σχεδόν αποκομμένος από το υπόλοιπο δίκτυο αλλά αποτελεί τμήμα ενός μονοπατιού δρομολόγησης, η επανα-κωδικοποίηση με RLNC επιτρέπει να παράγονται αρκετά καινοτόμα πακέτα ώστε να διατηρήσει την ικανότητα προώθησης των αρχικών πακέτων.

Τα οφέλη της χρήσης RLNC είναι πιο έντονα σε δίκτυα πολλαπλών παραληπτών της ίδιας πληροφορίας (σενάρια ευρυ-εκπομπής) και ιδιαίτερα έντονου θορύβου και κατά συνέπεια μεγάλων απωλειών στη μετάδοση πακέτων (90%). Ακόμη όμως και σε δίκτυα με ηπιότερα χαρακτηριστικά, παραμένουν ευθέως ανταγωνιστικά με τις συμβατικές μεθόδους δρομολόγησης πακέτων, χωρίς να εισάγουν μεγάλο αριθμό επιπλέον πακέτων στο δίκτυο ή πληροφοριών ανά πακέτο (overhead).

Η επιλογή του κατάλληλου μεγέθους πεδίου κωδικοποίησης είναι μία σημαντική παράμετρος της λειτουργίας του RLNC. Ένα μικρό μέγεθος (για παράδειγμα, q=2) σε σενάρια σφοδρών επιθέσεων οδηγεί στην παραγωγή κυρίως κωδικοποιημένων πακέτων που είναι γραμμικά εξαρτημένα και κατά συνέπεια δεν μπορούν να αποκωδικοποιηθούν κατά RLNC και να αντληθεί καινοτόμος πληροφορία. Ωστόσο, δεν είναι αναγκαίο να χρησιμοποιείται ένα ιδιαίτερα μεγάλο μέγεθος ή το μέγιστο επιτρεπτό, αλλά η κατάλληλη επιλογή εξαρτάται από τις συνθήκες που θα αντιμετωπίσει το δίκτυο κατά τη λειτουργία του.

Τα ευρήματα της μεταπτυχιακής διατριβής είναι αρκετά ενθαρρυντικά και μπορούν να αποτελέσουν εφαλτήριο για περαιτέρω μελέτες στο μέλλον. Οι διαθέσιμες υλοποιήσεις του RLNC εστιάζουν πρωτίστως στα χαμηλά επίπεδα της στοίβας πρωτοκόλλων του OSI. Μία ενδιαφέρουσα κατεύθυνση είναι η ανάπτυξη υλοποιήσεων RLNC που ενσωματώνονται σε πρωτόκολλα υψηλότερων επιπέδων. Αντίστοιχα και η ενσωμάτωσή τους σε πρωτόκολλα δρομολόγησης επιπέδου IP, ώστε να είναι δυνατός ο

έλεγχος επιθέσεων στη δρομολόγηση των πακέτων και η βελτίωση της διαθεσιμότητας κρίσιμων πρωτοκόλλων δικτύου. Μία τέτοια εξέλιξη θα επιτρέψει στο μέλλον τον έλεγχο πιο ευρηματικών επιθέσεων στη διαθεσιμότητα ενός δικτύου, όπου οι κακόβουλοι αφαιρούν στοχευμένα και επιλεγμένα πακέτα με κρίσιμες πληροφορίες για τη λειτουργία του δικτύου.

Μία δεύτερη κατεύθυνση, οδεύοντας προς την αποδοχή και ενσωμάτωση του RLNC στα πρωτόκολλα δικτύου, αφορά στα χαρακτηριστικά των τεχνικών υλοποιήσεων, ως προς το χρόνο επεξεργασίας των πακέτων, τον υπολογιστικό φόρτο σε κάθε κόμβο, αλλά και τις απαιτήσεις σε επιπλέον αποθηκευτικό χώρο ως και την ενεργειακή συμπεριφορά, ειδικά σε δίκτυα κόμβων με αυτόνομες πηγές ενέργειας.

Τέλος, η μελέτη και ενσωμάτωση εναλλακτικών τεχνικών κωδικοποίησης δικτύου (network coding), αποκλειστικά ή συνδυαστικά, συνεχώς ή κατά διαστήματα, όταν απαιτηθεί, αποτελεί μία τρίτη κατεύθυνση μελλοντικής εργασίας για τη βελτίωση της διαθεσιμότητας του δικτύου και της ασφάλειας που προσφέρει.

Βιβλιογραφία

Abdrashitov, V. & Medard, M. (2016). Staying alive — Network coding for data persistence in volatile networks. *2016 50th Asilomar Conference on Signals, Systems and Computers* (pp. 746-749). Pacific Grove, CA, USA: IEEE.

Aborujilah, A., Shahzad, A., Alsharafi, A., Musa, S. & Nazri, M. (2013). Flooding Based DoS Attack Feature Selection Using Remove Correlated Attributes Algorithm. *2013 International Conference on Advanced Computer Science Applications and Technologies* (pp. 93-96). Kuching, Malaysia: IEEE.

Advantages And Disadvantages Of Firewalls Computer Science Essay. (2016, Dec). Retrieved from UKessays: https://www.ukessays.com/essays/computer-science/advantages-and-disadvantages-of-firewalls-computer-science-essay.php

Ahlswede, R., Cai, N., Li, S.-Y. & Yeung, R. (2000, July). Network Information Flow. *IEEE TRANSACTIONS ON INFORMATION THEORY, 46*, 1204-1216. Retrieved from https://doi.org/10.1109/18.850663

Al-Khateeb, W., Al-Irhayim, S. & Al-Khateeb, K. (2010). Reliability Enhancement of Complex Networks through Redundancy Scaling. *International Conference on Computer and Communication Engineering, ICCCE'10*, (pp. 11-13). Kuala Lumpur, Malaysia.

Alsirhani, A., Sampalli, S. & Bodorik, P. (2018). DDoS Attack Detection System: Utilizing Classification Algorithms with Apache Spark. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS).* Paris, France: IEEE.

Angelopoulos, G., Paidimarri, A., Medard, M. & Chandrakasan, A. (2017, Sept). A Random Linear Network Coding Accelerator in a 2.4GHz Transmitter for IoT Applications. *IEEE Transactions on Circuits and Systems, 64*(9), 2582-2590.

Apiecionek, L. & Makowski, W. (2015). Firewall rule with token bucket as a DDoS protection tool. *IEEE 13th International Scientific Conference on Informatics* (pp. 32-35). Poprad, Slovakia: IEEE.

Bai, L., Ma, X., Ouyang, Z. & Zhan, X. (2014). Heterogeneous probabilistic model based spray routing protocol for delay tolerant networks. *6th International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 340-345). Shanghai, China: IEEE.

Bassoli, R., Marques, H., Rodriguez, J., Shum, K. & Tafazolli, R. (2013). Network Coding Theory: A Survey. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS. 15*, pp. 1950-1978. IEEE.

Bhatia, J., Patel, A. & Narmawala, Z. (2011). Review on variants of Network Coding in Wireless Ad-Hoc Networks. *2011 Nirma University International Conference on Engineering*, (pp. 1-6).

Bilbao, J., Crespo, P., Armendariz, I. & Medard, M. (2016, July). Network Coding in the Link Layer for Reliable Narrowband Powerline Communications. *IEEE Journal on Selected Areas in Communications, 34*(7), 1965-1977.

Bisogni, F., Cavallini, S., Franchina, L. & Saja, G. (2004). The European Perspective of Telecommunications as a Critical Infrastructure. *IFIP Advances in Information and Communication Technology*, *390.*

Bojkovic, Z. & Bakmaz, B. (2012). Smart Grid Communications Architecture: A Survey and Challenges. *11th WSEAS International Conference on Applied*, (pp. 83-89). Retrieved from http://www.wseas.us/e-library/conferences/2012/Rovaniemi/ACACOS/ACACOS-12.pdf

CCNA Security: Operational Strength & Weaknesses of Firewalls. (n.d.). Retrieved from CertificationKits: https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-implement-firewalls-with-sdm/ccna-security-operational-strength-a-weaknesses-of-firewalls/

Chen, Y., Liu, X., Liu, J., Taylor, W. & Moore, J. (2015). Delay-tolerant networks and network coding: Comparative studies on simulated and real-device experiments. *Computer Networks*, 349-362.

Chou, P. & Wu, Y. (2007). Network Coding for the Internet and Wireless Networks. *IEEE Signal Processing Magazine, 24*(5), 77-85.

Cimpanu, C. (2016, October 28). *Bug Bounty Hunter Launches Accidental DDOS Attack on 911 Systems via iOS Bug*. Retrieved from SoftPedia News: https://news.softpedia.com/news/bug-bounty-hunter-launches-accidental-ddos-on-911-systems-via-ios-bug-509738.shtml

Cloud, J. & Medard, M. (2015). Network Coding over SATCOM: Lessons Learned. *7th International conference, WiSATS 2015*, *154*, pp. 272-28. Retrieved from https://doi.org/10.1007/978-3-319-25479-1

Das, S. & Nene, M. (2017). A survey on types of machine learning techniques in intrusion prevention systems. *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 2296-2299). Chennai, India: IEEE.

David Gómez Fernández, Eduardo Rodríguez Maza & Ramón Agüero Calvo. (2014). *Network coding implementation on ns-3*. Retrieved from github: https://github.com/david-gomez-fernandez/network-coding-ns3

Devashryee, D. (2016, March 03). *Using redundant links to recover from network outage*. Retrieved from WITestLab: https://witestlab.poly.edu/blog/using-redundant-links-to-recover-from-network-outage/

Elias, P., Feinstein, A. & Shannon, C. (1956, December). A note on the maximum flow through a network. *IRE Transactions on Information Theory, 2*(4), 117-119. Retrieved from https://ieeexplore.ieee.org/document/1056816/

Elyengui, S., Bouhouchi, R. & Ezzedine, T. (2013). The Enhancement of Communication Technologies and Networks for Smart Grid Applications. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2*(6), 107-115.

Feng, Z., Zhu, Y., Zhang, Q. & Gao, M. (2012). Exploiting network coding for data availability in vehicular networks. *8th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)* (pp. 24-30). Chengdu, China: IEEE.

Ford, L. & Fulkerson, D. (1956). Maximal flow through a network. *Math*.

Fragouli, C. & Soljanin, E. (2006). *Network Coding Fundamentals* (Vol. 2).

Furdek, M., Wosinska, L., Goscien, R., Manousakis, K., Aibin, M., Walkowiak, K., . . . Marzo, J. (2016). An overview of security challenges in communication networks. *8th International Workshop on Resilient Networks Design and Modeling (RNDM)* (pp. 43-50). Halmstad, Sweden: IEEE.

Gomes, T., Tapolcai, J., Esposito, C., Hutchison, D., Kuipers, F., Rak, J., . . . Tornatore, M. (2016). A survey of strategies for communication networks to protect against large-scale natural disasters. *8th International Workshop on Resilient Networks Design and Modeling (RNDM).* Halmstad, Sweden: IEEE.

Ho, T., Koetter, R., Medard, M., Karger, D. & Effros, M. (2003). The benefits of coding over routing in a randomized setting. *IEEE International Symposium on Information Theory.* Yokohama, Japan: IEEE.

Ho, T., Medard, M., Koetter, R., Karger, D., Effros, M., Shi, J. & Leong, B. (2006, Oct). A Random Linear Network Coding Approach to Multicast. (IEEE, Ed.) *IEEE Transactions on Information Theory, 52*(10), 4413-4430.

Kim, T.-H., Choi, Y.-S., Kim, J. & Hong, S. (2008). Annulling SYN Flooding Attacks with Whitelist. *22nd International Conference on Advanced Information Networking and Applications* (pp. 371-376). Okinawa, Japan: IEEE.

Kiziloren, T. & Germen, E. (2007). Network traffic classification with Self Organizing Maps. *2007 22nd international symposium on computer and information sciences.* Ankara, Turkey: IEEE.

Koetter, R. & Medard, M. (2001). An Algebraic Approach to Network Coding. *ISIT2001* (pp. 782-795). Washington, DC: IEEE.

Krigslund, J., Hansen, J., Lucani, D., Fitzek, F. & Medard, M. (2015). Network Coded Software Defined Networking: Design and Implementation. *21th European Wireless Conference.* Budapest, Hungary.

Lee, S.-J. & Gerla, M. (2001). Split multipath routing with maximally disjoint paths in ad hoc networks. *IEEE International Conference on Communications* (pp. 3201-3205). Helsinki, Finland: IEEE.

Leschiutta, L., Zicca, G., Li, F., Vandoni, L. & Fragoulis, N. (2007). Achieving Reliability via Multi-Homing and Path Redundancy in Multi-hop Wireless Networks for Internet Access in Rural Areas. *16th IST Mobile and Wireless Communications Summit*.

Li, S.-Y., Yeung, R. & Cai, N. (2003). Linear Network Coding. *Li, S. Y. R., Yeung, R. W., & Cai, N. (2003). Linear network coding. IEEE Transactions on Information Theory, 49(2), 371–381. https://doi.org/Doi 10.1109/Tit.2002.807285*, 371-381.

Lim, H., Xu, K. & Gerla, M. (2003). TCP Performance over Multipath Routing in Mobile Ad Hoc Networks. *IEEE International Conference on Communications, 2003. ICC '03.* (pp. 1064-1068). Anchorage, AK, USA: IEEE.

Lima, L., Medard, M. & Barros, J. (2007). Random Linear Network Coding: A free cipher? *IEEE International Symposium on Information Theory* (pp. 546-550). Nice, France: IEEE.

Liu, J., Tang, M. & Yu, G. (2012). Adaptive Spray and Wait Routing based on Relay-Probability of Node in DTN. *International Conference on Computer Science and Service System* (pp. 1138-1141). Nanjing, China: IEEE.

Lun, D., Medard, M. & Koetter, R. (2006). Network Coding for Efficient Wireless Unicast. *Int. Zurich Seminar on Communications*, (pp. 74-77).

Mattioli, R. & Moulinos, K. (2015). Communication network interdependencies in smart grids. *Enisa*. European Union Agency For Network And Information Security.

Morris, K. (2011, September 30). *1 million ways to get banned from Reddit*. Retrieved from The Daily Dot: https://www.dailydot.com/news/rainmeter-denial-of-service-attack-reddit-block/

Nasipuri, A., Castaneda, R. & Das, S. (2001). Performance ofMultipath Routing for On-Demand Protocols in Mobile Ad Hoc Networks. *Mobile Networks and Applications, 6*, 339-349.

Nazer, B. & Gastpar, M. (2011). Reliable Physical Layer Network Coding. *Proceedings of the IEEE*, *99*, pp. 235-265.

Ostovari, P. & Wu, J. (2016). Fault-Tolerant and Secure Data Transmission Using Random Linear Network Coding. *14th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt).* Tempe, AZ, USA: IEEE.

Patterson, D. (2015, November 13). *Exclusive: Inside the ProtonMail siege: how two small companies fought off one of Europe's largest DDoS attacks*. Retrieved from TechRepublic: https://www.techrepublic.com/article/exclusive-inside-the-protonmail-siege-how-two-small-companies-fought-off-one-of-europes-largest-ddos/

Pedersen, M., Heide, J. & Fitzek, F. (2011). Kodo: An Open and Research Oriented Network Coding Library. *NETWORKING 2011 Workshops*, 145-152. Denmark: Aalborg University.

Qadir, S. & Quadri, S. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security, 7*(7), 185-194.

Rashmi, K., Shah, N. & Kumar, P. (2010, July). Network Coding. *Resonance – Journal of Science Education, 15*(7), 604-621.

Rayome, A. D. (2018, April 27). *Major DDoS attack lasts 297 hours, as botnets bombard businesses*. Retrieved from TechRepublic: https://www.techrepublic.com/article/major-ddos-attack-lasts-297-hours-as-botnets-bombard-businesses/

Segovia, B. G. (2012, May 31). Simulation of Random Linear Network Coding in Ad-Hoc Networks. Aalborg Universitet.

Speidel, U., Cocker, E., Vingelmann, P., Heide, J. & Medard, M. (2015). Can network coding bridge the digital divide in the pacific. *International Symposium on Network Coding (NetCod)* (pp. 86-90). Sydney, NSW, Australia: IEEE.

Stallings, W. (2011). *Cryptography and Network Security - Principles and Practice.* Prentice Hall.

Staudemayer, R., Voyiatzis, A., Moldovan, G., Lioumpas, A. & Alonso, D. (2018). Smart Cities under Attack: Cybercrime and Technology Response. In *Human-Computer Interaction and Cybersecurity Handbook.* CRC Press.

Sundararajan, K., Shah, D., Medard, M., Jakubczak, S., Mitzenmacher, M. & Barros, J. (2011, March). Network Coding Meets TCP: Theory and Implementation. *Proceedings of the IEEE, 99*, 490-512. Retrieved from https://doi.org/10.1109/JPROC.2010.2093850

Telecommunications Networks – A Vital Part of the Critical National Infrastructure. (n.d.). Electronic Communications Resilience & Repsonse Group (EC-RRG). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62279/telecommunications-sector-intro.pdf

The UGLY Truth Behind the Practice of IP Whitelisting... (2018, May 18). Retrieved from Akamai Community: https://community.akamai.com/customers/s/article/The-UGLY-Truth-Behind-the-Practice-of-IP-Whitelisting?language=en_US

Tooley, J. (1963, January). Network Coding for Reliability. *Transactions of the American Institute of Electrical Engineers, 81*(6), 407-414.

Tornatore, M., Andre, J., Babarczi, P., Braun, T., Folstad, E., Heegaard, P., . . . Voyiatzis, A. (2016). A Survey on Network Resiliency Methodologies against Weather-based Disruptions. *8th International Workshop on Resilient Networks Design and Modeling (RNDM).* Halmstad, Sweden: IEEE.

Urrutia, C., Ierace, N. & Bassett, R. (2005, June). *Intrusion Prevention Systems*. Retrieved from Ubiquity: https://ubiquity.acm.org/article.cfm?id=1071927

Vilela, J., Lima, L. & Barros, J. (2008). Lightweight Security for Network Coding. *IEEE International Conference on Communications* (pp. 1750-1754). IEEE.

Voyiatzis, A. (2012, June). A Survey of Delay- and Disruption-Tolerant Networking Applications. *Journal of Internet Engineering, 5*(1), 331-344. Retrieved from http://www.artemiosv.info/hosted/JIE-DTN-Survey.pdf

Vu, T. V. (2014). Application of network coding in wireless networks : coding conditions and adaptive redundancy control. Paris: Université Pierre et Marie Curie.

Wagner, D. (2018, March 25). *Cyberwarfare Against Critical Infrastructure*. Retrieved from International Policy Digest: https://intpolicydigest.org/2018/03/25/cyberwarfare-against-critical-infrastructure/

Weatherspoon, H. & Kubiatowicz, J. (2002). Erasure coding vs. replication: A quantitative comparison. *International Workshop on Peer-to-Peer Systems*, (pp. 328-337).

Xu, Y. & Lee, H. (2004). A Source Address Filtering Firewall to Defend against Denial of Service Attacks. *IEEE 60th Vehicular Technology Conference, 2004* (pp. 3296-3300). Los Angeles, CA, USA: IEEE.

Zhao, Y. & Yao, B. (2010). A Recent Study: Network Coding in Wireless Networks. *Fifth International Conference on Internet Computing for Science and Engineering* (pp. 124-129). Heilongjiang, China: IEEE.

Zhu, H. (2012). Reliability and availability analysis for large networking system. *2012 Proceedings Annual Reliability and Maintainability Symposium.* Reno, NV, USA: IEEE. doi:10.1109/RAMS.2012.6175453