Ατομική Διπλωματική Εργασία

ΑΣΦΑΛΕΙΑ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

Μύρια Χατζηθεορή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2013

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ασφάλεια σε Ασύρματα Δίκτυα Αισθητήρων

Μύρια Χατζηθεορή

Επιβλέπων Καθηγητής
Δρ. Βάσος Βασιλείου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου
Μάιος 2013

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Δρ. Βάσο Βασιλείου για την καθοδήγηση και για την όλη άψογη συνεργασία, κατά την διάρκεια της εκπόνησης της ατομικής αυτής, διπλωματικής εργασίας.

Επίσης θα ήθελα να ευχαριστήσω την διδακτορική φοιτήτρια του τμήματος Χριστιάνα Ιωάννου, για την υποστήριξη και την πολύτιμη βοήθεια που μου πρόσφερε μέσα σε αυτό το χρονικό διάστημα, για την ολοκλήρωση αυτής της εργασίας.

Τέλος, ήθελα να ευχαριστήσω την οικογένειά μου για την στήριξη και την συμπαράσταση καθ’ όλη την διάρκεια των σπουδών μου.

Περίληψη

Με την εμφάνιση του Διαδικτύου, κανείς δεν θα μπορούσε να φανταστεί πως αυτό θα μπορούσε να αποτελέσει μέσο για την εκτέλεση διαφόρων τύπων επιθέσεων, που βασικό σκοπό θα είχαν την εκμετάλλευση δεδομένων προκειμένου να προκαλέσουν σημαντικά προβλήματα, ίσως σε ένα ολόκληρο δίκτυο.

Όπως και τα παραδοσιακά δίκτυα, επιθέσεις είναι δυνατόν να δεχτούν και τα ασύρματα δίκτυα αισθητήρων, τα οποία αποτελούν τα τελευταία χρόνια ένα σημαντικό τομέα στον οποίο βασίζονται μεγάλες ερευνητικές δραστηριότητες.
Συγκεκριμένα θα μπορούσαμε να πούμε πως είναι ακόμα πιο ευάλωτα από τα συνηθισμένα δίκτυα λόγω της φύσεως τους.

Αυτού του είδους τα δίκτυα, αποτελούν μια εντελώς διαφορετική κατηγορία δικτύων από τα παραδοσιακά, παρουσιάζοντας κάποιες ιδιαιτερότητες και οι οποίες καθιστούν την μελέτη τους ξεχωριστή, σε σχέση με τα υπόλοιπα.
Ουσιαστικά αυτό που τα καθιστά ιδιαίτερα ως προς τα άλλα, είναι το ότι αποτελούνται από πολλούς κόμβους, μικρού μεγέθους, οι οποίοι λειτουργούν μερικώς αυτόνομα και έχουν περιορισμένες υπολογιστικές δυνατότητες.

Στην παρούσα λοιπόν διπλωματική εργασία, βασικός σκοπός, είναι η δημιουργία και μελέτη μερικών επιθέσεων που είναι δυνατόν να δεχτούν τα δίκτυα αισθητήρων.
Αρχικά γίνεται μια περιγραφή των ασύρματων δικτύων αισθητήρων όπως επίσης και πού μπορούν να βρουν εφαρμογή. Επιπλέον αναφέρονται μερικοί τρόποι αντιμετώπισης επιθέσεων και απειλών, που ενδεχομένως τα δίκτυα αυτά να δεχτούν.
Τέλος γίνεται λήψη κάποιων μετρήσεων και γίνεται μια περιγραφή του τρόπου με τον οποίο αντιδρά το σύστημα, όταν σε αυτό παρεμβάλουμε κάποιο κακόβουλο κώδικα.

Περιεχόμενα

Κεφάλαιο **1 Ασφάλεια Δικτύων** **6**

1.1 Εισαγωγή 6

1.2 Βασικές Έννοιες Ασφάλειας 7

1.2.1 Εμπιστευτικότητα 7

1.2.2 Ακεραιότητα 8

1.2.3 Αυθεντικοποίηση 8

1.3 Δυνατότητες Ασφάλειας 9

1.4 Εργαλεία Ασφάλειας Δικτύων 11

1.5 Αρχές ανάπτυξης αποτελεσματικού συστήματος ασφαλείας στο δίκτυο 12

1.6 Επιθέσεις στα δίκτυα 14

1.7 Πρωτόκολλα ασφάλειας δικτύων 17

Κεφάλαιο **2 Ασφάλεια σε Ασύρματα Δίκτυα** **20**

2.1 Εισαγωγή 20

2.2 Μέτρα μείωσης κινδύνων στα Ασύρματα Δίκτυα 21

Κεφάλαιο **3 Ασφάλεια στα ασύρματα δίκτυα αισθητήρων** **23**

3.1 Εισαγωγή 23

3.2 Πτυχές Ασφάλειας Ασυρμάτων Δικτύων Αισθητήρων 24

3.3 Επιθέσεις στα ασύρματα δίκτυα αισθητήρων 26

3.4 Περιορισμοί στα δίκτυα αισθητήρων 36

3.5 Λύσεις για την ασφάλεια στα ασύρματα δίκτυα αισθητήρων 37

3.6 Μέτρα αντιμετώπισης 43

3.7 Εφαρμογές στα ασύρματα δίκτυα αισθητήρων 44

Κεφάλαιο **4 Contiki OS** **47**

4.1 Εισαγωγή 48

4.2 Εργαλείο προσομοίωσης Cooja 50

Κεφάλαιο **5 Υλοποίηση Επιθέσεων και Εξαγωγή Αποτελεσμάτων** **51**

5.1 Flooding Attack 52

5.1.1 Unicast 52

5.1.2 Runicast 68
5.1.3 Multihop 78
5.2 Selective Forwarding Attack 92
5.2.1 Selective Forwarding Source 92
5.2.2 Selective Forwarding Ratio 123
5.2.3 Selective Forwarding Tree 139
5.3 Black Hole 148
Βιβλιογραφία 156

Κεφάλαιο 1

Ασφάλεια Δικτύων

1.1 Εισαγωγή
1.2 Βασικές Έννοιες Ασφάλειας
1.3 Δυνατότητες Ασφάλειας
1.4 Εργαλεία Ασφάλειας Δικτύων
1.5 Αρχές ανάπτυξης αποτελεσματικού συστήματος ασφαλείας στο δίκτυο
1.6 Επιθέσεις στα δίκτυα
1.7 Πρωτόκολλα ασφάλειας δικτύων

1.1 Εισαγωγή

Με την παρουσία του Διαδικτύου, αυτό που ουσιαστικά επιδιωκόταν, είναι η εξασφάλιση της επικοινωνίας και της ανταλλαγής δεδομένων μεταξύ διαφόρων χρηστών. Στην τελική, το Διαδίκτυο βρήκε περισσότερο χρήση στην εκτέλεση επιθέσεων παρά για οποιονδήποτε άλλο λόγο.
Σήμερα το σημαντικότερο θέμα στα σύγχρονα δίκτυα υπολογιστών είναι η ασφάλεια των δεδομένων, η οποία είναι εξίσου σημαντική τόσο για ένα χρήστη ενός προσωπικού υπολογιστή, μέχρι και για ένα ολόκληρο οργανισμό.
Οι εξελιγμένες τεχνικές και τεχνολογίες που χρησιμοποιούνται, έχουν πολλές δυνατότητες και παρέχουν μεγάλες διευκολύνσεις, μπορούν όμως πέρα από αυτό να δημιουργήσουν και προβλήματα σχετικά με την προστασία και την διαθεσιμότητα των πληροφοριών.
Ευαίσθητα θέματα τα οποία αφορούν στρατιωτικούς ή πολιτικούς σκοπούς μπορούν με πολύ μεγάλη ευκολία να υποκλαπούν, δημιουργώντας τεράστιο πρόβλημα.
Η ασφάλεια είναι απαραίτητη σε συνδυασμό με τις υπόλοιπες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, προκειμένου να μπορεί ένας οργανισμός να λειτουργεί σωστά και αξιόπιστα.

Ο βασικός σκοπός λοιπόν για τον οποίο εφαρμόζεται η ασφάλεια στα δίκτυα των υπολογιστών, έχει να κάνει με την ανίχνευση ασυνήθιστων δραστηριοτήτων και ενεργειών μέσα σε ένα δίκτυο και την λήψη κατάλληλων μέτρων για την αντιμετώπιση τους. Συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με την πρόληψη, την λήψη δηλαδή κάποιων μέτρων από την αρχή προκειμένου να αποφευχθούν προβλήματα μέσα στο δίκτυο, με την ανίχνευση, όπου λαμβάνονται κάποια μέτρα για να ανιχνευθεί πότε, πώς και από ποιόν προκλήθηκε κάποιο

πρόβλημα μέσα στο δίκτυο, και τέλος σχετίζεται με την αντίδραση όπου ουσιαστικά αυτό που επιδιώκεται, είναι η λήψη μέτρων για την αποκατάσταση ή την ανάκτηση των συστατικών μερών ενός δικτύου.

1.2 Βασικές Έννοιες Ασφάλειας

Η προστασία λοιπόν ενός δικτύου το οποίο συνδέεται με το Διαδίκτυο είναι ένα θέμα το οποίο αφορά όλους τους οργανισμούς και επιχειρήσεις, γιαυτό και προσπαθούν με οποιοδήποτε τρόπο να εφαρμόσουν όσο το δυνατόν καλύτερη ασφάλεια στα δίκτυα τους.
Η έννοια της ασφάλειας σήμερα, συνδέεται στενά με τρεις βασικές έννοιες που είναι η
εμπιστευτικότητα, η **πιστοποίηση** και ο **έλεγχος ακεραιότητας,** και οι οποίες αναλύονται παρακάτω.

1.2.1 Εμπιστευτικότητα

Με τον όρο εμπιστευτικότητα αναφερόμαστε στον τρόπο με τον οποίο ευαίσθητα δεδομένα μπορούν να κινηθούν μέσα στο δίκτυο χωρίς να υπάρχει ο κίνδυνος αυτά να γνωστοποιούνται σε μη εξουσιοδοτημένους χρήστες [36].
Η ασφάλεια των δεδομένων είναι ίσως το σημαντικότερο κομμάτι της ασφάλειας των δικτύων, γιαυτό και σε κάθε δίκτυο ο μηχανισμός της ασφάλειας επιδιώκει πρώτα την διαφύλαξη των δεδομένων.
Κάθε κόμβος πρέπει να διαφυλάσσει τα δεδομένα του , χωρίς να υπάρχει ο κίνδυνος αυτά να είναι προσβάσιμα από τους γείτονες. Ειδικότερα, σε περιπτώσεις όπου οι κόμβοι αυτοί χρησιμοποιούνται για στρατιωτικούς σκοπούς, τότε τα δεδομένα που είναι αποθηκευμένα μέσα στην μνήμη των αισθητήρων είναι ακόμα πιο ευαίσθητα, οπότε και πρέπει να είναι πλήρως προστατευμένα.
Συγκεκριμένα, στα δίκτυα αισθητήρων, η εμπιστευτικότητα συσχετίζεται στενά και με την επικοινωνία που υπάρχει μεταξύ γειτονικών κόμβων όπου είναι απαραίτητη η ανταλλαγή κάποιων ευαίσθητων δεδομένων, όπως τα κλειδιά που χρησιμοποιούνται στην συνέχεια για την κρυπτογράφηση των δεδομένων.
Σε αυτή την περίπτωση, είναι πολύ σημαντικό να δημιουργηθεί μια ασφαλής γραμμή επικοινωνίας για την διαφύλαξη των πληροφοριών.
Γενικώς, επιβάλλεται να διαφυλάσσονται ακόμα και οι δημόσιες πληροφορίες όπως είναι οι ταυτότητες των αισθητήρων ή τα δημόσια κλειδιά [37][34][24][48].
Η πρότυπη προσέγγιση για την διασφάλιση όλων αυτών των πληροφοριών, είναι η κρυπτογράφηση τους με ένα μυστικό κλειδί το οποίο γνωρίζουν μόνο οι κόμβοι για τους οποίους προορίζονται τα πακέτα.

1.2.2 Ακεραιότητα

Εκτός από τα μέτρα που πρέπει να λαμβάνονται έτσι ώστε να απαγορεύεται η πρόσβαση στα δεδομένα από μη εξουσιοδοτημένους χρήστες, πρέπει επίσης να διατηρείται και η ακεραιότητα τους. Κανένας δηλαδή μη εξουσιοδοτημένος χρήστης δεν πρέπει να έχει πρόσβαση σε αυτά έτσι ώστε να μπορέσει στην συνέχεια να προχωρήσει στην αλλοίωση τους, κατά την μετακίνηση τους μέσα στο δίκτυο. Μπορεί να εμποδιστεί μια κακόβουλη ενέργεια, όπως το να "κλαπούν" πληροφορίες, με την εμπιστευτικότητα όμως αυτό δεν μπορεί να εμποδίσει ένα εισβολέα να προκαλέσει ζημιά στο δίκτυο, αλλάζοντας το περιεχόμενο των πακέτων που διακινούνται μεταξύ των κόμβων.
Με την προσθήκη κάποιων επιπλέον κομματιών στα δεδομένα, την διαγραφή κάποιων πληροφοριών ή την αλλαγή του εσωτερικού των μηνυμάτων και την αποστολή του στον κόμβο για τον οποίο προοριζόταν, μπορεί να προκληθεί πρόβλημα σε ολόκληρο το δίκτυο [37][34][24].
Αλλοίωση των δεδομένων μπορεί να προκύψει και από το εχθρικό περιβάλλον στο οποίο λειτουργούν κάποιοι κόμβοι. Οπότε η ακεραιότητα των δεδομένων δεν πρέπει να διασφαλίζεται μόνο στην περίπτωση που υπάρχει κάποιος κακόβουλος κόμβος μέσα στο δίκτυο, αλλά και στην περίπτωση όπου προκαλείται ζημιά λόγω των άσχημων συνθηκών επικοινωνίας. Οπότε ο έλεγχος της ακεραιότητας των δεδομένων εγγυάται πως δεν υπήρχε καμία μεταβολή στα δεδομένα και ότι παραδόθηκαν στον προορισμό τους χωρίς καμία απολύτως αλλαγή.

1.2.3 Αυθεντικοποίηση

Μέχρι στιγμής δηλαδή, μπορούσαμε να διασφαλίσουμε ότι τα δεδομένα μας θα μεταδοθούν στον τελικό παραλήπτη με ακεραιότητα, όπως ακριβώς δηλαδή "έφυγαν" από τον αποστολέα, και πως είναι αναγνώσιμα μόνο από εξουσιοδοτημένους χρήστες, με την χρήση μηχανισμών κρυπτογράφησης. Αυτό όμως που δεν είναι δυνατόν να ελεγχθεί είναι το αν υπήρχε παρεμβολή επιπλέον πακέτων από κάποιον εισβολέα.
Η αυθεντικοποίηση, είναι μια λειτουργία η οποία απαγορεύει μη εξουσιοδοτημένη πρόσβαση μέσα στο δίκτυο και που επιτρέπει στους υπόλοιπους κόμβους να ανιχνεύσουν αν τα πακέτα έρχονται από τον πραγματικό αποστολέα ή από κάποιον άλλο κακόβουλο κόμβο, οπότε και μπορούν σε αυτή την περίπτωση να τα απορρίψουν. Γενικότερα έχει να κάνει με το αν ο παραλήπτης είναι όντως αυτός που λέει πως είναι.
Στην περίπτωση της ασφάλειας των δικτύων λοιπόν, γίνεται ένας έλεγχος προκειμένου να εξακριβωθεί κατά πόσο η ταυτότητα του αποστολέα είναι όντως αυτή που παρουσιάζει. Γίνεται λοιπόν μια επαλήθευση της ταυτότητας του αποστολέα και εγγυάται στον παραλήπτη πως ο αποστολέας δεν είναι κάποιος εισβολέας [37][34][36][52][48].
Αρχικά στην έναρξη της επικοινωνίας μεταξύ δύο κόμβων γίνεται μια

αυθεντικοποίηση της ταυτότητας και των δύο συμμετεχόντων. Στην συνέχεια γίνεται ένας ακόμα έλεγχος προκειμένου να επιβεβαιωθεί ότι δεν υπάρχει τρίτος χρήστης ο οποίος προσπαθεί να υποκλέψει τα δεδομένα που ανταλλάσσουν οι δύο κόμβοι μεταξύ των οποίων έχει εγκαθιδρυθεί επικοινωνία [24][36].
Σύμφωνα με τα [24][52][48], η αυθεντικοποίηση λειτουργεί με ένα συμμετρικό μηχανισμό, όπου τόσο ο αποστολέας όσο και ο παραλήπτης μοιράζονται ένα μυστικό κλειδί για να υπολογίσουν το message authentication code (MAC). Το MAC είναι σαν μια ετικέτα που προκύπτει όταν δώσουμε στον αλγόριθμο το μυστικό κλειδί και το μήνυμα.

Η δομή του δικτύου από μόνη της, επιτρέπει την εκτέλεση επιθέσεων. Για την παρεμπόδιση τους, πρέπει αυτές να γνωστοποιηθούν και να ερευνηθούν, έτσι ώστε να μπορέσει να βρεθεί μια αποτελεσματική μέθοδος αντιμετώπισης τους.

Με την ασφάλεια που εφαρμόζεται στα δίκτυα, αυτό που επιδιώκεται είναι να φυλάσσεται το ίδιο το δίκτυο και τα διάφορα συστατικά του μέρη από μη εξουσιοδοτημένες προσβάσεις σε αυτό. Μεγάλοι οργανισμοί λαμβάνουν μέτρα κατάλληλα για την αντιμετώπιση επιθέσεων, όπως είναι για παράδειγμα η δημιουργία εσωτερικών δικτύων τα οποία δεν έχουν επικοινωνία με το εξωτερικό δίκτυο.

1.3 Δυνατότητες Ασφάλειας

Για την ασφάλεια λοιπόν ενός δικτύου, δεν χρησιμοποιείται μονάχα μια μέθοδος, αλλά ένα σύνολο από πολλές και διαφορετικές μεθόδους, οι οποίες σε συνεργασία μεταξύ τους είναι ικανές να υπερασπίζονται από ένα μικρό δίκτυο στο σπίτι, μέχρι και ένα δίκτυο ενός ολόκληρου οργανισμού.
Στην περίπτωση όπου μία από τις μεθόδους αποτύχει σε ένα σημείο στην προστασία του δικτύου, τότε μια άλλη από τις υπόλοιπες μεθόδους θα μπορέσει να αντιμετωπίσει τον κίνδυνο. Έτσι τα δεδομένα που κινούνται μέσα στο δίκτυο παραμένουν προφυλαγμένα από διάφορες επιθέσεις.
Με αυτό τον τρόπο λοιπόν, υπάρχει η εγγύηση ότι τα ευαίσθητα δεδομένα και πληροφορίες παραμένουν μυστικά προς τον έξω κόσμο και προστατευμένα από οποιαδήποτε απειλή.
Συγκεκριμένα, οι δυνατότητες της ασφάλειας που εφαρμόζεται σε ένα δίκτυο αναφέρονται παρακάτω:

- Μπορεί ένα δίκτυο να προστατεύεται τόσο από εξωτερικές, όσο και από εσωτερικές απειλές. Οι απειλές που μπορεί να δεχτεί ένα δίκτυο, δεν προέρχονται απαραίτητα μόνο από τον εξωτερικό κόσμο. Ακόμα και ένας εσωτερικός παράγοντας μπορεί να προκαλέσει κάποιο πρόβλημα μέσα στο

δίκτυο, κάτι το οποίο μάλιστα, είναι πολλές φορές δύσκολο να εντοπιστεί και να καταπολεμηθεί εγκαίρως.
Θα μπορούσε να υπάρχει ένα σύστημα ασφαλείας, το οποίο θα παρακολουθεί την δραστηριότητα ολόκληρου του δικτύου. Στην περίπτωση που εντοπιστεί κάποια ασυνήθιστη συμπεριφορά μέσα στο δίκτυο, το σύστημα αντιδρά κατάλληλα, αφού πρώτα επισημάνει αυτή την συμπεριφορά.

- Διασφαλίζεται ότι όλες οι επικοινωνίες που γίνονται μέσα στο δίκτυο, είναι απόρρητες και προστατεύονται. Όλα τα δεδομένα που βρίσκονται αποθηκευμένα στο σύστημα και που κινούνται μέσα στο δίκτυο είναι ασφαλισμένα και πρόσβαση σε αυτά έχουν μόνο εξουσιοδοτημένοι χρήστες. Στην περίπτωση ενός ιδιωτικού οργανισμού, οι εργαζόμενοι μπορούν να συνδέονται στο δίκτυο από οπουδήποτε και αν βρίσκονται χωρίς να υπάρχει η ανησυχία ότι μπορεί κάποιος να υποκλέψει πληροφορίες.

- Στην περίπτωση όπου κάποιος χρήστης επιθυμεί να έχει πρόσβαση σε κάποιες πληροφορίες, γίνεται πρώτα ένας έλεγχος προκειμένου να εξασφαλιστεί ότι το άτομο αυτό έχει εξουσιοδότηση στα δεδομένα.
  Το αν έχει πρόσβαση στα δεδομένα, καθορίζεται από την ταυτότητα που έχει κάθε χρήστης, όπου μπορεί σύμφωνα με τις επαγγελματικές αρμοδιότητες ή με κάποια άλλα κριτήρια, τα οποία καθορίζονται από τον οργανισμό, να επιτρέπεται ή αντιθέτως να απαγορεύεται η πρόσβαση του σε κάποια δεδομένα.

Πρέπει λοιπόν ένα δίκτυο, είτε μικρό είτε μεγάλο να προστατεύεται και να επιτρέπει την ασφαλή χρήση του από τους νόμιμους χρήστες. Με την αύξηση και την εξέλιξη των διάφορων τύπων απειλών, πρέπει σκληρότερα μέτρα να λαμβάνονται για την αντιμετώπιση τους. Κανένας εισβολέας δεν επιτρέπεται να έχει πρόσβαση σε πληροφορίες και δεδομένα που διακινούνται μέσα στο δίκτυο, και γενικότερα πρέπει να εξασφαλίζεται πως το δίκτυο δεν έχει καμιά αδυναμία την οποία να μπορεί κάποιος να εκμεταλλευτεί.

1.4 Εργαλεία Ασφάλειας Δικτύων

Επειδή λοιπόν όλο και περισσότερες επιθέσεις γίνονται λόγω της συνεχούς ανάπτυξης του Διαδικτύου, και εφόσον υπάρχουν προσβάσιμες πληροφορίες μέσα σε ένα δίκτυο, αυτό που πρέπει να γίνει είναι να μελετηθούν διάφορες μέθοδοι οι οποίες αν όχι να εξαφανίσουν αυτές τις επιθέσεις, τουλάχιστον να είναι σε θέση να τις μειώσουν.
Διάφορες λοιπόν τεχνικές και μηχανισμοί έχουν αναπτυχθεί για αυτό τον σκοπό.
Για την προστασία λοιπόν κάποιων δεδομένων δεν πρέπει να λαμβάνεται υπόψη μόνο ένας τύπος ασφάλειας, όπως επίσης δεν πρέπει να γίνεται χρήση ενός μόνο εργαλείου

για την πλήρη προστασία ενός υπολογιστή ή οργανισμού [10][31].
Μερικά τέτοια εργαλεία είναι αναλύονται παρακάτω:

- Κρυπτογραφικά Συστήματα (Cryptographic Systems)
  Η κρυπτογράφηση είναι μια μέθοδος που χρησιμοποιείται ευρέως για σκοπούς προστασίας των δεδομένων. Αυτό που επιτυγχάνεται με την κρυπτογράφηση είναι τα δεδομένα να μετατρέπονται με τέτοιο τρόπο έτσι ώστε να μην μπορούν να διαβαστούν από άτομα τα οποία δεν έχουν καμιά εξουσιοδότηση σε αυτά .
  Η μέθοδος αυτή μπορεί να κρυπτογραφήσει τόσο τα δεδομένα τα οποία κινούνται μέσα στο δίκτυο για την επικοινωνία μεταξύ κάποιων κόμβων, όσο και δεδομένα τα οποία βρίσκονται απλώς αποθηκευμένα στο σύστημα.
  Το κείμενο μπορεί να αποκρυπτογραφηθεί μόνο από τον χρήστη ο οποίος έχει το κατάλληλο κλειδί.
  Ο μηχανισμός όμως αυτός δεν μπορεί να ξεχωρίσει ένα νόμιμο χρήστη από ένα μη νόμιμο αν τα κλειδιά τα οποία χρησιμοποιούν είναι τα ίδια [47][10][31][60].

- Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems)
  Τα συστήματα αυτά μπορούν να εντοπίζουν μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο και να βοηθούν στην απομάκρυνση κινδύνων που μπορεί να υπάρξουν. Παρακολουθούν την ροή των πακέτων που ανταλλάσσονται μεταξύ των κόμβων του δικτύου και ελέγχουν αν υπάρχει κάποια κακόβουλη ενέργεια.
  Κάποια τέτοια συστήματα μπορούν απλώς να δώσουν ένα σήμα σε μια κονσόλα διαχείρισης, το οποίο θα δείχνει όλες τις λεπτομέρειες για την ενέργεια που έχει προκύψει και πιθανώς να είναι κάποια επίθεση, ενώ κάποια άλλα προσπαθούν να εμποδίσουν την επίθεση δίνοντας εντολή σε κάποια άλλα μέρη του δικτύου, όπως είναι οι δρομολογητές, για διακοπή της σύνδεσης.
  Στην περίπτωση όμως όπου έχουμε ένα νόμιμο χρήστη ο οποίος μπορεί να έχει μια απαγορευμένη πρόσβαση σε πληροφορίες, τότε αυτός δεν μπορεί να ανιχνευθεί από το σύστημα ανίχνευσης εισβολής [10][31][60].

- Τείχος Προστασίας (Firewall)
  Το firewall μπορεί να είναι υλοποιημένο μέσα στην υποδομή του δικτύου, είτε στο υλικό (hardware) είτε στο λογισμικό (software), περιορίζοντας την πρόσβαση σε ορισμένους πόρους του δικτύου, από μη εξουσιοδοτημένους χρήστες.
  Ο μηχανισμός αυτός είναι ο πρώτος ο οποίος αντιμετωπίζει οποιαδήποτε

απειλή δεχτεί το δίκτυο. Προσπαθεί ουσιαστικά να εμποδίσει πακέτα τα οποία φτάνουν από άλλους κόμβους, και τα οποία θεωρεί κακόβουλα, να περάσουν στο εσωτερικό του δικτύου. Μπορεί επίσης να κάνει και το αντίθετο, να εμποδίσει δηλαδή πληροφορίες να βγουν έξω από το δίκτυο.
Ουσιαστικά βρίσκεται είτε στο gateway είτε στο access point, ελέγχοντας την ροή της κίνησης των πακέτων, εμποδίζοντας πακέτα να εισέλθουν ή να εξέλθουν σύμφωνα κάποιους κανόνες.
Το Firewall, δεν θα προστατέψει το δίκτυο από κάποιον ο οποίος βρίσκεται ήδη μέσα στο ίδιο το δίκτυο [10][57][31][60].

1.5 Αρχές ανάπτυξης αποτελεσματικού συστήματος ασφαλείας στο δίκτυο

Αυτό που επιδιώκεται για την ασφάλεια των δικτύων, είναι να μπορεί να παρέχεται προστασία στα δεδομένα που κινούνται μέσα σε αυτό, προκαλώντας όσο το δυνατόν λιγότερα προβλήματα στην προσβασιμότητα και παραγωγικότητα των χρηστών.
Το δίκτυο βέβαια πρέπει να είναι διαμορφωμένο με τέτοιο τρόπο έτσι ώστε να ανταποκρίνεται σε κάποιους κανόνες και απαιτήσεις.
Οπότε προκειμένου να μπορέσει να αναπτυχθεί ένα αποτελεσματικό σύστημα για την προστασία του δικτύου, πρέπει πρώτα να μελετηθούν κάποιες από τις παρακάτω αρχές, οι οποίες αναφέρονται στο άρθρο [57].

- Ταυτοποίηση των στοιχείων που αποτελούν ένα δίκτυο

Για να μπορέσουμε να προστατέψουμε αποτελεσματικά ένα δίκτυο πρέπει πρώτα να κατανοήσουμε ποια είναι τα βασικά συστατικά που το αποτελούν, έτσι ώστε να γνωρίζουμε πού πρέπει να δώσουμε περισσότερη προσοχή σε θέμα ασφάλειας.
Μερικά από τα μέρη που πρέπει να εξεταστούν συμπεριλαμβάνουν το υλικό, το λογισμικό, τις διεργασίες και τον εξοπλισμό.

- Καθορισμός σημείων που αντιμετωπίζουν ρίσκο

Πρέπει να ερευνηθούν τα σημεία τα οποία αντιμετωπίζουν υψηλό ρίσκο επίθεσης από εισβολείς. Γνωρίζοντας πώς και πού θα ενεργήσουν κάποιοι επιτιθέμενοι, μπορεί να αποτρέψει την δημιουργία μεγάλων προβλημάτων μέσα στο δίκτυο. Χρειάζεται να εντοπιστεί ποια είναι τα σημεία που πρέπει να προστατευτούν, από τί ακριβώς πρέπει να προστατευτούν και πώς πρέπει να προστατευτούν.

- Καθορισμός του κόστους των μέτρων ασφαλείας

Τα μέτρα ασφαλείας τα οποία επιβάλλονται, συχνά μπορούν να προκαλέσουν

εκτεταμένα προβλήματα στους χρήστες, και αυτό γιατί απαιτούν υπολογιστικούς πόρους για κατανάλωση.
Εκτός αυτού μπορεί η εφαρμογή των μέτρων αυτών, να προκαλέσει καθυστέρηση της εργασίας και ένα αριθμό άλλων επιβαρύνσεων.
Αν λοιπόν το κόστος που απαιτείται για την εφαρμογή αυτών των μέτρων για την ασφάλεια του δικτύου, ξεπερνά τα οφέλη του δικτύου, τότε αυτά καλύτερα να αποφεύγονται αφού προσφέρουν κακές υπηρεσίες στο δίκτυο.

- Περιορισμός της εμβέλειας της πρόσβασης

Μέσα σε ένα δίκτυο είναι προτιμότερο να προστατευθούν περισσότερο συγκεκριμένα μέρη της υποδομής τα οποία είναι πιο ευαίσθητα από κάποια άλλα. Για παράδειγμα μπορεί να δίνεται πρόσβαση σε ένα συγκεκριμένο μέρος του δικτύου, και η οποία να περιορίζεται μόνο σε αυτό το σημείο, να μην επιτρέπεται δηλαδή περαιτέρω πρόσβαση σε άλλα μέρη.

- Καθορισμός των υποθέσεων

Κάθε σύστημα ασφαλείας μπορεί να έχει κάποιες υποθέσεις σχετικά με την ασφάλεια του δικτύου. Για παράδειγμα ότι το δίκτυο είναι ασφαλισμένο ή όχι, ότι οι εισβολείς χρησιμοποιούν ένα συγκεκριμένο λογισμικό κτλ. Πρέπει όλες αυτές οι υποθέσεις να τεκμηριώνονται προκειμένου να μην δημιουργηθούν κενά στο σύστημα ασφαλείας του δικτύου, τα οποία στην συνέχεια θα βοηθήσουν τους εισβολείς στο έργο τους.

- Περιορισμός της εμπιστευτικότητας:

Πρέπει να μελετηθεί και να γνωστοποιηθεί ποιες συσκευές μπορεί ένα δίκτυο να εμπιστευθεί και σε ποιο λογισμικό μπορεί να στηριχθεί. Σε καμία περίπτωση δεν πρέπει να θεωρείται ως σωστή η υπόθεση πως δεν υπάρχουν καθόλου λάθη στο λογισμικό.

- Κατανόηση βασικών λειτουργιών του δικτύου:

Γνωρίζοντας πώς εκτελεί τις βασικές του λειτουργίες το δίκτυο και πώς χρησιμοποιούνται οι συσκευές του δικτύου, είναι πιο εύκολο να εντοπιστούν και να λυθούν προβλήματα ασφάλειας.

1.6 Επιθέσεις στα δίκτυα

Τα δίκτυα γενικώς, είναι δυνατόν να αντιμετωπίζουν κακόβουλες επιθέσεις που θέτουν σε κίνδυνο τις υπηρεσίες που αυτά παρέχουν, τα δεδομένα που είναι αποθηκευμένα στους κόμβους όπως και αυτά που μεταδίδονται μέσα στο δίκτυο.
Οι επιθέσεις αυτές μπορούν να χωριστούν σε δύο κατηγορίες οι οποίες είναι οι Παθητικές επιθέσεις (Passive attacks) και οι Ενεργητικές επιθέσεις (Active attacks).

Οι ενεργές επιθέσεις το τί κάνουν είναι να παίρνουν πληροφορίες και να τις

μετατρέπουν, επηρεάζοντας έτσι την λειτουργία του δικτύου.
Όπως αναφέρεται στο άρθρο [30][19][20][47], μερικές από τις ενεργές επιθέσεις που αντιμετωπίζει ένα δίκτυο είναι οι παρακάτω:

- Denial-of-service
- Masquerading
- Message Replay
- Modification

Η απλούστερη επίθεση **Denial-of-service** μπορεί να προκαλέσει καθυστέρηση στην παροχή υπηρεσιών σε ένα εξουσιοδοτημένο χρήστη, μέχρι και πλήρη διακοπή της παροχής υπηρεσιών, κάτι το οποίο ουσιαστικά σημαίνει πως μπορεί να ρίξει σε κάποιο βαθμό την απόδοση του συστήματος μέχρι και πλήρη κατάρρευση του δικτύου. Αυτό εξαρτάται από το αν ο επιτιθέμενος στοχεύει σε ένα συγκεκριμένο κόμβο(power exhaustion attack), ή το κανάλι επικοινωνίας (jamming attack).
Ο τρόπος με τον οποίο μπορεί να προκαλέσει μια τέτοια ζημιά στο δίκτυο κάποιος κακόβουλος κόμβος, είναι στέλνοντας συνεχώς αχρείαστα πακέτα μέσα στο δίκτυο. Οπότε με αυτό τον τρόπο προκαλούνται ακόμα και συγκρούσεις ή ακόμα και συμφόρηση μέσα στο δίκτυο μεταξύ των πακέτων και συνεπώς τα πακέτα από άλλους κόμβους δεν μπορούν να κινηθούν μέσα στο δίκτυο και να φτάσουν στον προορισμό τους [30][19][20][29][26][47].

Με την επίθεση **Masquerading**, ένας επιτιθέμενος μπορεί να έχει πρόσβαση σε ένα δίκτυο, παριστάνοντας κάποιον χρήστη ο οποίος έχει άδεια πρόσβασης, κλέβοντας το username και password κάποιου άλλου, ο οποίος έχει πρόσβαση στα δεδομένα. Με αυτό τον τρόπο, αποκτά και ο ίδιος πρόσβαση σε δεδομένα του δικτύου στα οποία κανονικά δεν έχει κανένα προνόμιο.
Κάποιος επιτιθέμενος μπορεί να πραγματοποιήσει αυτή την επίθεση είτε αυτός βρίσκεται μέσα στον οργανισμό στον οποίο επιθυμεί να δημιουργήσει πρόβλημα, είτε έξω από αυτόν, με την προϋπόθεση ότι ο οργανισμός ολόκληρος είναι συνδεδεμένος σε ένα δημόσιο δίκτυο.
Στην συνέχεια, μπορεί να κάνει κάποιες μη επιτρεπτές ενέργειες προκειμένου να δημιουργήσει πρόβλημα στο δίκτυο [30][19][29][47].
Η αδύναμη αυθεντικοποίηση διευκολύνει την εκτέλεση μιας τέτοιας επίθεσης, μιας και παρέχει ευκολότερη πρόσβαση στον επιτιθέμενο. Αν ο εισβολέας καταφέρει να κερδίσει μια αυθεντικοποιημένη πρόσβαση σε ένα οργανισμό, τότε σημαίνει πως μπορεί να έχει πρόσβαση σε κρίσιμα δεδομένα του οργανισμού, μπορεί να αλλάξει και να διαγράψει πληροφορίες, και να κάνει αλλαγές στην διαμόρφωση του δικτύου και τις πληροφορίες δρομολόγησης.

Η επίθεση **Message Replay** αυτό που ουσιαστικά κάνει , είναι να αναμεταδίδει πακέτα κάποιου αποστολέα μέσα στα οποία μπορεί να παρεμβάλει κακόβουλο κώδικα, ξεγελώντας τον παραλήπτη.
Η επίθεση αυτή είναι απλή γιατί είναι πολύ εύκολο κάποιος να καταγράψει δεδομένα

για αναμετάδοση, χρησιμοποιώντας ένα πρόγραμμα ανίχνευσης (sniffer program), καταγράφοντας όλα τα πακέτα που κινούνται μέσα στο δίκτυο.
Για παράδειγμα, ο εισβολέας, μπορεί να υποκλέψει τα μηνύματα που στέλνει ένας εξουσιοδοτημένος χρήστης για να εισέλθει μέσα σε ένα δίκτυο, τα οποία περιέχουν ευαίσθητα δεδομένα όπως για παράδειγμα κωδικούς, και να τα αναμεταδώσει κάποια άλλη χρονική στιγμή. Με αυτό τον τρόπο λοιπόν, θα μπορεί να έχει πρόσβαση μέσα στο δίκτυο, ακόμα και αν αυτά τα μηνύματα είναι κρυπτογραφημένα και δεν γνωρίζει τα μυστικά κλειδιά που χρησιμοποιούνται.
Σε αυτή την περίπτωση παρουσιάζεται και η επίθεση Masquerading κατά την οποία ο κόμβος που αναμεταδίδει τα πακέτα παρουσιάζεται ως ένας νόμιμος κόμβος [19][29][47].
Τρόπος για αντιμετώπιση της συγκεκριμένης επίθεσης, είναι η χρήση δυνατών ψηφιακών υπογραφών οι οποίες θα περιέχουν κάποιο χρονικό σημείο και κάποιες μοναδικές πληροφορίες οι οποίες θα αποδεικνύουν πως κάθε πακέτο είναι διαφορετικό από κάθε άλλο προηγούμενο, όπως είναι για παράδειγμα ένας συνεχής αυξανόμενος αριθμός.

Μια ακόμα επίθεση είναι η **Message Modification**, κατά την οποία επηρεάζεται η ακεραιότητα των δεδομένων που στέλνει ένας κόμβος σε ένα άλλο ενδιάμεσο κόμβο ή στον τελικό προορισμό. Με αυτή την επίθεση, ένας μη εξουσιοδοτημένος χρήστης μπορεί όχι μόνο να διαβάσει αλλά και να μεταβάλει το περιεχόμενο ενός πακέτου, το οποίο προέρχεται από ένα νόμιμο κόμβο [19][29][26][47].
Για παράδειγμα, αλλοιώνοντας την διεύθυνση που βρίσκεται στην κεφαλίδα ενός πακέτου, θα μπορούσε κάποιος να κατευθύνει το πακέτο σε ένα ανεπιθύμητο προορισμό, να προκαλέσει καθυστέρηση στην μετάδοση του πακέτου ή να το μεταδώσει με διαφορετική σειρά. Επίσης υπάρχει η δυνατότητα αλλαγής των πληροφοριών του χρήστη, οι οποίες μεταφέρονται μέσω του πακέτου, δημιουργώντας μια σύγχυση στην επικοινωνία.
Τα πρωτόκολλα συχνά, για την αντιμετώπιση τέτοιου είδους επιθέσεων χρησιμοποιούν κρυπτογράφηση.

Οι παθητικές επιθέσεις είναι αυτές κατά τις οποίες ο εισβολέας μπορεί να έχει πρόσβαση στα δεδομένα, να διαβάσει ή να χρησιμοποιήσει διάφορες πληροφορίες δηλαδή του δικτύου, χωρίς όμως να τις αλλοιώνει.

Παραδείγματα από τέτοιες επιθέσεις είναι τα παρακάτω:

- Release of message contents
- Traffic analysis

Η πρώτη επίθεση που είναι η **Release of message contents**, αυτό που επιδιώκει είναι να μπορέσει να διαβάσει “ευαίσθητες” πληροφορίες που ανταλλάσσονται μεταξύ κάποιων κόμβων. Για παράδειγμα τέτοιες πληροφορίες θα μπορούσαν να είναι κωδικοί, κλειδιά για κρυπτογράφηση κτλ.

Η επίθεση **Traffic** μπορεί να λειτουργήσει κανονικά ακόμα και αν υπάρχει ασφάλεια στο περιεχόμενο των πακέτων, δηλαδή είναι κρυπτογραφημένα, οπότε ακόμα και αν κάποιο τρίτο άτομο καταφέρει να τα υποκλέψει δεν θα μπορεί να τα διαβάσει.
Ο επιτιθέμενος όμως μπορεί να εντοπίσει την τοποθεσία των κόμβων που επικοινωνούν, καθώς και την ταυτότητα τους. Στην συνέχεια με αυτά τα στοιχεία, παρατηρώντας την συχνότητα με την οποία ανταλλάσσονται τα πακέτα μεταξύ των κόμβων, όπως και το μέγεθος τους, είναι πολύ εύκολο να αποκαλυφθεί το είδος της συνομιλίας που διεξάγεται [47].

Η ανίχνευση παθητικών επιθέσεων καθίσταται πολύ δύσκολη από την άποψη ότι δεν περιλαμβάνει καμιά μεταβολή ή τροποποίηση των δεδομένων. Τα δεδομένα αποστέλλονται και λαμβάνονται χωρίς καμιά ανησυχία από τον αποστολέα ή τον παραλήπτη εάν αυτά τα μηνύματα έχουν διαβαστεί από ένα εισβολέα, ή αν ακόμα και ολόκληρο το μοτίβο επικοινωνίας έχει μελετηθεί από κάποιον τρίτο. Έμφαση σε αυτή την περίπτωση πρέπει να δοθεί κυρίως στην πρόληψη, που είναι η κρυπτογράφηση, και όχι στην ανίχνευση.

1.7 Πρωτόκολλα ασφάλειας δικτύων

Λόγω της μεγάλης και απότομης ανάπτυξης του Διαδικτύου, όλο και περισσότεροι οργανισμοί στηρίζουν τις εργασίες τους στο Διαδίκτυο, οπότε υπάρχει μια αύξηση της ανταλλαγής ηλεκτρονικών μηνυμάτων, ανάπτυξη του ηλεκτρονικού εμπορίου και των ηλεκτρονικών συναλλαγών.
Το γεγονός όμως αυτό, αυξάνει την ανησυχία και πολλές φορές απαιτείται η ύπαρξη ασφάλειας και μυστικότητας στην ηλεκτρονική επικοινωνία και ηλεκτρονικό εμπόριο.
Για αυτό τον λόγο, προτάθηκαν κάποια πρωτόκολλα και πρότυπα.
Το κύριο εργαλείο που χρησιμοποιείται για την προστασία της πληροφορίας που κινείται μέσα σε ένα δίκτυο, είναι η κρυπτογράφηση των δεδομένων, η οποία χρησιμοποιεί αλγόριθμους για να αποκρύψει τα δεδομένα έτσι ώστε να μην μπορούν να διαβαστούν από μη εξουσιοδοτημένα άτομα. Χωρίς αυτά τα πρωτόκολλα κρυπτογράφησης καμιά λειτουργία όπως είναι το ηλεκτρονικό εμπόριο δεν θα ήταν δυνατή.
Μερικά από αυτά τα πρωτόκολλα είναι το Secure Electronic Transactions (SET) για το Application Layer, το Secure Socket Layer (SSL)για το Transport και το Secure HTTP (S-HTTP), τα οποία περιγράφονται πιο κάτω.

Secure Socket Layer (SSL)

Το πρωτόκολλο SSL σχεδιάστηκε για να παρέχει ένα ασφαλισμένο μονοπάτι από τον αποστολέα στον παραλήπτη, για την ασφαλή μετάδοση των δεδομένων μέσα στο δίκτυο.
Είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο και είναι κατάλληλο ειδικά για περιπτώσεις που έχουν να κάνουν με το ηλεκτρονικό εμπόριο λόγω των διάφορων υπηρεσιών που προσφέρει, όπως είναι η κρυπτογράφηση των δεδομένων, η αυθεντικοποίηση του server και του client και η ακεραιότητα του μηνύματος.
Με την κρυπτογράφηση των μηνυμάτων, αυτό που επιτυγχάνεται είναι η προστασία των δεδομένων κατά την μεταφορά τους, όπου ουσιαστικά δεν μπορούν να υποκλαπούν από τρίτο άτομο αφού με αυτό τον τρόπο μπορούν να διαβαστούν μόνο από τον παραλήπτη.
Με την χρήση κρυπτογράφησης μέσω ενός πρότυπου κλειδιού, γίνεται αυθεντικοποίηση του ενός κόμβου στον άλλο κόμβο με τον οποίο βρίσκεται σε επικοινωνία.
Επίσης, η ακεραιότητα του μηνύματος επιτυγχάνεται με την χρήση κάποιων κλειδιών, έτσι ώστε τα δεδομένα να μην αλλοιωθούν με κανένα τρόπο.
Χρησιμοποιεί ένα μυστικό κλειδί για την κρυπτογράφηση των δεδομένων, αφού προηγουμένως πραγματοποιήσει μια κρυπτογράφηση με δημόσιο κλειδί στα δεδομένα [10][57][32][28].

Secure Electronic Transactions (SET)

Το πρωτόκολλο αυτό αναπτύχθηκε κυρίως για να επιτρέπει ασφαλισμένες συναλλαγές μέσα στο Διαδίκτυο, με την χρήση των πιστωτικών καρτών. Το προηγούμενο πρωτόκολλο, το SSL, μπορεί να κρατήσει τις ευαίσθητες λεπτομέρειες ασφαλισμένες από τρίτους που προσπαθούν να τις υποκλέψουν, αυτό όμως που δεν μπορεί να κάνει, είναι να εξακριβώσει την ταυτότητα των συμμετεχόντων σε μια συναλλαγή.
Λύση στο πρόβλημα δίνει το πρωτόκολλο SET, όπου ουσιαστικά απαιτείται από τους συμμετέχοντες να εγγραφούν, πριν την έναρξη της μεταξύ τους συναλλαγής.
Ο πελάτης και ο πωλητής, προκειμένου να εγγραφούν, χρειάζεται να έρθουν σε επικοινωνία με μια αρχή έκδοσης πιστοποιητικού, δίνοντας τις απαραίτητες λεπτομέρειες ασφάλειας, όπως και το δημόσιο κομμάτι του κλειδιού υπογραφής τους.
Η εγγραφή αυτή επιτρέπει τον έλεγχο του αιτούμενου ατόμου και σε περίπτωση που αυτός εγκριθεί τότε λαμβάνει ένα πιστοποιητικό το οποίο επιβεβαιώνει ότι το κλειδί υπογραφής του είναι έγκυρο.
Αφού λοιπόν είναι σίγουρο ότι οι συμμετέχοντες είναι αυτοί που υποστηρίζουν πως είναι, επιτρέπει την ανταλλαγή δεδομένων μεταξύ τους, κρυπτογραφώντας βέβαια όλες τις πληροφορίες της πιστωτικής κάρτας, πριν να σταλούν διαμέσου του Διαδικτύου, με RSA public-key encryption και DES single-key τεχνολογία.
Για κάθε συναλλαγή που πραγματοποιείται, το πρωτόκολλο SET παρέχει τις

υπηρεσίες αυθεντικοποίησης, τόσο του πελάτη όσο και του έμπορου σε μια συναλλαγή, εμπιστευτικότητας των πληροφοριών που ανταλλάσσουν και την διασφάλιση της ακεραιότητας των εντολών πληρωμής που μεταφέρονται μέσω των μηνυμάτων [32][57].

Secure HTTP (S-HTTP)

Κατά την δημιουργία του πρωτοκόλλου HTTP, το Διαδίκτυο ήταν πολύ απλό, γιαυτό και ο σχεδιασμός του ίδιου του πρωτοκόλλου ήταν εξίσου απλός. Δεν υπήρχε καμιά απαίτηση για κρυπτογράφηση ή αυθεντικοποίηση των δεδομένων.
Καθώς λοιπόν το Διαδίκτυο εξελισσόταν, έγινε αντιληπτό πως το πρωτόκολλο που θα χρησιμοποιούταν, θα έπρεπε να υποστεί κάποιες αλλαγές έτσι ώστε να προστατεύει τα δεδομένα από απειλές οι οποίες παρουσιάζονταν.
Οπότε προέκυψε το S-HTTP για την υποστήριξη της ασφαλούς αποστολής των δεδομένων μέσα στο Διαδίκτυο. Κάθε S-HTTP αρχείο είτε είναι κρυπτογραφημένο, είτε περιέχει ένα ψηφιακό πιστοποιητικό, είτε και τα δύο.
Το πρωτόκολλο S-HTTP χρησιμοποιείται σε συνδυασμό με το πρωτόκολλο HTTP, προκειμένου να επιτρέπεται στον client και τον server να δημιουργούν μια ιδιωτική και ασφαλισμένη ανταλλαγή δεδομένων, και είναι σχεδιασμένο έτσι ώστε να μπορεί να ενσωματωθεί με HTTP εφαρμογές.
Είναι πολύ παρόμοιο με το πρωτόκολλο SSL, το οποίο χρησιμοποιείται περισσότερο από το S-HTTP. Το S-HTTP παρέχει τις ίδιες λειτουργίες αυθεντικοποίησης και κρυπτογράφησης με το SSL, όμως το πρώτο, μπορεί να κρυπτογραφήσει μόνο μηνύματα του HTTP επιπέδου, ενώ το SSL έχει την ικανότητα να κρυπτογραφεί όλα τα δεδομένα που κινούνται μεταξύ client-server συμπεριλαμβανομένων και των δεδομένων στο IP επίπεδο.
Το S-HTTP όμως, εξακολουθεί να χρησιμοποιείται σε πολλές περιπτώσεις, υποστηρίζοντας μια ποικιλία από κρυπτογραφικούς αλγορίθμους τρόπους λειτουργίας. Τα μηνύματα μπορούν να προστατεύονται με την χρήση ψηφιακών υπογραφών, αυθεντικοποίησης και κρυπτογράφησης [32].

Κεφάλαιο 2

Ασφάλεια σε Ασύρματα Δίκτυα

2.1 Εισαγωγή
2.2 Μέτρα μείωσης κινδύνων στα Ασύρματα Δίκτυα

2.1 Εισαγωγή

Ένα ασύρματο τοπικό δίκτυο, μπορεί να προσφέρει άνετη πρόσβαση στο Διαδίκτυο, όμως παρουσιάζει κάποια άλλα ρίσκα όσο αφορά το θέμα της ασφάλειας, τα οποία πρέπει με κάποιο τρόπο να περιοριστούν όσο το δυνατόν περισσότερο.
Για την ανάπτυξη ενός ασφαλούς ασύρματου δικτύου λοιπόν, πρέπει πρώτα να εξεταστούν αυτά τα πιθανά ρίσκα, όπως και να ταυτοποιηθούν και να ερευνηθούν οι επιθέσεις που μπορεί να προκύψουν.
Ο λόγος για τον οποίο τα ασύρματα δίκτυα, παρουσιάζουν περισσότερους κινδύνους από τα ενσύρματα δίκτυα, οφείλεται στο γεγονός ότι τα σήματα που στέλνονται από τον ένα κόμβο στον άλλο, κατά την διάρκεια μιας επικοινωνίας, μπορούν να περάσουν μέσα από δημόσιους χώρους.
Αυτό σημαίνει πως επιτρέπει στον καθένα, ο οποίος βρίσκεται σε ένα τέτοιο δημόσιο περιβάλλον και έχοντας τα κατάλληλα εργαλεία, να υποκλέψει τα δεδομένα τα οποία κινούνται μέσα στο δίκτυο. Για αυτό τον λόγο αποφεύγεται πλέον, από τους περισσότερους οργανισμούς, η υποστήριξη ασύρματων δικτύων, τα οποία δεν παρέχουν ασφάλεια στην μετάδοση των δεδομένων.
Σε περίπτωση που χρειάζεται να γίνει χρήση ενός τέτοιου δικτύου για την μεταφορά των δεδομένων πρέπει πρώτα να ληφθούν μέτρα, τα οποία θα μειώσουν τους κινδύνους.

2.2 Μέτρα μείωσης κινδύνων στα Ασύρματα Δίκτυα

Access Point Security

Ένα ασύρματο σημείο πρόσβασης (wireless access point - AP), είναι μια συσκευή, η οποία επιτρέπει σε ασύρματες συσκευές, όπως είναι για παράδειγμα τα PDAs και τα mobile computers, να συνδεθούν σε ένα ασύρματο δίκτυο.
Συνήθως ένα AP, συνδέεται πάνω σε ένα ενσύρματο δίκτυο και παρέχει μια γέφυρα για ασύρματη επικοινωνία μεταξύ ασύρματων και ενσύρματων συσκευών.
Ρυθμίζοντας λοιπόν το AP, για ασφάλεια στο δίκτυο, είναι μια σημαντική αρχή για την ανάπτυξη ενός ασφαλούς δικτύου.
Ιδανικά, το AP θα επιτρέψει την δημιουργία ενός WEP κλειδιού, το οποίο είναι ουσιαστικά ένας κωδικός που χρησιμοποιείται στα ασύρματα δίκτυα, έτσι ώστε να μπορούν οι συσκευές στο εσωτερικό του δικτύου, να ανταλλάσσουν κωδικοποιημένα μηνύματα.
Αυτό το κλειδί δεν πρέπει να μπορεί να βρεθεί εύκολα, αφού ο σκοπός του είναι να εμποδίζει κάποιον εισβολέα να αποκρυπτογραφήσει τα δεδομένα, ή τουλάχιστον να τον δυσκολεύει.
Επίσης μπορεί να χρησιμοποιηθούν MAC διευθύνσεις προκειμένου να περιορίζουν τον αριθμό των συσκευών που μπορούν να ενωθούν πάνω στο δίκτυο, βοηθώντας στην καλύτερη διαχείριση του φόρτου μέσα στο δίκτυο.
Ένα ακόμα σημαντικό μέτρο όσο αφορά το AP, είναι η επιβεβαίωση ότι ένα AP δεν κάνει broadcast το SSID αν αυτό είναι δυνατόν. Αυτό σημαίνει πως περιορίζεται και πάλι ο αριθμός των συσκευών που μπορούν να ενωθούν πάνω στο AP, αφού γίνεται χρήση αυτού του κωδικού για να μπορέσουν διαφορετικές συσκευές να ενωθούν πάνω στο ίδιο δίκτυο. Έτσι με την χρήση ενός δυνατού κωδικού μπορεί να εμποδιστεί η εύκολη πρόσβαση ενός εισβολέα μέσα στο δίκτυο.
Ένα ακόμα σημείο που μπορεί να ληφθεί υπόψη, είναι και η τοποθεσία του AP. Αφού τα σήματα σε ένα ασύρματο δίκτυο μπορούν να καλύψουν μια μεγάλη απόσταση, τοποθετώντας το AP σε ένα μέρος τέτοιο ώστε τα σήματα να μην βγαίνουν εκτός της περιοχής που θέλουμε να καλύψουμε, θα περιορίσει και τις πιθανότητες κάποιος εισβολέας να αποκτήσει πρόσβαση στο δίκτυο [31][39].

Transmission Security

Αν και με το WEP key, όπως προαναφέρθηκε υπάρχει ακόμα ο κίνδυνος ένας εισβολέας να έχει πρόσβαση μέσα στο δίκτυο, εντούτοις πρέπει ακόμα αυτό να χρησιμοποιείται. Είναι προτιμότερο, από το μην υπάρχει καθόλου προστασία από το δίκτυο, αφού χρειάζεται προσπάθεια από κάποιον για να σπάσει αυτό τον κωδικό.
Γνωρίζοντας λοιπόν πως το WEP, δεν προστατεύει επαρκώς τις ευαίσθητες πληροφορίες, είναι δυνατόν να χρησιμοποιηθεί κάποιος άλλος τρόπος για κρυπτογράφηση των μηνυμάτων.

Μπορεί λοιπόν, να χρησιμοποιηθεί ένα Εικονικό Προσωπικό Δίκτυο(Virtual Private Network (VPN)), στην περίπτωση όπου υπάρχει μετάδοση ευαίσθητων ή προσωπικών πληροφοριών, πάνω σε ένα δημόσιο ασύρματο δίκτυο.
Με το VPN, επιβεβαιώνεται ότι υπάρχει εμπιστευτικότητα στην επικοινωνία χρησιμοποιώντας τεχνολογίες κρυπτογράφησης. Τα περισσότερα VPNs, χρησιμοποιούν ισχυρούς αλγορίθμους, οι οποίοι δεν παρουσιάζουν τους ίδιους τύπους προβλημάτων παρουσιάζει το WEP [31][56].

Workstation Security

Ένας εισβολέας μέσα σε ένα ασύρματο δίκτυο, είναι δυνατόν να πραγματοποιήσει μια επίθεση απευθείας σε ένα workstation. Αν καταφέρει να μπει μέσα σε ένα τέτοιο δίκτυο, μπορεί με την χρήση ενός προγράμματος να εντοπίσει άλλα workstations μέσα στο δίκτυο.
Ακόμα και αν δεν μπορεί να επιτεθεί σε εσωτερικά συστήματα ή να κρυφακούσει πληροφορίες που κινούνται μέσα στο δίκτυο, μπορεί να πραγματοποιήσει κάποια επίθεση σε άλλα workstations, παίρνοντας πληροφορίες από αυτά.
Ο τρόπος για να προστατευθούν αυτές οι μηχανές, είναι να χρησιμοποιηθούν κατάλληλα λογισμικά για αντιμετώπιση διάφορων ιών (anti-virus software), που μπορεί να χρησιμοποιηθούν για αυτό τον σκοπό.
Στην περίπτωση όπου υπάρχει υψηλός κίνδυνος, είναι δυνατόν να αναπτυχθούν ακόμα και προσωπικά firewalls στα workstations [31].

Site Security

Αν ένα ασύρματο δίκτυο δεν θεωρείται πλήρως έμπιστο, τότε δεν υπάρχει κανένας λόγος αυτό να τοποθετηθεί σε ένα εσωτερικό δίκτυο όπου θα έχει την ίδια πρόσβαση σε ευαίσθητα συστήματα, όπως άλλα εσωτερικά workstations.
Μια πολύ καλή κίνηση θα ήταν να τοποθετηθεί το ασύρματο δίκτυο ξεχωριστά από το εσωτερικό δίκτυο και ανάμεσα σε αυτά τα δύο να εγκατασταθεί ένα firewall, αν θεωρήσουμε ότι το ασύρματο δίκτυο είναι δημόσιο. Παράλληλα, θα μπορούσε να αναπτυχθεί ένα Σύστημα ανίχνευσης εισβολής (IDS) μέσα στο ασύρματο δίκτυο προκειμένου να μπορεί να ανιχνεύει μη εξουσιοδοτημένους επισκέπτες. Αυτό δεν θα δώσει την δυνατότητα να γνωρίζουμε πού ακριβώς βρίσκεται ο εισβολέας, όμως θα υπάρχει η γνώση πως κάποιος βρίσκεται μέσα στο δίκτυο ενώ δεν θα έπρεπε, αν πραγματοποιεί κάποιο είδος ενεργής επίθεσης [31][39].

Κεφάλαιο 3

Ασφάλεια στα ασύρματα δίκτυα αισθητήρων

3.1 Εισαγωγή
3.2 Πτυχές Ασφάλειας Ασυρμάτων Δικτύων Αισθητήρων
3.3 Επιθέσεις στα ασύρματα δίκτυα αισθητήρων
3.4 Περιορισμοί στα δίκτυα αισθητήρων
3.5 Λύσεις για την ασφάλεια στα ασύρματα δίκτυα αισθητήρων
3.6 Μέτρα αντιμετώπισης
3.7 Εφαρμογές στα ασύρματα δίκτυα αισθητήρων

3.1 Εισαγωγή

Τα ασύρματα δίκτυα αισθητήρων, μπορούν να χαρακτηριστούν ως μια μεγάλη συλλογή από αισθητήρες οι οποίοι είναι σχεδιασμένοι να έχουν μικρές διαστάσεις, επιβάλλοντας έτσι κάποιους περιορισμούς στο υλικό αλλά και στο λογισμικό. Ο κάθε ένας από αυτούς τους κόμβους αισθητήρες λειτουργεί αυτόνομα μέσα σε ένα περιβάλλον από το οποίο συλλέγει χρήσιμες πληροφορίες τις οποίες επεξεργάζεται και στην συνέχεια μεταδίδει στους γείτονες του μέχρι να φτάσουν στον τελικό προορισμό.

Ο κάθε κόμβος αποτελείται από ένα ή περισσότερους microcontrollers, CPUs ή DSP chips τα οποία του δίνουν την δυνατότητα να επεξεργάζεται τα δεδομένα, να προγραμματίζει διάφορες διεργασίες και να ελέγχει την λειτουργικότητα των άλλων συστατικών του υλικού και στην συνέχεια μπορεί να τα αποθηκεύει στην μνήμη του, η οποία όμως είναι περιορισμένη.
Για την ασύρματη επικοινωνία μεταξύ των κόμβων, υπεύθυνος είναι ένας πομποδέκτης. Ως συνήθως η επικοινωνία με radio frequency είναι αυτή που επιλέγεται στις περισσότερες εφαρμογές ασύρματων δικτύων.
Επίσης διαθέτουν μια πηγή ενέργειας, που μπορεί να είναι είτε μπαταρία είτε πυκνωτής, η οποία χρησιμοποιείται για την συλλογή των δεδομένων, την επεξεργασία τους και για την ανταλλαγή των δεδομένων μεταξύ των κόμβων. Η περισσότερη κατανάλωση ενέργειας γίνεται κατά την επικοινωνία του ενός κόμβου με τους υπόλοιπους, παρά κατά την επεξεργασία των δεδομένων ή την συλλογή τους.

Τέλος ακόμα ένα συστατικό κομμάτι του κόμβου είναι και ο αισθητήρας, ο οποίος ουσιαστικά παράγει ένα σήμα ως απόκριση στην αλλαγή μιας φυσικής κατάστασης.

Στην συνέχεια, το αναλογικό αυτό σήμα μετατρέπεται σε ψηφιακό, μέσω ενός μετατροπέα και αποστέλλεται για περαιτέρω επεξεργασία [48][54].

Λόγω του εχθρικού αφύλακτου περιβάλλοντος στο οποίο ίσως να λειτουργούν, και λόγω των ευαίσθητων πληροφοριών που πιθανώς να επεξεργάζονται, πρέπει οι πληροφορίες να προστατεύονται έτσι ώστε να διατηρείται η ακεραιότητα των δεδομένων.

Οι παραδοσιακές τεχνικές ασφάλειας είναι αδύνατον να εφαρμοστούν και στα δίκτυα αισθητήρων.
Αυτό οφείλεται στην περιορισμένη ενέργεια που έχουν οι αισθητήρες στην διάθεση τους, στους περιορισμένους υπολογισμούς που μπορούν να πραγματοποιήσουν, όπως επίσης και στον περιορισμένη χωρητικότητα μνήμης.
Μια ακόμα βασική διαφορά είναι και η δυνατότητα αλλοίωσης ή καταγραφής των δεδομένων από κάποιους εξωτερικούς παράγοντες [37][34].

3.2 Πτυχές Ασφάλειας Ασυρμάτων Δικτύων Αισθητήρων

Λόγω των αναξιόπιστων καναλιών επικοινωνίας μεταξύ των κόμβων και του αφύλακτου τρόπου λειτουργίας τους, δυσκολεύουν ακόμα περισσότερο το έργο της αντιμετώπισης επιθέσεων οι οποίες λειτουργούν εκμεταλλευόμενες αυτά τα χαρακτηριστικά των ασύρματων δικτύων [34].

Οι πτυχές της ασφάλειας στα ασύρματα δίκτυα αισθητήρων μπορούν να χωριστούν σε τρεις βασικές κατηγορίες οι οποίες είναι τα *εμπόδια στην ασφάλεια των ασύρματων δικτύων, οι απαιτήσεις ενός ασφαλούς ασύρματου δικτύου αισθητήρων, οι επιθέσεις και τα μέτρα αντιμετώπισης τους* [37][34][24].

Λόγω της ιδιαιτερότητας των ασύρματων δικτύων αισθητήρων και της διαφοράς που εμφανίζουν από τα παραδοσιακά δίκτυα, δεν είναι δυνατόν να εφαρμοστούν οι ίδιες τεχνικές και στις δύο περιπτώσεις.
Στην περίπτωση των ασύρματων δικτύων αισθητήρων, χρειάζεται να γίνεται εξοικονόμηση της ενέργειας του κάθε αισθητήρα γιαυτό και παρουσιάζονται περιορισμοί στην επεξεργασία των δεδομένων τους και στην μεταξύ τους επικοινωνία. Ακόμα ένας σημαντικός παράγοντας ο οποίος δεν επιτρέπει την απευθείας εφαρμογή των τεχνικών που χρησιμοποιούνται στα υπόλοιπα δίκτυα, οφείλεται στο ότι οι αισθητήρες είναι τοποθετημένοι σε περιβάλλοντα στα οποία υπάρχουν πολλές φυσικές απειλές και είναι εύκολα προσβάσιμα από ανθρώπινο παράγοντα[24].
Προκειμένου λοιπόν να αναπτυχθεί ένας αποτελεσματικός μηχανισμός ασφάλειας στα ασύρματα δίκτυα αισθητήρων, χρησιμοποιώντας ιδέες και τεχνικές που

εφαρμόζονται στα παραδοσιακά δίκτυα, χρειάζεται να γνωστοποιηθούν αρχικά όλα τα εμπόδια που περιορίζουν την δημιουργία ενός ασφαλούς δικτύου [37].

Για την σωστή λειτουργία των αισθητήρων λοιπόν, χρειάζεται μια συγκεκριμένη ποσότητα πόρων, όπως είναι η μνήμη και η ενέργεια.

Όσο αφορά λοιπόν την μνήμη των κόμβων, αυτή είναι πολύ περιορισμένη, προκειμένου οι κόμβοι να μπορούν να λειτουργούν αποτελεσματικά. Οπότε για την αποθήκευση των δεδομένων και για τον κώδικα χρειάζεται ένα πολύ μικρό μέρος της μνήμης, γιαυτό και ο κώδικας ασφάλειας πρέπει να είναι επίσης πολύ περιορισμένος [37][34][24].

Ένας ακόμα σοβαρός περιοριστικός παράγοντας είναι και η ενέργεια. Οι κόμβοι βρίσκονται διασκορπισμένοι σε ένα περιβάλλον μαζεύοντας διάφορες πληροφορίες. Για τον λόγο αυτό δεν μπορεί να γίνεται μεγάλη σπατάλη ενέργειας, αφού η αντικατάσταση των κόμβων από καινούργιους ή ακόμα και η επαναφόρτιση τους, κοστίζει. Οπότε κύριο μέλημα είναι να διατηρηθεί η ενέργεια για όσο μεγαλύτερο χρονικό διάστημα είναι δυνατόν[34][24].
Η ενέργεια που καταναλώνεται από ένα κώδικα ο οποίος προστίθεται στον κόμβο για λόγους ασφαλείας , οφείλεται στην επεξεργασία των συναρτήσεων για κρυπτογράφηση, αποκρυπτογράφηση κτλ, στην μετάδοση δεδομένων που σχετίζονται με την ασφάλεια και την αποθήκευση παραμέτρων ασφαλείας [34].
Μια ακόμα απειλή προς τα ασύρματα δίκτυα αισθητήρων είναι και η αναξιόπιστη επικοινωνία που μπορεί να υπάρξει μεταξύ των κόμβων.

Τα πακέτα κινούνται μέσα στο δίκτυο ανεξάρτητα μεταξύ τους. Το κάθε πακέτο μπορεί να ακολουθεί διαφορετικό μονοπάτι δρομολόγησης, σύμφωνα με τον τύπο του πρωτοκόλλου δρομολόγησης που χρησιμοποιείται.
Λόγω λοιπόν αυτής της αναξιόπιστης επικοινωνίας μεταξύ των κόμβων, είναι πιο εύκολο να καταστραφούν πακέτα κατά την μετάδοση τους.
Ακόμα και στην περίπτωση όπου η επικοινωνία μεταξύ των κόμβων είναι αξιόπιστη, υπάρχει το ενδεχόμενο να προκύψουν συγκρούσεις μεταξύ των πακέτων. Αυτό συμβαίνει κυρίως σε περιπτώσεις όπου υπάρχει μεγάλη συμφόρηση μέσα στο δίκτυο οπότε κάποια πακέτα κατά την μετάδοση τους υπάρχει η πιθανότητα να βρεθούν και να συγκρουστούν μεταξύ τους. Σε ένα δίκτυο όπου υπάρχει μεγάλη κίνηση των πακέτων, αυτό είναι και το κυριότερο πρόβλημα.

Εξαιτίας του τρόπου με τον οποίο λειτουργούν τα ασύρματα δίκτυα αισθητήρων, οι κόμβοι μένουν αφύλακτοι και εκτεθειμένοι σε φυσικές επιθέσεις για μεγάλα χρονικά διαστήματα. Οπότε σύμφωνα με τα [37][34][24], ένας κόμβος ενός ασύρματου δικτύου είναι πιο πιθανόν να αντιμετωπίσει περισσότερες επιθέσεις, οι οποίες προέρχονται από φυσικούς παράγοντες, παρά από ένα Η/Υ ο οποίος βρίσκεται τοποθετημένος σε ένα ασφαλισμένο περιβάλλον και αντιμετωπίζει επιθέσεις μέσω του δικτύου.

Η απομακρυσμένη διαχείριση των κόμβων, καθιστά αδύνατη την ανίχνευση κάποιων αλλοιώσεων από το φυσικό περιβάλλον, ή να αντιληφθεί κάποιος πως η ενέργεια του κόμβου έχει εξαντληθεί.

3.3 Επιθέσεις στα ασύρματα δίκτυα αισθητήρων

Τα δίκτυα αισθητήρων είναι πολύ ευαίσθητα σε επιθέσεις, ειδικότερα σε επιθέσεις άρνησης υπηρεσιών, οι οποίες είναι και οι πιο συχνά εμφανιζόμενες. Υπάρχει ένας μεγάλος αριθμός τεχνικών όπως είναι οι επιθέσεις σε πρωτόκολλα δρομολόγησης αλλά και επιθέσεις στην φυσική ασφάλεια των κόμβων, μερικές από τις οποίες περιγράφονται στην συνέχεια:

Physical Layer

Ο βασικός σκοπός του φυσικού επιπέδου είναι να αυξήσει την αξιοπιστία. Είναι υπεύθυνο για την εγκαθίδρυση σύνδεσης, για την επικοινωνία μεταξύ κάποιων κόμβων, για τον ρυθμό μετάδοσης των δεδομένων, για την κρυπτογράφηση των δεδομένων, την επιλογή της συχνότητας κτλ. Συγκρίνοντας τις απειλές που δέχονται τα παραδοσικά δίκτυα στο φυσικό επίπεδο, με τις απειλές που δέχονται τα ασύρματα δίκτυα αισθητήρων, αυτές είναι πολύ περισσότερες [4][11].

- Jamming

Οι κόμβοι σε ένα ασύρματο δίκτυο, επικοινωνούν με radio frequencies, σύμφωνα με τα [1][4][11][5], οπότε κάποιος εισβολέας μπορεί να προκαλέσει παρεμβολές σε αυτές τις συχνότητες.
Κάποιος λοιπόν που μπορεί να ελέγχει μερικούς κόμβους στο δίκτυο, μπορεί να έτσι να δημιουργήσει διαταραχή στην επικοινωνία ολόκληρου του δικτύου, προκαλώντας σκόπιμες παρεμβολές με radio frequencies[4]. Το πρόβλημα αυτό είναι μεγαλύτερο στην περίπτωση όπου οι κόμβοι επιλέγονται με στρατηγικό τρόπο ώστε να έχουν την δυνατότητα να ‘μπλοκάρουν’ περισσότερες επικοινωνίες στο δίκτυο[1].
Μπορεί κάποιος να παρεμβάλει επιπρόσθετα πακέτα στο δίκτυο, τα οποία οι υπόλοιποι κόμβοι στην προσπάθεια τους να τα λάβουν, καταναλώνουν ενέργεια άσκοπα, μιας και αυτά τα πακέτα δεν είναι νόμιμα[11]. Στο ίδιο άρθρο αναφέρεται επίσης πως στην περίπτωση που σε όλο το δίκτυο χρησιμοποιείται μονάχα μία συχνότητα, αυτό μπορεί να προκαλέσει κατάρρευση ολόκληρου του δικτύου

- Tampering

Σε αυτό τον τύπο επίθεσης, ο επιτιθέμενος εκμεταλλεύεται την φύση των WSNs, η οποία του επιτρέπει να έχει πολύ εύκολη πρόσβαση στους κόμβους, και να αποκτήσει τον πλήρη έλεγχο κάποιου κόμβου. Ο λόγος που η πρόσβαση στους κόμβους καθίσταται υπερβολικά εύκολη οφείλεται στο γεγονός ότι οι κόμβοι δεν επιβλέπονται, αφού πρέπει να είναι όσο το δυνατόν πιο φτηνοί, οπότε και δεν υπάρχει καμιά απόδειξη σε περίπτωση παραβίασης. Στην συνέχεια ο επιτιθέμενος μπορεί πολύ εύκολα να αντλήσει σημαντικές πληροφορίες όπως για παράδειγμα κλειδιά κρυπτογράφησης και άλλα σημαντικά δεδομένα από τον κόμβο.
Οι επιθέσεις tampering μπορούν να χωριστούν σε δύο κατηγορίες, Invasive attacks και Non Invasive attacks.
Στο invasive attack απαιτείται πρόσβαση στα υλικά συστατικά όπως είναι τα chips. Αυτό το είδος επίθεσης απαιτεί ακριβότερο εξοπλισμό και περισσότερο χρόνο σε σχέση με την non invasive επίθεση[16].

- Sybil attack

Διαφορετικά ονομάζεται και Identity attack και περιγράφει την περίπτωση επίθεσης όπου ο επιτιθέμενος, μπορεί να αποκτήσει παράνομα πολλές ταυτότητες ταυτόχρονα μέσα στο δίκτυο.
Οι ταυτότητες αυτές που παρουσιάζει ο malicious node μπορεί να είναι είτε κατασκευασμένες είτε κλεμμένες από άλλους κόμβους που υπάρχουν μέσα στο δίκτυο[4], και οι οποίοι σε αυτή την περίπτωση ονομάζονται Sybil nodes [5].
Η διαδικασία κατά την οποί ο κακόβουλος κόμβος αποκτά τις νέες ταυτότητας έχει ως εξής:

Στην περίπτωση όπου έχουμε κατασκευασμένες ταυτότητες, ο επιτιθέμενος δημιουργεί στην ουσία κάποιες αυθαίρετες Sybil ταυτότητες παράγοντας αυθαίρετους τυχαίους αριθμούς σαν αναγνωριστικά για τους Sybil κόμβους

Στην περίπτωση όπου οι ταυτότητες είναι κλεμμένες, ο επιτιθέμενος αναγνωρίζει τις ταυτότητες όλων των κόμβων μέσα στο δίκτυο και στην συνέχεια τις αναθέτει στους Sybil nodes που παράγονται από τον επιτιθέμενο.

Ο κακόβουλος κόμβος λοιπόν μπορεί να παρουσιάζεται ως ένας Sybil node αποστολέας στους υπόλοιπους κόμβους, στους οποίους στέλνει κακόβουλα μηνύματα ή λανθασμένες πληροφορίες, όπως για παράδειγμα θέσεις κόμβων, ισχύ κάποιου σήματος κτλ όπως αναφέρεται στα [45][5].
Κάτι παρόμοιο συμβαίνει και στην περίπτωση όπου οι άλλοι κόμβοι στην προσπάθεια τους να στείλουν πακέτα σε κάποιον Sybil node τα στέλνουν στην πραγματικότητα στον εισβολέα [5].
Μια άλλη περίπτωση του Sybil attack είναι να απαγορεύει την πρόσβαση στους Sybil nodes από τους υπόλοιπους για άμεση επικοινωνία, οπότε ο κακόβουλος κόμβος δρα ως μεσολαβητής. Ουσιαστικά το τι κάνει είναι να λαμβάνει τα μηνύματα που

προορίζονται προς τους Sybil, χωρίς όμως στην πραγματικότητα να τα προωθεί προς αυτούς [5].

Το Sybil attack μπορεί να αποτελέσει μια σημαντική απειλή για το γεωγραφικό πρωτόκολλο δρομολόγησης. Σύμφωνα με το [18], κατά την ανταλλαγή πληροφοριών μεταξύ κόμβων προκειμένου να δρομολογηθεί σωστά ένα πακέτο, στην περίπτωση επίθεσης, ένας κόμβος μπορεί να εμφανίζεται πολλές φορές σε διαφορετικούς τόπους ταυτόχρονα προκαλώντας έτσι πρόβλημα στην δρομολόγηση του πακέτου. Στην ουσία αυτό που γίνεται είναι να παρέχονται πολλά διαφορετικά hops [45][4].

Data Link Layer

Αυτό το επίπεδο είναι υπεύθυνο για την πολύπλεξη της ροής των δεδομένων, κατά την οποία πολλαπλά αναλογικά ή ψηφιακά σήματα συνδιάζονται σε ένα σήμα, σε ένα κοινό μέσο. Επίσης το data link layer είναι υπεύθυνο για την ανίχνευση και τον έλεγχο των λαθών, την παρεμπόδιση της σύγκρουσης των πακέτων κτλ.
Ο λόγος που αυτό το επίπεδο είναι εξίσου ευαίσθητο σε διάφορες επιθέσεις, οφείλεται στο ότι τα δεδομένα και οι πληροφορίες μεταφέρονται σε ένα ανοικτό, μη ασφαλισμένο μέσο. Μερικές από τις επιθέσεις που μπορούν να γίνουν στο επίπεδο αυτό περιγράφονται παρακάτω [4][11][44].

- Collision

Ο επιτιθέμενος σε αυτή την περίπτωση αυτό που επιδιώκει είναι να ακούσει την συχνότητα πάνω στην οποία μεταδίδονται τα πακέτα μέσα στο δίκτυο[9]. Μόλις λοιπόν "ακούσει" ένα κόμβο ο οποίος μεταδίδει ένα πακέτο σε ένα άλλο κόμβο τότε στέλνει ένα δικό του σήμα δημιουργώντας έτσι παρεμβολή [16][9].
Ουσιαστικά θα μπορούσαμε να πούμε πως στέλνεται ένα μικρό πακέτο με θόρυβο από τον κακόβουλο κόμβο το οποίο συγκρούεται με τις μεταδόσεις των γειτόνων του. Αυτό έχει ως συνέπεια το πακέτο αυτό να φθάνει αλλοιωμένο στον παραλήπτη. Λόγω αυτής της αλλαγής από την σύγκρουση, το πακέτο θα αποτύχει στον έλεγχο checksum και ο παραλήπτης θα ζητήσει να του ξανασταλεί το ίδιο πακέτο,οπότε έχουμε αναμετάδοση (retransmission) [1][9]. Η αλλαγή της τιμής ενός μόνο byte είναι αρκετή για να δημιουργήσει CRC error κατά τον έλεγχο, και να καταστραφεί το μήνυμα[16].
Συγκρίνοντας το collision attack με το jamming attack, όπως γίνεται στα άρθρα [16][9], παρατηρείται πως το collision attack έχει πλεονέκτημα, λόγω του ότι κυρίως ακούει πακέτα που μεταδίδονται πάνω στο δίκτυο, σε αντίθεση με το jamming το οποίο μεταδίδει άλλα μη νόμιμα πακέτα. Αφού λοιπόν η κατανάλωση ενέργειας για μετάδοση πακέτων είναι πολύ μεγαλύτερη από την κατανάλωση που γίνεται όταν απλώς ο εισβολέας 'ακούει' για πακέτα, γίνεται μεγάλη εξοικονόμηση ενέργειας του

κόμβου.
Ένα άλλο πλεονέκτημα στο οποίο και πάλι συμφωνούν τα δύο άρθρα,[16][9], είναι πως υπάρχει χαμηλή κατανάλωση ενέργειας από την συσκευή η οποία προκαλεί την επίθεση και αυτό οφείλεται στο ότι ο χρόνος κατά τον οποίο γίνονται ραδιομεταδόσεις είναι πολύ μικρότερος σε σχέση με τον χρόνο που σπαταλάται από το jamming σε αυτές. Ουσιαστικά όπως προαναφέρθηκε το jamming έχει ως απώτερο σκοπό την παρεμβολή συχνοτήτων.
Ένα ακόμα πλεονέκτημα του collision έναντι του jamming είναι το ότι δύσκολα μπορεί να ανιχνευθεί η πρώτη επίθεση, αφού η μοναδική απόδειξη είναι το αλλοιωμένο μήνυμα που φθάνει στον παραλήπτη.
Στο [16] αναφέρεται πως στόχος αυτής της επίθεσης είναι να εξαντληθεί η ενέργεια των υπολοίπων κόμβων, αφού με την συνεχή αποστολή αλλοιωμένων πακέτων αυτά απορρίπτονται στον έλεγχο και ξαναστέλνονται συνεχώς. Αυτό όμως εκτός του ότι προκαλεί άσκοπη σπατάλη του bandwidth, μειώνει μέχρι και εξαφανίζει τις πιθανότητες ο κόμβος να μπει σε sleep mode. Αυτό βοηθά στο να εξαντλούνται οι απαραίτητοι για το δίκτυο πόροι που είναι η ενέργεια, τόσο του παραλήπτη όσο και του αποστολέα κόμβου[7].
Το αποτέλεσμα από αυτή την επίθεση θα είναι η μερική υποβάθμιση του δικτύου, ίσως και ολόκληρου σε περίπτωση που οι "μολυσμένοι" κόμβοι είναι περισσότεροι από ένα.

- Spoofed, altered, or replayed routing information

Αυτός ο τύπος επίθεσης επιδιώκει την αλλοίωση των πληροφοριών των δεδομένων που ανταλλάζουν μεταξύ τους οι δρομολογητές του δικτύου. Αυτή είναι η πιο κοινή και άμεση επίθεση εναντίον ενός πρωτοκόλλου δρομολόγησης.
Σύμφωνα με το [8] αλλάζοντας τις πληροφορίες δρομολόγησης από τα πρωτόκολλα δρομολόγησης μέσω ενός κακόβουλου κώδικα, τότε αυτό θα μπορούσε να αλλάξει ολόκληρη την δομή δρομολόγησης του δικτύου.
Τρόποι για να επιτευχθεί το πιο πάνω είναι η πλαστογράφηση, η αλλοίωση ή αναπαραγωγή της πληροφορίας η οποία μεταδίδεται, από τον εισβολέα μπορεί να προκαλέσει σοβαρές ζημιές στο δίκτυο όπως για παράδειγμα βρόγχους δρομολόγησης (ένα πακέτο κινείται μεταξύ ορισμένων δρομολογητών συνεχώς, χωρίς να μπορεί να φτάσει στον τελικό του προορισμό), μπορούν να προσελκύσουν ή να απωθήσουν την κυκλοφορία του δικτύου από ένα συγκεκριμένο κόμβο σε αυτό, μπορούν να μεταβάλουν τις διαδρομές δρομολόγησης προς τον τελικό προορισμό μεγαλώνοντας ή μικραίνοντας τες, υπάρχει η πιθανότητα δημιουργίας ψευδών μηνυμάτων κτλ. [18][50][4][33].
Τα WSNs παρουσιάζονται πιο ευάλωτα σε τέτοιου είδους επιθέσεις λόγω του ότι κάθε κόμβος στο δίκτυο συμπεριφέρεται και ως router. Οπότε κάθε κόμβος μπορεί να έχει άμεση πρόσβαση στις πληροφορίες των δεδομένων που κινούνται στο δίκτυο και κατά συνέπεια αυτό διευκολύνει το έργο των εισβολέων.[17]
Επιπλέον ένας τρόπος αντιμετώπισης τέτοιων επιθέσεων σύμφωνα με το [33] είναι η

αυθεντικοποίηση όπου ένας router θα δέχεται δεδομένα μόνο από ένα άλλο router του οποίου η ταυτότητα έχει ελεγχθεί.

- Exhaustion attack

Σύμφωνα με το άρθρο [1], η επίθεση exhaustion χρησιμοποιεί την επίθεση collision πολλαπλές φορές προκειμένου να εξαντλήσει την ενέργεια των κόμβων που επικοινωνούν μεταξύ τους [7].
Το τι ακριβώς γίνεται, είναι να εισάγονται collisions στα frames, στο τέλος της μετάδοσης, οπότε ο κόμβος αναγκάζεται να κάνει retransmit τα πακέτα του συνεχώς μέχρι να εξαντληθεί η ενέργεια του[16].
Μια ακόμα λύση που προτείνεται, είναι να τεθεί ένα χρονικό όριο για τον κάθε κόμβο του δικτύου, μέσα στο οποίο να μπορεί να έχει πρόσβαση πάνω στο κανάλι προκειμένου να μεταδώσει τα πακέτα του σε κάποιους άλλους κόμβους. Με αυτό τον τρόπο περιορίζεται η υπερβολική χρήση του καναλιού MAC[16].
Η επίθεση αυτή παρουσιάζει τα ίδια χαρακτηριστικά με το collision attack με την μόνη διαφορά ότι το exhaustion attack εκμεταλλεύεται το checksum fault του μεταδιδόμενου πακέτου.

- Acknowledgement spoofing

Η επίθεση αυτή βασίζεται στο ότι πολλοί αλγόριθμοι δρομολόγησης στα ασύρματα δίκτυα εξαρτώνται είτε έμμεσα είτε άμεσα από τα acknowledgements [23][18][33][51].
Ένα πρωτόκολλο λοιπόν το οποίο χρησιμοποιεί link-layer acknowledgements τότε αυτά για πακέτα τα οποία μπορεί να ακούσει ο εισβολέας, μπορεί να πλαστογραφηθούν. Η πλαστογράφηση αυτή μπορεί να πείσει τους υπόλοιπους κόμβους που στέλνουν κάποια acks σε άλλους κόμβους του δικτύου, οι οποίοι είναι αδύναμοι ή απενεργοποιημένοι, ότι είναι δυνατοί ή ενεργοποιημένοι για να δεχτούν οποιοδήποτε πακέτο[23][18][17][33][51].
Ουσιαστικά το τι γίνεται, είναι ότι ο εισβολέας απαντά στο ack του άλλου κόμβου προσποιούμενος τον παραλήπτη του ack, πλαστογραφώντας το[33]. Όπως φαίνεται και στο [18][33] τα πακέτα τα οποία καταλήγουν σε αυτούς τους κόμβους χάνονται. Σε αυτό το σημείο αφού τα πακέτα τα οποία μεταδίδονται πάνω σε “νεκρές” ή “αδύναμες” γραμμές χάνονται,τότε μπορεί να ξεκινήσει ένα selective forwarding attack χρησιμοποιώντας acknowledgment spoofing προκειμένου να μπορεί να πείσει τους κόμβους να στέλνουν τα πακέτα τους μέσω αυτών των γραμμών [18][33]. Έτσι επιλεκτικά εμποδίζει την διάδοση των πακέτων που προέρχονται από κάποιους συγκεκριμένους κόμβους.
Ένας καλός τρόπος για την αντιμετώπιση τέτοιου είδους επιθέσεων είναι η εφαρμογή καλών τεχνικών κρυπτογράφησης και ύπαρξη κατάλληλης αυθεντικοποίησης για την επικοινωνία[33].

Network Layer

Το επίπεδο αυτό είναι υπεύθυνο για την ανάθεση των διευθύνσεων στα πακέτα και για να καθορίζει τον τρόπο με τον οποίο θα δρομολογούνται αυτά μέσα στο δίκτυο. Ο σκοπός του network layer είναι να παρέχει μια αξιόπιστη μετάδοση των πακέτων από το ένα άκρο στο άλλο.
Το βασικότερο θέμα είναι ότι κάθε κόμβος λειτουργεί routing hop, επιτρέποντας με αυτό τον τρόπο την ύπαρξη πολλών επιθέσεων [4][11].

- Selective forwarding

Το selective forwarding επηρεάζει την επικοινωνία σε ένα multi-hop δίκτυο. Ενώ αναμένεται όλοι οι κόμβοι να μεταδίδουν κανονικά τα πακέτα τους στον προορισμό τους, εντούτοις υπάρχει περίπτωση αυτό να μην γίνεται. Σε αυτή την περίπτωση έχουμε ένα εισβολέα στο δίκτυο[18][50][1][40].
Στο [23][18][33][8] αναφέρεται πως ένας εισβολέας όταν καταστρέφει όλα τα πακέτα, προκειμένου αυτά να μην μεταδοθούν παρακάτω, συμπεριφέρεται ως black hole. Αυτό όμως είναι ένα ρίσκο αφού οι υπόλοιποι κόμβοι οι οποίοι προωθούν τα πακέτα τους στον συγκεκριμένο, υποψιάζονται πως αυτός αποτυγχάνει να μεταδώσει τα πακέτα παρακάτω, και έτσι αναζητούν ένα νέο κόμβο αντικαθιστώντας τον. Για να αποφευχθεί αυτό, ο κακόβουλος κόμβος δεν ‘πετά’ όλα τα πακέτα. Τα [50][40][33] αναφέρουν πως τέτοιοι κόμβοι μπορούν απλώς να καταστρέφουν ή να αλλοιώνουν πακέτα τα οποίοι προέρχονται από συγκεκριμένους κόμβους τους δικτύου.
Για μεγαλύτερη αποτελεσματικότητα, σύμφωνα με το [18], ο εισβολέας επιλέγει να ‘μολύνει’ κάποιο κόμβο ο οποίος βρίσκεται κοντά ή ακόμα καλύτερα πάνω στο μονοπάτι της ροής των δεδομένων. Αυτό συμβαίνει γιατί μπορεί να έχει πιο εύκολη πρόσβαση στα πακέτα τα οποία κινούνται στο δίκτυο και μπορεί να ελέγχει ακόμα περισσότερα πακέτα ιδίως όταν ο κόμβος είναι κοντά στην πηγή ή στον τελικό παραλήπτη[18][40].
Είναι επίσης δυνατόν ένας κακόβουλος κόμβος ο οποίος μπορεί να ακούσει μια ροή από μηνύματα, να ξεκινήσει ένα selective forwarding attack χρησιμοποιώντας jamming ή collision attack σε κάθε πακέτο που προωθείται μέσα στο δίκτυο και επιθυμεί να το καταστρέψει.

Όπως γράφεται στο [17], η επίθεση αυτή μπορεί να προκαλέσει Dos attack για ένα συγκεκριμένο κόμβο. Δηλαδή ένας κόμβος υπάρχει περίπτωση να παραμένει μπλοκαρισμένος επ' αόριστον χωρίς να μπορεί να στείλει κανένα πακέτο στον τελικό παραλήπτη.
Ο τρόπος για να ανιχνευθεί το selective forwarding attack, είναι να ελέγχονται συνεχώς τα sequence numbers των πακέτων, και με την πρόσθεση data packet sequence number στο packet header[33].

- Sinkhole (Blackhole attack) attack

Σε αυτή την περίπτωση, γίνεται μια προσπάθεια προσέλκυσης της κίνησης του δικτύου, σύμφωνα με το πρωτόκολλο το οποίο χρησιμοποιείται στο δίκτυο.[18][50][45]
Σύμφωνα λοιπόν με τα άρθρα [18][50][1], ο επιτιθέμενος ο οποίος παραβιάζει ένα κόμβο του δικτύου, αναπαράγει ή πλαστογραφεί μια 'διαφήμιση' κατά την οποία παρουσιάζει τον εαυτό του να προσφέρει μια πολύ υψηλή ποιότητα δρομολόγησης των πακέτων προς τον τελικό παραλήπτη [8].
Σε αυτή την περίπτωση λοιπόν το τι γίνεται είναι αν το πρωτόκολλα δρομολόγησης το οποίο χρησιμοποιείται είναι 'low cost route first', τότε ο κάθε κόμβος ο οποίος μεταδίδει το πακέτο του προς το παραλήπτη, ψάχνει τον επόμενο κόμβο για τον οποίο απαιτείται το λιγότερο κόστος. Με αυτό τον τρόπο οι άλλοι κόμβοι θα τον επιλέξουν ως ενδιάμεσο κόμβο έτσι ώστε να φτάσουν τα πακέτα τους στον τελικό προορισμό.[1]
Με αυτό τον τρόπο δημιουργείται μια μαύρη τρύπα (black hole) στο δίκτυο, με κέντρο τον προσβαλλόμενο κόμβο, μαζεύεται δηλαδή ένας μεγάλος αριθμός από πακέτα σε αυτό τον κόμβο ο οποίος επιλεκτικά τα καταστρέφει ή τα αλλοιώνει.[18][1][4][11]
Στο [33] αναφέρεται πως ο εισβολέας επιλέγει και μολύνει συνήθως ένα κόμβο ο οποίος βρίσκεται κοντά στον κόμβο για τον οποίο προορίζεται το πακέτο, έτσι ώστε να μπορεί να παρουσιαστεί ως ο κόμβος παραλήπτης, όπως επίσης στα [23][18][50], ο κόμβος επιλέγεται να είναι όσο πιο κοντά ή ακόμα καλύτερα πάνω στο μονοπάτι δρομολόγησης, έτσι ώστε να μπορεί να 'πειράξει' όσο περισσότερα πακέτα γίνεται.
Ένα ακόμα μεγαλύτερο πρόβλημα που μπορεί να δημιουργήσει ένας επιτιθέμενος στο δίκτυο, είναι χρησιμοποιώντας ένα laptop και παρέχοντας πολύ καλή ποιότητα δρομολόγησης. Οπότε με αυτό τον τρόπο οι υπόλοιποι γειτονικοί κόμβοι θα προτιμήσουν τον κακόβουλο κόμβο σαν ενδιάμεσο κόμβος, στέλνοντας του τα πακέτα τους [8]. Μπορεί να προσεγγίσει ακόμα και κόμβους οι οποίοι βρίσκονται μερικά hops μακριά από τον παραλήπτη.
Κατά συνέπεια αυτή η επίθεση κάνει το selective forwarding να φαίνεται ακόμα πιο εύκολο [18][11][51].
Ουσιαστικά το τι επιτυγχάνει αυτή η επίθεση είναι προσελκύει την κίνηση από γειτονικούς κόμβους μέχρι και κόμβους οι οποίοι βρίσκονται μέχρι και αρκετά hops πιο πέρα από τον μολυσμένο κόμβο.[18][33]
Ο λόγος λοιπόν που τα WSNs είναι ευάλωτα σε αυτό τον τύπο επίθεσης είναι γιατί όλοι οι κόμβοι του δικτύου προσπαθούν να στείλουν τα πακέτα τους στον ίδιο τελικό προορισμό. Οπότε μόλις βρεθεί κάποιος κόμβος ο οποίος μπορεί να παρέχει μια πολύ υψηλή ποιότητα μετάδοσης, σε σχέση με τους άλλους, μπορεί να προσελκύσει ένα μεγάλο αριθμό κόμβων[18].

- Wormhole attack

Σε αυτό το είδος επίθεσης συνήθως χρειάζονται 44 προσβαλλόμενοι κόμβοι[17][5], όπου σε αυτή την περίπτωση, σύμφωνα με τα [50][1][17][4][11] δημιουργείται ένα

wormhole link μεταξύ των δύο κόμβων. Μέσω αυτού του link στέλνονται πακέτα, πληροφορίες δρομολόγησης, ACKs κτλ σε ένα άλλο σημείο του δικτύου. Όλες αυτές οι πληροφορίες ελευθερώνονται σε ένα άλλο σημείο του δικτύου το οποίο μπορεί να είναι πολύ μακριά από τον προσβαλλόμενο κόμβο που τα στέλνει.
Ο επιτιθέμενος θα μπορούσε να προσβάλει ένα κόμβο ο οποίος βρίσκεται πολύ κοντά στον τελικό προορισμό, οπότε με αυτό τον τρόπο θα μπορούσε να διαταράξει ολόκληρη την δρομολόγηση των πακέτων [18]. Ουσιαστικά με την επιλογή αυτού του κόμβου σαν κακόβουλος θα μπορούσε με την δημιουργία ενός wormlink να πείσει όλους τους υπόλοιπους κόμβους μέσα στο δίκτυο, ακόμα και αυτούς που βρίσκονται hops μακριά να του στείλουν τα πακέτα τους.
Ο επιτιθέμενος, με το worm hole, μπορεί να ξεγελάσει τους γειτονικούς κόμβους πως ο παραλήπτης του πακέτου είναι μόνο 43-44 Hops μακριά, μέσω του wormhole, ενώ είναι πολλά περισσότερα μακριά.[18][33]. Ένα παράδειγμα το wormhole σύμφωνα με το άρθρο [41] είναι η περίπτωση όπου έχουμε 44 εισβολείς Α και Β όπου ο Α στέλνει δεδομένα στον Β, οποίος μπορεί να βρίσκεται πολύ πιο μακριά από τον Α, μέσω ενός καναλιού (wormhole). Στην συνέχεια ο Β αναμεταδίδει το μήνυμα όπως ακριβώς το έλαβε από τον κόμβο Α, στους γειτονικούς του κόμβους, κάνοντας τους να πιστεύουν πως ο αρχικός αποστολέας είναι μόνο μερικά Hops μακριά.

- Hello flood

Υπάρχουν κάποια πρωτόκολλα τα οποία απαιτούν να γίνεται ένα broadcast από όλους τους κόμβους του δικτύου έτσι ώστε να γνωρίσει ο κάθε ένας τον γείτονα του. Ουσιαστικά μεταδίδονται hello πακέτα μεταξύ κόμβων. Κάθε κόμβος ο οποίος λαμβάνει από κάποιον άλλο ένα πακέτο, είναι σίγουρος πως αυτός είναι γείτονας του. Αυτό όμως δεν μπορεί να ισχύει πάντα αφού ένας εισβολέας μπορεί (με ένα laptop) να αρχίσει να μεταδίδει πληροφορίες δρομολόγησης ή άλλες πληροφορίες προς τους υπόλοιπους κόμβους, με μεγάλη ισχύ[18][45]. Εδώ μπορεί να σημειωθεί πως ο επιτιθέμενος δεν χρειάζεται να δημιουργήσει μια νόμιμη κίνηση μέσα στο δίκτυο αλλά να κάνει rebroadcast,record ή replay άλλα πακέτα[18][17]. Αφού λοιπόν μεταδίδονται πακέτα μέσα στο δίκτυο, αυτό θα έχει ως αποτέλεσμα πολλοί κόμβοι οι οποίοι είναι αρκετά hops μακριά, να τον αναγνωρίσουν ως γείτονα τους και να αρχίσουν να ανταλλάζουν δεδομένα με αυτόν [50][41][1][17].
Το αποτέλεσμα από αυτή την ανταλλαγή δεδομένων, όπου ίσως οι περισσότεροι κόμβοι είναι αρκετά μακριά από τον εισβολέα, είναι η ύπαρξη Multi-hop routed μηνυμάτων, μηνυμάτων δηλαδή που διανύουν μια απόσταση πολλών hop για να φτάσουν στον κακόβουλο κόμβο. Κατά συνέπεια έχουμε αύξηση της καθυστέρησης, χάσιμο δεδομένων, ακόμα και σπατάλη ενέργειας των κόμβων[45][33][51].
Στο άρθρο [33], στην περίπτωση όπου ο κακόβουλος κόμβος διαφημίζει τον εαυτό του για χαμηλού κόστους δρομολογήσεις, μπορεί επίσης να πείσει τους υπόλοιπους κόμβους να προωθήσουν τα πακέτα τους προς αυτόν. Στο ίδιο άρθρο, αναφέρεται πως τα hello flood μπορούμε να πούμε πως είναι one-way broadcast wormholes, αφού μπορούν να sπροσελκύσουν άλλους κόμβους και να μεταφέρουν τα μηνύματα τους σε ένα άλλο σημείο του δικτύου.

Αυτή η επίθεση μπορεί να αντιμετωπιστεί ελέγχοντας την αναδρομικότητα της γραμμής πριν να χρησιμοποιηθεί από οποιονδήποτε κόμβο. Στην περίπτωση που στο άλλο άκρο της γραμμής βρίσκεται ένας κακόβουλος κόμβος τότε ένας υγιής κόμβος δεν θα έχει την δυνατότητα λήψης πακέτων με τον μολυσμένο κόμβο [33].

Application Layer

Το application layer είναι υπεύθυνο για την συλλογή των δεδομένων την διαχείριση και την επεξεργασία τους μέσω ενός application software, για να πάρει τις χρήσιμες πληροφορίες.
Μερικοί από τους ιούς οι οποίοι μπορούν να λειτουργήσουν λόγω κάποιων αδυναμιών πάνω σε αυτό το επίπεδο αναφέρονται αναλυτικά πιο κάτω [55][44].

- Flooding

Ο βασικός σκοπός αυτού του τύπου επίθεσης όπως αναφέρεται στο [1][11][16] είναι να εξαντλήσει τους πόρους, την μνήμη και την ενέργεια δηλαδή, ενός άλλου κόμβου θύματος.
Ο τρόπος που γίνεται αυτό , είναι ένας κακόβουλος κόμβος να στέλνει συνέχεια αιτήματα σύνδεσης στους άλλους κόμβους του δικτύου, τα οποία είναι περισσότερα από όσα μπορεί να χειριστεί, και συνεπώς το buffer του κόμβου υπερχειλίζει, στην προσπάθεια του να αποθηκεύσει κατάσταση για κάθε αίτημα[11][16].
Η επίθεση αυτή μπορεί να γίνει με μόνο ένα απλό κόμβο ή περισσότερους, τους οποίους προσβάλλει, ή με ένα laptop με το οποίο να μπορεί να δημιουργήσει ένα μεγάλο αριθμό πακέτων προκειμένου να καταφέρει να εξαντλήσει τους πόρους του θύματος [11][16].
Και αφού ο κύριος στόχος της επίθεσης είναι όπως είπαμε η εξάντληση πόρων, δεν χρειάζεται κάτι ιδιαίτερο από τον επιτιθέμενο αλλά μια καλή μπαταρία προκειμένου να μπορέσει να στείλει όλα αυτά τα συνεχόμενα αιτήματα [16].

- Desynchronisation

Στόχος αυτής της επίθεσης όπως αναφέρεται στο [16], είναι η διαταραχή της υπάρχουσας επικοινωνίας μεταξύ δύο κόμβων, ακόμα και η διακοπή της. Για αυτό τον σκοπό δεν απαιτείται καμιά ειδική τεχνική δυνατότητα από τον επιτιθέμενο [16].
Ο τρόπος με τον οποίο γίνεται εφικτό αυτό, είναι να αποστέλλονται συνέχεια πλαστά μηνύματα στους κόμβους, μηνύματα τα οποία θα έχουν δηλαδή ψεύτικο sequence number ή control flag. Με αυτό τον τρόπο παρεμποδίζεται η σωστή ανταλλαγή δεδομένων ή υποβαθμίζεται η επικοινωνία μεταξύ των δύο κόμβων, αφού λαμβάνοντας ο παραλήπτης ένα πακέτο με διαφορετικό sequence number από αυτό που αναμενόταν, ζητά ξανά και ξανά να γίνει επαναμετάδοση του πακέτου, μέχρι να

λάβει αυτό με το σωστό sequence number [1][16][38].
Μια απλή αντιμετώπιση της επίθεσης αυτής, είναι να γίνεται έλεγχος της ταυτότητας και της ακεραιότητας των πακέτων [16][38].

3.4 Περιορισμοί στα δίκτυα αισθητήρων

Για τον σχεδιασμό ασφαλισμένων διεργασιών στα δίκτυα αισθητήρων υπάρχουν κάποιοι περιορισμοί σε σχέση με τον σχεδιασμό αυτών των διεργασιών στα παραδοσιακά δίκτυα.
Οι περιορισμοί αυτοί αναφέρονται παρακάτω.

- Περιορισμοί κόμβου: Ένας κανονικός κόμβος αποτελείται από ένα επεξεργαστή με συχνότητα 4-8 Mhz, έχει μέγεθος μνήμης RAM 4 KB, μια flash μνήμη 128 KB και radio frequency 916 Mhz. Λόγω της ετερογενούς φύσης που παρουσιάζουν, περιορίζουν ακόμα περισσότερο στο να βρεθεί μια λύση για την ασφάλεια των κόμβων.

- Περιορισμοί δικτύου: Τα ασύρματα δίκτυα αισθητήρων παρουσιάζουν μια έλλειψη φυσικής υποδομής και στηρίζονται σε ένα μη ασφαλισμένο μέσο, το οποίο είναι “ανοικτό”, για να μεταφέρουν τα δεδομένα τους.

- Φυσικοί περιορισμοί: Το γεγονός ότι οι κόμβοι αυτοί πολλές φορές μπορεί να εγκαθίστανται σε περιβάλλοντα τα οποία δεν είναι φιλικά, με αυτό τον τρόπο είναι ευαίσθητοι σε επιθέσεις από εξωτερικούς παράγοντες.
  Ένας τρόπος για την προστασία των κόμβων από τέτοιες επιθέσεις είναι η χρήση υλικού που να μπορεί να παρέχει προστασία στον κόμβο, κάτι το οποίο όμως αυξάνει το κόστος δημιουργίας των κόμβων [15].

3.5 Λύσεις για την ασφάλεια στα ασύρματα δίκτυα αισθητήρων

Τα συστήματα ασφάλειας εφαρμόζονται έτσι ώστε να μπορούν να προστατεύσουν το δίκτυο από τις επιθέσεις που πιθανώς να δεχτούν. Λόγω όμως της φύσης τους, παρουσιάζονται πολλές δυσκολίες όσο αφορά την υλοποίηση και εφαρμογή ενός ικανοποιητικού συστήματος ασφάλειας.
Μερικές λύσεις για ασφάλεια στα δίκτυα αισθητήρων, είναι είτε η αλλαγή του τρόπου με τον οποίο οι κόμβοι είναι σχεδιασμένοι, είτε η δημιουργία κάποιων βελτιωμένων πρωτοκόλλων για τα ασύρματα δίκτυα αισθητήρων.
Η πλέον κατάλληλη και διαδεδομένη λύση, για την εξυπηρέτηση της ασφάλειας σε αυτού του είδους τα δίκτυα, θεωρείται η εφαρμογή των πρωτοκόλλων [46].

Παρακάτω, αναλύονται τα σημαντικότερα πρωτόκολλα δρομολόγησης τα οποία χρησιμοποιούνται για τα ασύρματα δίκτυα αισθητήρων.

Flooding Protocol

Το Flooding, αποτελεί ένα παλιό μηχανισμό δρομολόγησης , όπου ουσιαστικά ένας κόμβος στέλνει τα δεδομένα που λαμβάνει, σε όλους του τους γείτονες μέσω broadcasting, μέχρι να φτάσουν στον τελικό τους προορισμό ή μέχρι το "time to live" του πακέτου να γίνει 0, όπου ουσιαστικά εδώ το πακέτο θα έχει φτάσει στον μέγιστο του αριθμό από hops [2][27].

Αυτή η τεχνική όμως δρομολόγησης των πακέτων παρουσιάζει κάποια ελαττώματα, όπως είναι για παράδειγμα η κατάρρευση του δικτύου. Αυτό οφείλεται στο ότι το Flooding αποτελεί μια τυφλή μέθοδο αποστολής των μηνυμάτων, οπότε μπορεί πολύ εύκολα ένας κόμβος να λάβει πολλές φορές το ίδιο πακέτο από πολλούς κόμβους. Συγκεκριμένα, υπάρχει η πιθανότητα να γίνεται μια κυκλική μετάδοση των πακέτων μέσα στο δίκτυο, τα οποία πολύ πιθανόν να φτάνουν ξανά και ξανά στο ίδιο σημείο. Αυτό το πρόβλημα ονομάζεται κατάρρευση του δικτύου (Implosion).

Ένα ακόμα πρόβλημα, είναι αυτό της επικάλυψης (Overlapping) όπου κάποιοι κόμβοι καλύπτουν την ίδια περιοχή για ανίχνευση γεγονότων. Όταν λοιπόν κάποιοι κόμβοι ανιχνεύσουν ένα γεγονός σε ένα κοινό τους σημείο, τότε θα γίνει μετάδοση των δεδομένων που συνέλεξαν, σε όλους τους γείτονες, την ίδια ώρα. Οπότε με αυτό τον τρόπο κάποιοι κόμβοι θα λάβουν και πάλι διπλότυπα πακέτα.

Το τρίτο πρόβλημα που δημιουργεί αυτό το πρωτόκολλο, είναι το ότι σπαταλά τους ενεργειακούς πόρους του συστήματος (Resource blindness) χωρίς να υπολογίζει τους περιορισμούς στην ενέργεια του συστήματος. Ο λόγος που το πρωτόκολλο αυτό προκαλεί μεγάλη σπατάλη ενέργειας είναι επειδή δημιουργεί αχρείαστες αναμεταδόσεις [2][27][25].

Gossip Protocol

Για την αντιμετώπιση των προβλημάτων που παρουσιάζονταν στο πρωτόκολλο Flooding, σχεδιάστηκε το πρωτόκολλο Gossip. Ο τρόπος με τον οποίο λειτουργεί αυτό το πρωτόκολλο, είναι ένας κόμβος να στέλνει ένα πακέτο σε ένα γείτονα του τον οποίο επιλέγει τυχαία και αυτός σε κάποιον άλλο κτλ [25].
Η διαδικασία αυτή επαναλαμβάνεται μέχρι όλοι οι γείτονες λάβουν το πακέτο, όπου ένας κόμβος θα λάβει μόνο ένα αντίγραφο του πακέτου που στέλνεται.

Σκοπός του πρωτοκόλλου είναι να μειώσει τον αριθμό των αναμεταδόσεων,

αναγκάζοντας κάποιους κόμβους να καταστρέψουν κάποιο πακέτο, παρά να το προωθήσουν παρακάτω. Σύμφωνα με κάποια πιθανότητα, μιας και η φύση του πρωτοκόλλου αυτού είναι τέτοια, αποφασίζεται εάν ο κόμβος θα προωθήσει το πακέτο αυτό ή όχι.
Οπότε ουσιαστικά μπορεί να εμποδίσει την κατάρρευση του δικτύου αποφεύγοντας την μετάδοση ενός μεγάλου αριθμού πακέτων, δεν μπορεί όμως να αντιμετωπίσει και την επικάλυψη.

Το πρόβλημα αυτού του πρωτοκόλλου είναι η καθυστέρηση στην μετάδοση της πληροφορίας, όπως επίσης και το γεγονός ότι και αυτό καταναλώνει ενέργεια, με πιο αργό όμως ρυθμό [2][27][25].

Προκειμένου να βελτιωθούν τα προβλήματα που παρουσιάζει το Flooding πρωτόκολλο και για την ικανοποίηση των απαιτήσεων που αφορούν την ασφάλεια των δικτύων αισθητήρων, ήταν απαραίτητη η δημιουργία του SPIN.
Το SPIN είναι σχεδιασμένο βασισμένο σε 2 βασικές ιδέες οι οποίες είναι:
Να λειτουργεί σωστά και να διατηρεί την ενέργεια των κόμβων, στέλνοντας μονάχα μεταδεδομένα, τα οποία χρειάζεται ο κόμβος, και όχι ολόκληρα τα δεδομένα τα οποία ήδη έχουν οι κόμβοι.
Η δεύτερη ιδέα είναι ότι οι κόμβοι πρέπει να γνωρίζουν για την κατάσταση της ενέργειας τους ανά πάσα στιγμή, έτσι ώστε να μπορούν να προσαρμοστούν με σκοπό να παρατείνουν όσο περισσότερο την λειτουργία τους.
Έτσι, οι κόμβοι είναι ικανοί να υπολογίζουν την ενέργεια που χρειάζεται να καταναλωθεί για την λήψη των δεδομένων, την επεξεργασία και την αποστολή τους [2][25].

Ο μηχανισμός αυτός, ο οποίος ουσιαστικά βασίζεται στην διαφήμιση των υπαρχόντων δεδομένων αλλά και των αναγκών σε δεδομένα, δεν μπορεί να εγγυηθεί την παράδοση των δεδομένων, αφού μεταξύ των κόμβων οι οποίοι ζητούν κάποια πληροφορία και των κόμβων που την διαθέτουν, είναι δυνατόν να παρεμβάλλονται κόμβοι οι οποίοι δεν ενδιαφέρονται στην ουσία για τα συγκεκριμένα δεδομένα.

Το SPIN αποτελείται από 2 βασικά δομικά στοιχεία τα οποία είναι το SNEP και το μTESLA, και τα οποία τρέχουν πάνω από το TinyOS λειτουργικό σύστημα.

SNEP

Το SNEP έχει την δυνατότητα να παρέχει εμπιστευτικότητα , αυθεντικοποίηση και ακεραιότητα των δεδομένων. Με την κρυπτογράφηση μπορεί να πετύχει την εμπιστευτικότητα, ενώ με τον Κώδικα Αυθεντικοποίησης Μηνύματος (Message

Authentication Code -MAC), μπορεί να πετύχει αυθεντικοποίηση και ακεραιότητα, για τους δύο τελικούς κόμβους που επικοινωνούν [43][6][35][22].

Το SNEP παρουσιάζει και κάποια άλλα πλεονεκτήματα, όπως είναι για παράδειγμα το χαμηλό κόστος επικοινωνίας μεταξύ των κόμβων που επικοινωνούν, και η κρυπτογράφηση των μηνυμάτων με τέτοιο τρόπο ώστε να μην μπορεί κάποιος εισβολέας να αντιληφθεί το περιεχόμενο. Επίσης χρησιμοποιείται κάποιος μετρητής, όπως σε κάθε πρωτόκολλο, του οποίου η τιμή δεν μεταφέρεται από τον ένα κόμβο στον άλλο, αλλά κρατείται κατάσταση για αυτόν σε κάθε κόμβο, προκειμένου να αποφεύγεται η αύξηση του κόστους επικοινωνίας.

Εκτός από τις πιο πάνω τρεις βασικές υπηρεσίες που προσφέρει το συγκεκριμένο πρωτόκολλο, παρέχει και σημασιολογική ασφάλεια, κατά την οποία γίνεται μια τέτοια κρυπτογράφηση των δεδομένων, έτσι ώστε ένας εισβολέας να μην μπορεί να έχει καμία πληροφορία για τα δεδομένα αυτά, ακόμα και αν παρουσιάζεται κρυπτογράφηση του ίδιου κομματιού. Ο τρόπος με τον οποίο αυτό επιτυγχάνεται, είναι η τυχαία κρυπτογράφηση, κατά την οποία προκύπτουν διαφορετικές κωδικοποιήσεις του ίδιου κομματιού [6][35][22].

Το SNEP λοιπόν μπορεί να παρέχει τις ακόλουθες ιδιότητες οι οποίες περιγράφονται αναλυτικότερα, και μερικές από τις οποίες έχουν ήδη προαναφερθεί:

- Σημασιολογική ασφάλεια (Semantic security)

Όπως προαναφέρθηκε, το συγκεκριμένο πρωτόκολλο παρέχει εμπιστευτικότητα των δεδομένων, κάτι το οποίο θεωρείται ως μια από τις βασικότερες αρχές και χρησιμοποιείται σχεδόν σε κάθε πρωτόκολλο ασφαλείας. Μια απλή μορφή εμπιστευτικότητας, μπορεί να επιτευχθεί από την κρυπτογράφηση των δεδομένων, όμως μια απλή κρυπτογράφηση, δεν θα ήταν τόσο αποτελεσματική.
Για αυτό τον σκοπό, εφαρμόζεται μια άλλη τεχνική κρυπτογράφησης, η σημασιολογική κρυπτογράφηση, η οποία επιβεβαιώνει ότι ένας υποκλοπέας, ακόμα και αν μπορεί να δει πολλαπλές κωδικοποιήσεις του ίδιου καθαρού κομματιού δεδομένων, εντούτοις δεν μπορεί να έχει καμία πληροφορία για αυτό [35].

Για παράδειγμα αν ένας εισβολέας γνωρίζει τον τρόπο κωδικοποίησης 1 bit και 0 bit, αυτό δεν θα τον βοηθήσει να αναγνωρίσει στην συνέχεια αν μια καινούργια κρυπτογραφημένη μορφή ενός κειμένου είναι κρυπτογράφηση 0 ή 1 [35].

Αυτό επιτυγχάνεται με την χρήση του μετρητή που κρατείται στους κόμβους, και η τιμή του οποίου αυξάνεται μετά από κάθε μήνυμα. Χρησιμοποιώντας λοιπόν την τιμή αυτού του μετρητή για την κωδικοποίηση του μηνύματος, αυτό σημαίνει πως για μια σειρά ανταλλαγής μηνυμάτων, δεν θα υπάρχουν κοινά μηνύματα, αν και το περιεχόμενο τους είναι ίδιο [35].

- Προστασία αναπαραγωγής (Replay protection)

Προκειμένου να αποφευχθεί η αναπαραγωγή παλιών μηνυμάτων, χρησιμοποιείται ένας μετρητής στο MAC, η τιμή του οποίου εμποδίζει προηγούμενα μηνύματα τα οποία είχαν σταλεί μέσα στο δίκτυο, να ξανασταλθούν. Αν δεν υπήρχε ο μετρητής στ MAC, τότε ένας εισβολέας θα μπορούσε πολύ εύκολα να ξαναχρησιμοποιήσει παλιά μηνύματα.

- Αδυναμία φρεσκάδας μηνύματος (Weak freshness)

Ένα μήνυμα το οποίο φτάνει στον προορισμό του, περνά από ένα έλεγχο επαλήθευσης, κατά τον οποίο το μήνυμα είναι έγκυρο στην περίπτωση όπου η τιμή του μετρητή του πακέτου είναι χαμηλότερη από την τιμή που είχαν τα πακέτα τα οποία έφτασαν μέχρι στιγμής. Με αυτό τον τρόπο υποδηλώνεται ουσιαστικά ότι το πακέτο το οποίο έφτασε στον συγκεκριμένο κόμβο, την συγκεκριμένη χρονική στιγμή, είναι το πιο πρόσφατο.
Η ύπαρξη ενός μετρητή και του ελέγχου της τιμής του μετρητή, βοηθά στο να διατηρείται η σωστή σειρά των πακέτων.

- Χαμηλό κόστος επικοινωνίας (Low communication overhead)

Το κόστος της επικοινωνίας μεταξύ των κόμβων, όπως προαναφέρθηκε, διατηρείται χαμηλό λόγω του ότι η τιμή του μετρητή δεν χρειάζεται να αποστέλλεται από τον ένα κόμβο στον άλλο για κάθε μήνυμα που ανταλλάσσουν, αφού κρατείται κατάσταση του σε κάθε τελικό κόμβο του δικτύου [46][35].

μTESLA

Το μTESLA αποτελεί μια βελτιστοποιημένη μορφή του πρωτοκόλλου TESLA, η οποία λύνει κάποια προβλήματα που παρουσιάζει το δεύτερο, προκειμένου να μπορεί να εφαρμοστεί σε ασύρματα δίκτυα. Ο λόγος για τον οποίο το αρχικό πρωτόκολλο δεν εφαρμόζεται σε δίκτυα αισθητήρων, οφείλεται στις απαιτήσεις του για μεγάλη υπολογιστική δυνατότητα και την ύπαρξη ικανοποιητικών πόρων προς εκμετάλλευση [46][6].
Για παράδειγμα, ενώ στο TESLA χρησιμοποιείται μια ψηφιακή υπογραφή για την αυθεντικοποίηση του πακέτου, στο μTESLA χρησιμοποιούνται μόνο κάποιοι συμμετρικοί μηχανισμοί. Η αλλαγή αυτή οφείλεται στο ότι οι ψηφιακές υπογραφές είναι πολύ πιο ακριβές για να χρησιμοποιηθούν στα δίκτυα αισθητήρων.
Στο TESLA, χρειάζεται να γίνεται γνωστοποίηση του κλειδιού, για κάθε πακέτο, οπότε αυτό σημαίνει ότι θα χρειαζόταν πολλή περισσότερη ενέργεια για την αποστολή και λήψη των πακέτων. Αντιθέτως, στο μTESLA, γνωστοποιείται μόνο ένα κλειδί σε κάποιο χρονικό διάστημα [26][46][35].

Η ύπαρξη κάποιων μηχανισμών κωδικοποίησης μηνυμάτων μπορεί να αποτρέψει την δημιουργία πολλών προβλημάτων μέσα σε ένα δίκτυο, εμποδίζοντας κάποιον εισβολέα να δει τα μηνύματα που ανταλλάσσονται μεταξύ των κόμβων.
Τέτοιοι μηχανισμοί όμως έχουν υψηλό κόστος υπολογισμού, επικοινωνίας και αποθήκευσης δεδομένων κάτι που μπορεί να δημιουργήσει κάποιο άλλο πρόβλημα μέσα στο δίκτυο και συγκεκριμένα αυτή την φορά στους κόμβους, λόγω των περιορισμένων πόρων που διαθέτουν [35].

TinySec

Το πρωτόκολλο αυτό, αποτελεί μια αρχιτεκτονική για ασφάλεια στο επίπεδο σύνδεσης για ασύρματα δίκτυα. Είναι ένα γενικό πακέτο για ασφάλεια το οποίο μπορεί να ενσωματωθεί σε εφαρμογές δικτύων αισθητήρων.

Μοιάζει με το SNEP και κάπου το συμπληρώνει. Συγκεκριμένα, παρέχει εμπιστευτικότητα, αυθεντικοποίηση και ακεραιότητα των δεδομένων, όπως επίσης και εγγύηση όταν δεν θα υπάρχει αναμετάδοση παλαιότερων πακέτων.
Η βασική διαφορά του με το SNEP, είναι ότι σε αυτή την περίπτωση δεν παρουσιάζονται καθόλου μετρητές [26].

Η επεξεργασία των δεδομένων στα ασύρματα δίκτυα αισθητήρων, όπως είναι για παράδειγμα οι εξάλειψη αντιγράφων, γίνεται εντός του δικτύου, έτσι ώστε να γίνεται εξοικονόμηση ενέργειας, προτού τα πακέτα αυτά να μεταδοθούν προς τον τελικό προορισμό που βρίσκεται εκτός του δικτύου [43].

Όσο αφορά όμως τους μηχανισμούς για ασφάλεια στα άκρα του δικτύου, μεταξύ των εσωτερικών κόμβων και του τελικού προορισμού, δεν μπορούν να εγγυηθούν αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα των μηνυμάτων, εφόσον οι μηχανισμοί αυτοί είναι εκτεθειμένοι σε άλλες εξωτερικές επιθέσεις.
Στην περίπτωση λοιπόν όπου ο έλεγχος της ακεραιότητας των μηνυμάτων γίνεται μόνο όταν φτάσουν στον τελικό τους προορισμό, τότε είναι πολύ πιθανόν τα πακέτα που λαμβάνονται από αυτόν, να είναι “μολυσμένα” από κάποιον εισβολέα. Στην περίπτωση αυτή, θα μπορούσε ο οποιοσδήποτε να αλλοιώσει τα πακέτα, μερικά hops προηγουμένως, χωρίς αυτό να γίνει αντιληπτό. Οι συνέπειες αυτής της ενέργειας θα ήταν η σπατάλη ακόμα περισσότερης ενέργειας και bandwidth [43].

Οπότε μια αρχιτεκτονική για ασφάλεια στο επίπεδο της σύνδεσης, θα πρέπει να μπορέσει να ανιχνεύσει πακέτα τα οποία έχει παρεμβάλει ή αλλοιώσει κάποιος άλλος.
Το TinySec, παρέχει τις βασικές αρχές ασφάλειας για την αυθεντικοποίηση και ακεραιότητα των μηνυμάτων, όπως επίσης και εμπιστευτικότητα, σημασιολογική ασφάλεια και προστασία από την αναμετάδοση πακέτων [43][26].

LEAP

Το πρωτόκολλο αυτό, είναι ένα βασικό πρωτόκολλο διαχείρισης στα δίκτυα αισθητήρων, το οποίο είναι σχεδιασμένο για την υποστήριξη της ενδοδίκτυας επεξεργασίας και παρέχει ασφαλισμένη επικοινωνία στα δίκτυα αισθητήρων. Παρέχει τις βασικές υπηρεσίες για ασφάλεια όπως η αυθεντικοποίηση και η εμπιστευτικότητα [26].
Τα μηνύματα που ανταλλάσσονται μεταξύ διαφορετικών κόμβων, έχουν και διαφορετικές απαιτήσεις σε θέμα ασφάλειας, γιαυτό και ο σχεδιασμός του πρωτοκόλλου αυτού, επηρεάζεται από το γεγονός αυτό [43][26].

Σύμφωνα με το πιο πάνω λοιπόν, ότι δηλαδή δεν μπορεί να υπάρξει ένας μόνο μηχανισμός ενιαίου κλειδιού ο οποίος να μπορέσει να προστατεύσει όλες τις επικοινωνίες μέσα στο δίκτυο, το πρωτόκολλο LEAP υποστηρίζει την εγκαθίδρυση τεσσάρων τύπων κλειδιών, για κάθε κόμβο αισθητήρα.
Υπάρχει λοιπόν ένα κλειδί το οποίο είναι κοινό με τον τελικό παραλήπτη (base station), ένα ζεύγος κλειδιών όπου παίρνει ο ένας κόμβος το ένα και δίνει το άλλο σε κάποιον άλλο αισθητήρα, ένα κλειδί που είναι κοινό για μια ολόκληρη ομάδα από πολλαπλούς κόμβους γείτονες και τέλος ένα κλειδί επίσης για μια ομάδα, το οποίο είναι κοινό για όλους τους κόμβους μέσα σε ολόκληρο το δίκτυο [26][46].

3.6 Μέτρα αντιμετώπισης

Όπως όλα τα δίκτυα, το ίδιο και τα ασύρματα δίκτυα αισθητήρων, έχουν κάποιες απαιτήσεις όσο αφορά την εφαρμογή της ασφάλειας σε αυτά. Με την ικανοποίηση αυτών των απαιτήσεων προστατεύονται τα δίκτυα αυτά.

- Εγκαθίδρυση κλειδιού (Key Establishment)

Μια πτυχή της ασφάλειας η οποία έχει μεγάλη σημασία, είναι και η διαχείριση του κλειδιού.
Τα ασύρματα δίκτυα αισθητήρων είναι μοναδικά σε σχέση με άλλα ενσωματωμένα ασύρματα δίκτυα, όσο αφορά το μέγεθος τους, την κινητικότητα τους και τους περιορισμούς στην υπολογιστική τους ισχύ.
Το ότι γίνεται μια προσπάθεια τα ασύρματα δίκτυα αισθητήρων, να γίνουν τάξεις μεγαλύτερα από άλλα παραδοσιακά ενσωματωμένα δίκτυα, σε συνδυασμό με τους λειτουργικούς περιορισμούς που παρουσιάζουν, αυτό καθιστά την διαχείριση του κλειδιού πολύ σημαντική, όσο αφορά των σχεδιασμό των περισσότερων ασύρματων δικτύων αισθητήρων.
Τα θέματα που αφορούν την διαχείριση κλειδιού στα δίκτυα δεν περιορίζονται μόνο στα ασύρματα δίκτυα αισθητήρων. Συγκεκριμένα, η εγκαθίδρυση κλειδιού και το

θέμα της διαχείρισης του, έχει μελετηθεί σε βάθος και εκτός της περιοχής των ασυρμάτων δικτύων.

- Άμυνα εναντίον των DoS επιθέσεων (Defending Against DoS Attacks)

Οι επιθέσεις DoS είναι πολύ κοινές, γιαυτό και πρέπει να υπάρχουν αποτελεσματικοί τρόποι αντιμετώπισης τους.
Μια στρατηγική για την αντιμετώπιση αυτού του τύπου επιθέσεων, είναι να βρεθεί το μέρος του δικτύου το οποίο μπλοκάρεται, επηρεάζεται δηλαδή από τον εισβολέα. Αφού ταυτοποιηθεί το κομμάτι αυτό του δικτύου, τότε ο τρόπος με τον οποίο δρομολογούνται τα πακέτα πλέον στο δίκτυο, θα αποκλείει αυτό το μονοπάτι. Ουσιαστικά τα πακέτα θα ακολουθούν μια διαδρομή γύρω από την προσβαλλόμενη περιοχή.

Ένας άλλος τρόπος άμυνας, είναι να γίνεται μια ανάλυση του αριθμού των πακέτων που φτάνουν σε ένα κόμβο, όπου στην συνέχεια το δίκτυο θα μπορεί να αγνοήσει κάποια αιτήματα τα οποία στέλνονται με σκοπό να προκαλέσουν πρόβλημα στο δίκτυο, εξαντλώντας τους πόρους του κόμβου. Αυτό όμως δεν αποδεικνύει ότι όντως υπάρχει κάποιο πρόβλημα μέσα στο δίκτυο, αφού υπάρχει και το ενδεχόμενο να κινούνται μεγάλες ποσότητες νόμιμων πακέτων ούτως η άλλως και τα οποία είναι υπεύθυνο το δίκτυο να επεξεργάζεται.

Στην περίπτωση όπου μπορεί να υπάρξει κάποιος "μολυσμένος" κόμβος μέσα στο δίκτυο, τότε αυτός μπορεί να καταστρέφει τα πακέτα που φτάνουν σε αυτόν με σκοπό να φτάσουν στον τελικό τους προορισμό. Ο τρόπος με τον οποίο μπορεί να αντιμετωπιστεί αυτό το πρόβλημα, είναι ένας κόμβος να επιλέγει πολλά μονοπάτια για να στείλει το πακέτο του στον τελικό προορισμό. Οπότε προωθώντας ένα πακέτο σε πολλαπλά μονοπάτια, μειώνει τις πιθανότητες αυτό να χαθεί. Βέβαια ακόμα υπάρχει το ενδεχόμενο αυτό να μην πετύχει για κάποια τοπολογία δικτύου, αφού συνήθως το μονοπάτι που ακολουθεί ένα πακέτο για να φτάσει στον τελικό του προορισμό, δεν βασίζεται μόνο σε ένα κόμβο και συνεπώς αυξάνονται οι πιθανότητες ένας από αυτούς να είναι κακόβουλος.

- Secure Broadcasting and Multicasting

Έχει αποδειχθεί ότι το σημαντικότερο πρότυπο επικοινωνίας στα ασύρματα δίκτυα αισθητήρων είναι το broadcasting και multicasting, αντί η παραδοσιακή σημείο-προς-σημείο (point-to-point) επικοινωνία που παρουσιάζεται στο Διαδίκτυο.
Στα ασύρματα δίκτυα αισθητήρων, ένα μεγάλο μέρος της ασφάλειας προέρχεται από την εξασφάλιση ότι μόνο τα μέλη τα οποία συμμετέχουν σε μια broadcast ή multicast επικοινωνία, κατέχουν τα κλειδιά τα οποία χρησιμοποιούνται για αποκρυπτογράφηση των μηνυμάτων[34][24].

- Defending Against Attacks on Routing Protocols

Η δρομολόγηση των πακέτων μέσα σε ένα ασύρματο δίκτυο αισθητήρων, έχει μελετηθεί αρκετά καλά, όμως το περισσότερο μέρος των ερευνών επικεντρώνονται στην παροχή μιας δρομολόγησης όπου θα παρέχει την ελάχιστη κατανάλωση σε ενέργεια.
Υπάρχουν βέβαια αρκετοί τύποι επιθέσεων όπως είναι το sinkhole, workmhole και sybil attack, οι οποίοι αποδεικνύουν πως τα πρωτόκολλα δρομολόγησης πρέπει να είναι ικανά να παρέχουν τόσο ασφαλισμένα όσο και αποδοτικά από θέμα ενέργειας δρομολόγια για την μετάδοση των πακέτων.
Με την αύξηση του μεγέθους και της χρησιμότητας των ασύρματων δικτύων αισθητήρων, η ασφάλεια στην δρομολόγηση των πακέτων πρέπει να παίζει σημαντικό ρόλο στον σχεδιασμό ενός δικτύου αισθητήρων [34].

3.7 Εφαρμογές στα ασύρματα δίκτυα αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων, μπορούν να καλύψουν ένα ευρύ φάσμα εφαρμογών, σε πολλά διαφορετικά πεδία. Μπορούν να βρουν εφαρμογή για παρακολούθηση του περιβάλλοντος, σε πόλεμο, για εκπαίδευση παιδιών και για μικρο-χειρουργικές επεμβάσεις.
Επιπλέον, προβλέπεται ότι τα δίκτυα αισθητήρων, αναμένεται να βρουν εφαρμογή και στην εξερεύνηση του διαστήματος στο μέλλον.
Αυτά είναι μόνο μερικά από τα πεδία στα οποία βρίσκουν εφαρμογή τα WSNs.

Γενικότερα, τα ασύρματα δίκτυα αισθητήρων, θα βρίσκονται παντού, στο κοντινό μέλλον, αφού υποστηρίζουν νέες ευκαιρίες για την αλληλεπίδραση μεταξύ των ανθρώπων και του φυσικού τους κόσμου.

Η πρόσφατη ανάπτυξη των ασύρματων επικοινωνιών, συνέτεινε στην ανάπτυξη ενός ασύρματου δικτύου αισθητήρων υψηλής κλίμακας, χαμηλής ισχύος και χαμηλού κόστους. Μια τέτοια προσέγγιση, υπόσχεται πλεονέκτημα απέναντι στις παραδοσιακές αισθητήριες μεθόδους σε πολλά σημεία, όπως είναι για παράδειγμα η μεγάλη κλίμακα, η πυκνή ανάπτυξη η οποία παρέχει καλύτερη κάλυψη του χώρου αλλά και πολύ καλύτερη ανάλυση, επίσης αυξάνεται η αξιοπιστία και η ανθεκτικότητα του συστήματος.
Μερικές από τις εφαρμογές των ασύρματων δικτύων αισθητήρων παρουσιάζονται αναλυτικότερα πιο κάτω [3].

- Military applications

Σε στρατιωτικές εφαρμογές, ο σκοπός των κόμβων είναι κυρίως η παρακολούθηση ενός περιβάλλοντος, το οποίο είναι συχνά το περιβάλλον του εχθρού, παρακολουθούνται οι κινήσεις των μονάδων του στρατού σε ξηρά και θάλασσα, μπορούν να εντοπίζονται πιθανές επιθέσεις από χημικά, να έχουν πρόσβαση σε συνομιλίες των αντιπάλων και πολλά άλλα.
Οι κόμβοι μπορεί απλώς να ρίχνονται μέσα στο πεδίο το οποίο πρόκειται να εξερευνηθεί, και ελέγχονται από ένα απομακρυσμένο χρήστη, ο οποίος συλλέγει όλες τις πληροφορίες που μαζεύουν οι κόμβοι.
Μια πολύ σημαντική εφαρμογή των αισθητήριων αυτών κόμβων, είναι η περίπτωση όπου με κάποιους αλγορίθμους γίνεται κατηγοριοποίηση των δεδομένων που οι αισθητήρες μπορούν να συλλέξουν και τα οποία προέρχονται από σεισμικά και ακουστικά σήματα.
Αυτή η μέθοδος μπορεί να χρησιμοποιηθεί για την αντικατάσταση των ναρκών, οι οποίες στο κοντινό μέλλον θα θεωρούνται απαρχαιωμένες. Αφού λοιπόν οι αισθητήρες αυτοί εντοπίσουν κάποια εισβολή από τον εχθρό τότε θα ενεργοποιείται ένα σύστημα άμυνας για την αντιμετώπιση του εχθρού [56] [3].

- Smart Energy

Το θέμα του ηλεκτρισμού είναι ίσως η σημαντικότερη υποδομή σήμερα αφού τα πάντα κινούνται και λειτουργούν με την παροχή ηλεκτρικού ρεύματος.
Αυτό που επιδιώκεται να γίνει, είναι να εφαρμοστεί ένα αυτοματοποιημένο σύστημα για την δημιουργία και παροχή ηλεκτρισμού. Σήμερα, ο άνθρωπος είναι αυτός που πρέπει να υπολογίσει την ποσότητα ενέργειας που θα καταναλωθεί, και να παράξει επαρκή ποσότητα έτσι ώστε να καλύψει τις ανάγκες του πληθυσμού, χωρίς όμως να υπάρχουν μεγάλες απώλειες ενέργειας. Όπως είναι αναμενόμενο, οι απώλειες είναι αναπόφευκτες, οπότε η δημιουργία ενός συστήματος το οποίο θα μπορούσε να καλύψει ακριβώς τις ανάγκες σε ενέργεια, θα μπορούσε να βοηθήσει στην εξοικονόμηση ενός σημαντικού ποσοστού χρημάτων.
Ένα τέτοιο σύστημα λοιπόν, είναι το Smart Grid, το οποίο είναι ουσιαστικά μια εφαρμογή των ασύρματων δικτύων αισθητήρων. Είναι ένα μεγάλο δίκτυο το οποίο μπορεί να χωριστεί σε 3 κύρια εννοιολογικά κομμάτια, όπως είναι η δημιουργία ενέργειας, το δεύτερο η μετάδοση ενέργειας και η κατανομή ηλεκτρισμού, και το τρίτο είναι η υποδομή της κατανάλωσης της ενέργειας.
Τα ασύρματα δίκτυα, έχουν ένα ευρύ φάσμα εφαρμογών σε κάθε ένα από τα τρία πιο πάνω κομμάτια [56][59].

- Environmental monitoring

Η παρακολούθηση του περιβάλλοντος όπως είναι η παρακολούθηση ζώων, ανίχνευση

πλημμύρας, πρόβλεψη του καιρού και παρακολούθηση και ανίχνευση σεισμικής δραστηριότητας είναι μερικές ακόμα εφαρμογές των δικτύων αισθητήρων.
Η ικανότητα των κόμβων να "αισθάνονται" και να ανιχνεύουν την θερμοκρασία που επικρατεί μέσα σε ένα περιβάλλον, τον φωτισμό, τα ρεύματα αέρος όπως και την εσωτερική μόλυνση του αέρα που μέσα σε ένα εσωτερικό χώρο, μπορεί να χρησιμοποιηθεί για ένα βέλτιστο έλεγχο του εσωτερικού αυτού περιβάλλοντος. Οπότε με την αχρείαστη χρήση της θέρμανσης, υπάρχει μεγάλη σπατάλη ενέργειας, κάτι το οποίο μπορεί να αντιμετωπιστεί με την χρήση αυτών των αισθητήριων κόμβων, βοηθώντας στην δημιουργία ενός πιο υγιούς και άνετου περιβάλλοντος.
Μια ακόμα σημαντική εφαρμογή για τα ασύρματα δίκτυα αισθητήρων, είναι και η περίπτωση όπου μπορεί να προκληθεί πυρκαγιά. Με την εγκατάσταση ενός τέτοιου δικτύου, θα μπορούσαν να συνδυαστούν τα φωτεινά σήματα που δείχνουν τις εξόδους διαφυγής μέσα σε ένα δίκτυο, μαζί με τους αισθητήρες καπνού, οπότε μόλις ανιχνευθεί πυρκαγιά το δίκτυο θα είναι ικανό να σχεδιάσει το ασφαλέστερο μονοπάτι προς την έξοδο.
Κάποιες ακόμα εφαρμογές, οι οποίες αφορούν εξωτερικά περιβάλλοντα, είναι η παρακολούθηση κάποιων ειδών ζώων τα οποία είναι προς εξαφάνιση. Μελετώντας με αισθητήρες ή ακόμα και με την χρήση ψηφιακής κάμερας στον κάθε κόμβο, το περιβάλλον στο οποίο ζουν διάφορα είδη μπορεί να επιφέρει πολλά θετικά αποτελέσματα [3].

- Health applications

Εφαρμογές οι οποίες έχουν να κάνουν με την υγεία, όπως είναι η παρακολούθηση τόσο των ασθενών όσο και των γιατρών, εντός και εκτός νοσοκομείου, μπορούν να παρέχονται από τα δίκτυα αισθητήρων.
Ασθένειες όπως είναι το Alzheimer μπορούν να παρακολουθούνται και να ελέγχονται σε πρώιμο στάδιο με την χρήση ασύρματων αισθητήρων. Οι κόμβοι μπορούν να καταγράφουν και να αποθηκεύουν συμπεριφορές ατόμων τα οποία αντιμετωπίζουν τέτοιες ασθένειες, και στην συνέχεια να μελετούνται από ειδικούς.
Μια ακόμη εφαρμογή που μπορούν να βρουν τα ασύρματα δίκτυα αισθητήρων στα θέματα υγείας, σχετίζεται με την όραση των ατόμων, όπου μπορεί με την πρόσθεση ενός τεχνητού αμφιβληστροειδούς χιτώνα, ο οποίος αποτελείται από πολλούς μικρο-αισθητήρες, να υπάρξει επαναφορά της όρασης κάποιου ατόμου. Οι αισθητήρες εμφυτεύονται στο ανθρώπινο μάτι και για την υποστήριξη κάποιας λειτουργίας, επικοινωνούν ασύρματα με ένα εξωτερικό σύστημα υπολογιστή. Η δουλειά αυτού του συστήματος είναι να προχωρεί σε μια ειδική επεξεργασία της εικόνας για αναγνώριση και επικύρωση, δίνοντας μια ανάδραση στον ασθενή για καλύτερο έλεγχο. Αυτό βοηθά άτομα με περιορισμένη ή καθόλου όραση να βλέπουν σε ένα ικανοποιητικό επίπεδο. Λόγω όμως περιορισμών στην ενέργεια, ακόμα δεν υπάρχει δυνατότητα εφαρμογής αυτής της ιδέας [56][3].

Κεφάλαιο 4

Contiki OS

4.1 Εισαγωγή
4.2 Εργαλείο προσομοίωσης Cooja

4.1 Εισαγωγή

Για την διεκπεραίωση της διπλωματικής αυτής εργασίας, η οποία βασίζεται στην δημιουργία ασύρματων δικτύων με αισθητήρες, χρειάστηκε να δουλέψω με το λειτουργικό σύστημα Contiki το οποίο είναι ανοιχτού κώδικα, έχει την δυνατότητα να εκτελεί πολλαπλές διεργασίες παράλληλα και έχει υψηλή φορητότητα [58].

Το Contiki είναι γραμμένο σε C γλώσσα προγραμματισμού, τρέχει πάνω σε μια ποικιλία από πλατφόρμες που συμπεριλαμβάνουν μικροελεγκτές όπως είναι ο MSP430 και το AVR, μέχρι και κανονικούς προσωπικούς υπολογιστές[13].
Η τάξη του κώδικα που χρησιμοποιείται στο Contiki, είναι μερικά kilobytes, και η χρήση της μνήμης που χρησιμοποιείται μπορεί να ρυθμιστεί με τέτοιο τρόπο έτσι ώστε να είναι μερικές δεκάδες από bytes [58].
Όσο αφορά τις βιβλιοθήκες που παρέχει το Contiki, μπορούν να χρησιμοποιηθούν για την διαχείριση της μνήμης και για λειτουργίες που σχετίζονται με συνδεδεμένες λίστες.

Το Contiki μπορεί να χρησιμοποιηθεί σε ένα μεγάλο αριθμό συστημάτων όπως είναι η βιομηχανική παρακολούθηση, συστήματα συναγερμού, απομακρυσμένη παρακολούθηση ενός σπιτιού κτλ

Είναι σχεδιασμένο για μικρές συσκευές, οι οποίες λειτουργούν με χαμηλή κατανάλωση ενέργειας και έχουν μια μικρή ποσότητα μνήμης.
Οι τυπικοί αισθητήρες είναι εφοδιασμένοι με 8-bit μικροελεγκτές, με μνήμη κώδικα 100kilobytes και με μνήμη RAM, λιγότερη από 20kilobytes [13].

Στηρίζει την λειτουργία του σε ένα event-driven πυρήνα, ο οποίος παρέχει υποστήριξη τόσο για πολυνηματικές διεργασίες, όσο και για protothreads, τα οποία μοιάζουν με threads, με μια πιο "απλή" μορφή, η οποία δεν περιλαμβάνει στοίβα.

Ο λόγος που το συγκεκριμένο λειτουργικό σύστημα στηρίζει την λειτουργία του σε ένα event-driven μοντέλο, οφείλεται στο ότι αυτά τα μοντέλα δεν απαιτούν δέσμευση μνήμης, για κάθε στοίβα η οποία αντιστοιχεί σε ένα thread. Οπότε με αυτό τον τρόπο οι απαιτήσεις όσο αφορά την μνήμη είναι πολύ μικρότερες σε σχέση με άλλα μοντέλα προγραμματισμού.
Ο προγραμματισμός event-driven χρησιμοποιείται για προγραμματισμό μικρών ενσωμάτων συστημάτων, αισθητήριων κόμβων οι οποίοι λειτουργούν μέσα σε ένα δίκτυο και γενικότερα χρησιμοποιείται σε συστήματα των οποίων η μνήμη είναι πολύ περιορισμένη. Εντούτοις αν και αυτός ο τύπος προγραμματισμού, μπορεί να κρατήσει την χρήση μνήμης σε χαμηλά επίπεδα, το γράψιμο κώδικα και η αποσφαλμάτωση του καθίσταται πολύ δύσκολη [12][13].

Με την χρήστη όμως των protothreads, είναι δυνατόν να γραφούν event-driven προγράμματα των οποίων ο τρόπος γραφής είναι πολύ παρόμοιος με τον τρόπο με τον οποίο γράφονται προγράμματα που χρησιμοποιούν threads.
Αποδεικνύεται λοιπόν πως με την χρήση των protothreads, μειώνεται σημαντικά τόσο η πολυπλοκότητα ενός αριθμού προγραμμάτων τα οποία ήταν γραμμένα με event-driven state machines, όσο και το μέγεθος του κώδικα [12].

Το Contiki περιέχει 2 στοίβες επικοινωνίας οι οποίες είναι η uIP και Rime.

Η uIP TCP/IP στοίβα, παρέχει στο Contiki την δυνατότητα επικοινωνίας με το Διαδίκτυο, μέσω της TCP/IP στοίβας πρωτοκόλλων. Η uIP είναι μικρή και απλή, και της οποίας οι peers επίσης δεν έχουν πολύπλοκες στοίβες, μπορεί όμως να υπάρξει επικοινωνία με peers οι οποίοι τρέχουν μια παρόμοια "ελαφριά" στοίβα.
Όσο αφορά το μέγεθος του κώδικα, είναι μερικά kilobytes, ενώ η χρήση της RAM είναι
πολύ χαμηλή [58].
Η uIP είναι γραμμένη σε C γλώσσα προγραμματισμού, είναι υλοποιημένη για να έχει μόνο τα βασικά χαρακτηριστικά, τα οποία χρειάζονται για μια πλήρη TCP/IP στοίβα και περιέχει τα πρωτόκολλα IP, ICMP, UDP και TCP.
Μπορεί να τρέξει σαν μια διεργασία σε ένα σύστημα το οποίο μπορεί να εκτελεί πολλαπλές διεργασίες παράλληλα, ή σαν ένα βασικό πρόγραμμα σε ένα σύστημα το οποίο μπορεί να τρέξει μόνο μια διεργασία. Και στις δύο περιπτώσεις, ο βασικός σκοπός είναι να γίνεται έλεγχος αν ένα πακέτο έχει φτάσει από το δίκτυο και αν έχει προκύψει λήξη του χρόνου.

Η στοίβα Rime, είναι μια "ελαφριά" στοίβα επικοινωνίας σχεδιασμένη για να υποστηρίζει απλές λειτουργίες, όπως είναι η αποστολή ενός μηνύματος σε όλους τους γείτονες, ή σε ένα συγκεκριμένο γείτονα. Μπορεί επίσης να υποστηρίζει και πιο πολύπλοκους μηχανισμούς, όπως είναι η "πλημμύρα" του δικτύου (network flooding). Τα πρωτόκολλα στην στοίβα Rime, είναι διατεταγμένα με ένα πολυεπίπεδο τρόπο όπου τα περισσότερο πολύπλοκα πρωτόκολλα είναι υλοποιημένα με πρωτόκολλα λιγότερο πολύπλοκα.

Για την Rime στοίβα, έχουν επιλεχθεί αρχέτυποι τύποι επικοινωνίας, σύμφωνα με τα πρωτόκολλα που χρησιμοποιεί ένα δίκτυο αισθητήρων, οι οποίοι μπορεί να είναι ενός ή πολλαπλών hops.
Πρωτόκολλα ή εφαρμογές που τρέχουν πάνω από την Rime στοίβα, μπορούν να υλοποιήσουν επιπρόσθετα πρωτόκολλα τα οποία δεν βρίσκονται μέσα στην στοίβα [58].

4.2 Εργαλείο προσομοίωσης Cooja

Το Cooja είναι ένα εργαλείο προσομοίωσης δικτύου του Contiki, το οποίο επιτρέπει την δημιουργία δικτύων οποιουδήποτε μεγέθους, από Contiki motes, και στην συνέχεια γίνεται μια προσομοίωση του δικτύου, σε επίπεδο υλικού. Η προσομοίωση σε επίπεδο υλικού είναι μεν πολύ πιο αργή, όμως επιτρέπει ακριβή έλεγχο της συμπεριφοράς του συστήματος.
Βέβαια υπάρχει και η δυνατότητα προσομοίωσης η οποία δίνει λιγότερες πληροφορίες με μεγαλύτερη ταχύτητα, επιτρέποντας έτσι προσομοιώσεις δικτύων μεγαλύτερου μεγέθους.
Οι προσομοιώσεις που γίνονται με το Cooja εξυπηρετούν στην αξιολόγηση του κώδικα πριν αυτός χρησιμοποιηθεί για τον τελικό σκοπό [58]. Ουσιαστικά ο κώδικας ο οποίος θα δημιουργηθεί με την χρήση του εργαλείου αυτού είναι δυνατόν να προσαρμοστεί απευθείας σε κάποιον αισθητήριο κόμβο.

4.3 Συστήματα Ανίχνευσης Εισβολής

Με την χρήση λοιπόν του Contiki OS, δημιουργήθηκαν και προσομοιώθηκαν κάποιοι τύποι επιθέσεων, προκειμένου να βρεθούν στην συνέχεια κάποιοι τρόποι αντιμετώπισης αυτών των τύπων επιθέσεων.

Συστήματα λοιπόν για την αντιμετώπιση κακόβουλων επιθέσεων που μπορεί να δεχτεί ένα δίκτυο, ονομάζονται Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection System).
Βασικός στόχος ενός τέτοιου συστήματος, είναι να προστατεύσει το δίκτυο από πιθανές επιθέσεις που μπορεί να προκύψουν. Προσπαθεί να προστατεύσει τόσο τις υπηρεσίες οι οποίες προσφέρονται από το δίκτυο, όσο και τα δεδομένα που διακινούνται μέσα στο δίκτυο. [53]

Αυτό που ουσιαστικά κάνει ένα τέτοιο σύστημα είναι να παρακολουθεί το δίκτυο μέχρι να ανιχνεύσει πιθανή εισβολή , οπότε ειδοποιεί τους χρήστες αφού όντως ανιχνεύσει κάποια εισβολή και στην συνέχεια γίνεται προσπάθεια για

αναδιαμόρφωση του δικτύου, έτσι ώστε να εμποδιστεί η ολοκλήρωση της επίθεσης [42][14][60].

Μερικά IDS χρησιμοποιούν τα αρχεία καταγραφής system log files, network traffic ή πακέτα μέσα στο δίκτυο για να μαζέψουν πληροφορίες για να προχωρήσουν στο συμπέρασμα αν όντως υπάρχει προσπάθεια για εισβολή μέσα στο δίκτυο.

Το IDS βασίζεται σε δύο σενάρια ανίχνευσης επιθέσεων. Στην μια περίπτωση, συνδυάζει τα προηγούμενα και κατά συνέπεια γνωστά, μοτίβα ανώμαλης συμπεριφοράς, τα οποία βρίσκονται σε μια εσωτερική βάση υπογραφών, ενώ στην δεύτερη περίπτωση ελέγχει την συμπεριφορά που προκύπτει από κανονικά δεδομένα και συγκρίνει την απόκλιση της συμπεριφοράς του δικτύου με την συμπεριφορά η οποία αναμενόταν βάσει των δεδομένων αυτών [53].

Κάποια συστήματα μπορούν απλώς να ανιχνεύσουν την εισβολή μέσα στο δίκτυο και να προσπαθήσουν να την αποτρέψουν, ενώ κάποια άλλα προχωρούν στην συλλογή πληροφοριών για την επίθεση, όπως για παράδειγμα ποιος είναι ο τύπος της επίθεσης κτλ. [42]

Το σύστημα αυτό έχει την δυνατότητα να παρέχει προστασία από επιθέσεις οι οποίες γίνονται είτε από εσωτερικούς είτε από εξωτερικούς κόμβους. Αυτό καθιστά πολύ απαραίτητη την ύπαρξη του μέσα στο δίκτυο αφού μόνο ο μηχανισμός της κρυπτογράφησης δεν είναι ικανός να παρεμποδίσει επιθέσεις που προέρχονται από κόμβους οι οποίοι βρίσκονται στο εσωτερικό του δικτύου, μιας και αυτοί έχουν ήδη το κλειδί της αποκρυπτογράφησης [49][34].

Προκειμένου το IDS να είναι λειτουργικό και να δουλεύει με επιτυχία, χρειάζεται να έχει κάποιες συγκεκριμένες δυνατότητες όπως είναι οι παρακάτω:
-Απλότητα, δεν πρέπει δηλαδή να σπαταλά άδικα τους πόρους των κόμβων αφού αυτοί είναι περιορισμένοι και χρειάζονται στην εξυπηρέτηση της μεταξύ τους επικοινωνίας και της επεξεργασίας των δεδομένων τους.
-Ευελιξία, να μπορεί δηλαδή να συμπεριλάβει νέους μηχανισμούς ανίχνευσης επίθεσης.
-Ανθεκτικότητα, που σημαίνει πως το σύστημα πρέπει να είναι ανθεκτικό στις επιθέσεις που γίνονται ενάντια στο ίδιο το σύστημα [29].

Η ασφάλεια είναι ένας πολύ σημαντικός παράγοντας όσο αφορά τα ασύρματα δίκτυα αισθητήρων, προκειμένου να μπορούν να αντιμετωπιστούν οι επιθέσεις που γίνονται, το σύστημα ανίχνευσης βρίσκεται στην δεύτερη γραμμή άμυνας κατά των επιθέσεων, αφού με αυτό τον τρόπο γίνεται προσπάθεια αντιμετώπισης των επιθέσεων πριν αυτές να γίνουν, συμπληρώνοντας έτσι με αυτό τον τρόπο την ασφάλεια των δικτύων [42].

Κεφάλαιο 5

Υλοποίηση Επιθέσεων και Εξαγωγή Αποτελεσμάτων

5.1 Flooding Attack
5.2 Selective Forwarding Attack
5.3 Black Hole Attack

Αφού λοιπόν μελετήθηκαν κάποιοι ιοί ως προς τον τρόπο με τον οποίο δρουν, ακολούθησε η υλοποίηση μερικών από αυτούς. Οι επιθέσεις αυτές υλοποιήθηκαν και προσομοιώθηκαν με την βοήθεια του λειτουργικού συστήματος Contiki, και συγκεκριμένα χρησιμοποιώντας το εργαλείο Cooja, το οποίο περιγράφτηκε πιο πάνω ως προς τον τρόπο λειτουργίας του.

Σκοπός ήταν ουσιαστικά αφού τοποθετηθούν μερικοί κακόβουλοι κόμβοι, μολυσμένοι με αυτούς τους ιούς, να μελετηθεί ο τρόπος με τον οποίο αυτοί επηρεάζουν ολόκληρο το δίκτυο, λαμβάνοντας κάποιες μετρήσεις, μέσω των προσομοιώσεων. Με αυτό τον τρόπο είναι δυνατόν πλέον να βρεθούν ευκολότερα τρόποι αντιμετώπισης των συγκεκριμένων ιών.

Στην συνέχεια της διπλωματικής αυτής εργασίας, παρουσιάζονται τα αποτελέσματα και τα συμπεράσματα που προέκυψαν κατά την προσομοίωση των ιών αυτών στο περιβάλλον Cooja, με την δημιουργία κατάλληλων γραφικών παραστάσεων.

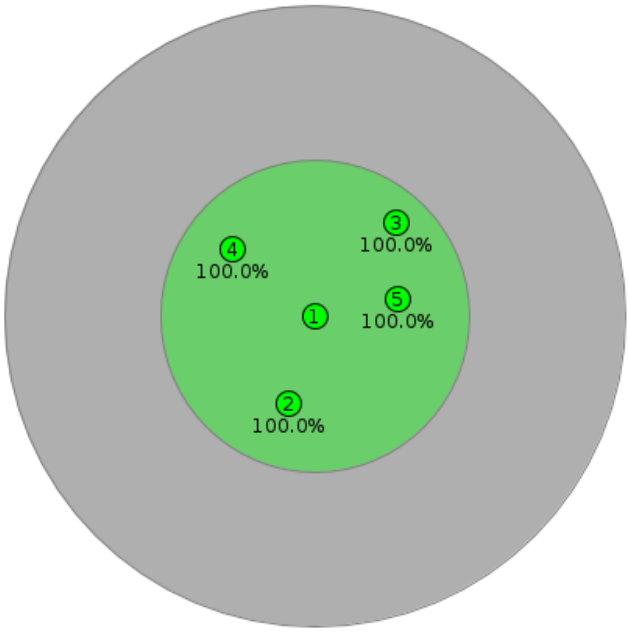
Αρχικά παρουσιάζεται ο ιός Flooding με μια περιγραφή του τι μπορεί αυτός ο ιός να προκαλέσει, και με ποιο τρόπο. Στην συνέχεια περιγράφεται αναλυτικά ο ιός Selective Forwarding, και τέλος ο ιός Black Hole.

5.1 Flooding Attack

5.1.1 Unicast

Στην πιο κάτω εικόνα φαίνεται η τοπολογία του δικτύου το οποίο χρησιμοποιώ για να πάρω τις μετρήσεις μου, χρησιμοποιώντας unicast μετάδοση πακέτων.

Βασική προϋπόθεση είναι όλοι οι κόμβοι να βρίσκονται μέσα στην εμβέλεια του κόμβου 1 ο οποίος είναι και ο παραλήπτης των πακέτων που στέλνουν οι υπόλοιποι κόμβοι.
Ο λόγος που πρέπει να βρίσκονται όλοι οι κόμβοι μέσα στην εμβέλεια του παραλήπτη του πακέτου είναι γιατί ο κόμβος 1 (τελικός παραλήπτης), ελέγχει τον αποστολέα του πακέτου το οποίο φτάνει και αν αυτός είναι πάνω από 1 hop μακριά τότε το πακέτο καταστρέφεται.



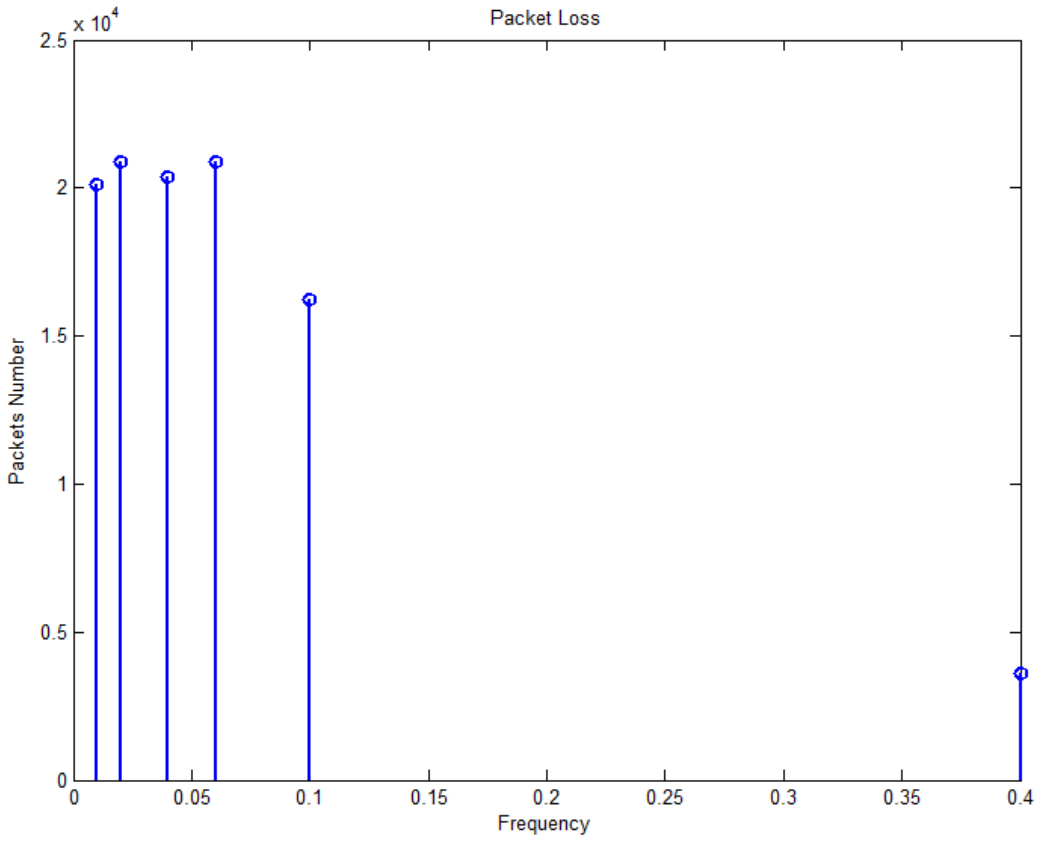
Τοπολογία 1.1.1

Στην πρώτη μέτρηση σκοπός ήταν να βρεθεί για ποιά συχνότητα το δίκτυο θα μπορέσει να δώσει πιο ξεκάθαρα αποτελέσματα όταν σε αυτό προστεθούν κακόβουλοι κόμβοι. Δείχνει δηλαδή καλύτερα την διαφορά που προκαλεί στο δίκτυο ένας κόμβος ο οποίος είναι κακόβουλος.

Η πιο κάτω γραφική παράσταση προκύπτει από την πρώτη προσομοίωση όπου έχουμε ένα δίκτυο με καθόλου κακόβουλους κόμβους. Δείχνει πόση είναι η απώλεια των πακέτων μέσα σε ένα δίκτυο το οποίο χρησιμοποιεί Unicast μετάδοση πακέτων, σύμφωνα με την συχνότητα που χρησιμοποιείται.

Ο άξονας x παριστάνει τις συχνότητες οι οποίες χρησιμοποιήθηκαν για την λήψη των μετρήσεων και ο άξονας y δείχνει των αριθμό των πακέτων που χάνονται για κάθε μία συχνότητα.

Όσο πιο μικρή είναι η τιμή της συχνότητας αυτό σημαίνει πως ο αριθμός των πακέτων που στέλνεται μέσα σε ένα συγκεκριμένο χρονικό διάστημα αυξάνεται, όπου προκαλείται έτσι μια υπερφόρτωση στο δίκτυο. Στην αντίθετη περίπτωση όπου η τιμή της συχνότητας είναι υπερβολικά μεγάλη, πλησιάζει δηλαδή το 1, τότε δεν θα παρουσιάζεται σημαντική διαφορά στον αριθμό των πακέτων που στέλνονται.



Όπως παρατηρείται και από την γραφική παράσταση, η συχνότητα η οποία προκαλεί την μεγαλύτερη απώλεια πακέτων είναι το 0.02 ενώ αυτή με την μικρότερη απώλεια είναι η 0,4.

Για την λήψη αυτών των τιμών χρειάστηκε να δημιουργηθεί ένα
δίκτυο (Τοπολογία 1.1.1) στο οποίο έγιναν 3 προσομοιώσεις για κάθε διαφορετική συχνότητα αλλάζοντας κάθε φορά το seed.
Επιλέγεται ένα random seed για κάθε νέα προσομοίωση έτσι ώστε να γίνεται ένας έλεγχος για διάφορες περιπτώσεις σεναρίων, όπως για παράδειγμα ποιός είναι ο χρόνος στον οποίο ξεκίνησε ο κάθε κόμβος να μεταδίδει.

Στην συνέχεια χρησιμοποιείται ο αριθμός των πακέτων που στάλθηκαν (sent) και ο αριθμός των πακέτων που λήφθηκαν (received), για να βρεθεί ο μέσος όρος για το κάθε σύνολο πακέτων (sent/received), για κάθε μία από τις συχνότητες.
Στην συνέχεια βρίσκοντας την διαφορά των μέσων όρων των δύο συνόλων πακέτων για κάθε συχνότητα προκύπτει ουσιαστικά το μέγεθος της απώλειας των πακέτων μέσα στο δίκτυο.

Για την επιλογή της συχνότητας με την οποία θα γίνουν οι υπόλοιπες προσομοιώσεις, χρειάζεται να βρεθεί ο μέσος όρος των πακέτων που δεν έφτασαν στον τελικό προορισμό (packet loss), για την συχνότητα η οποία προκαλεί την μικρότερη απώλεια πακέτων μέσα στο δίκτυο και για την συχνότητα που προκαλεί την μεγαλύτερη απώλεια μέσα στο δίκτυο:

(packet_loss_freq_0.4 + packet_loss_freq_0.02)/2=12256

Ακολούθως γίνεται σύγκριση του μέσου όρου κάθε μίας από τις συχνότητες με τον μέσο όρο που προκύπτει από τον σύνολο των συχνοτήτων. Η συχνότητα η οποία έχει την πιο κοντινή τιμή μέσου όρου με την πιο πάνω τιμή, τότε αυτή θα επιλεγεί για τις υπόλοιπες μετρήσεις.

Σενάρια

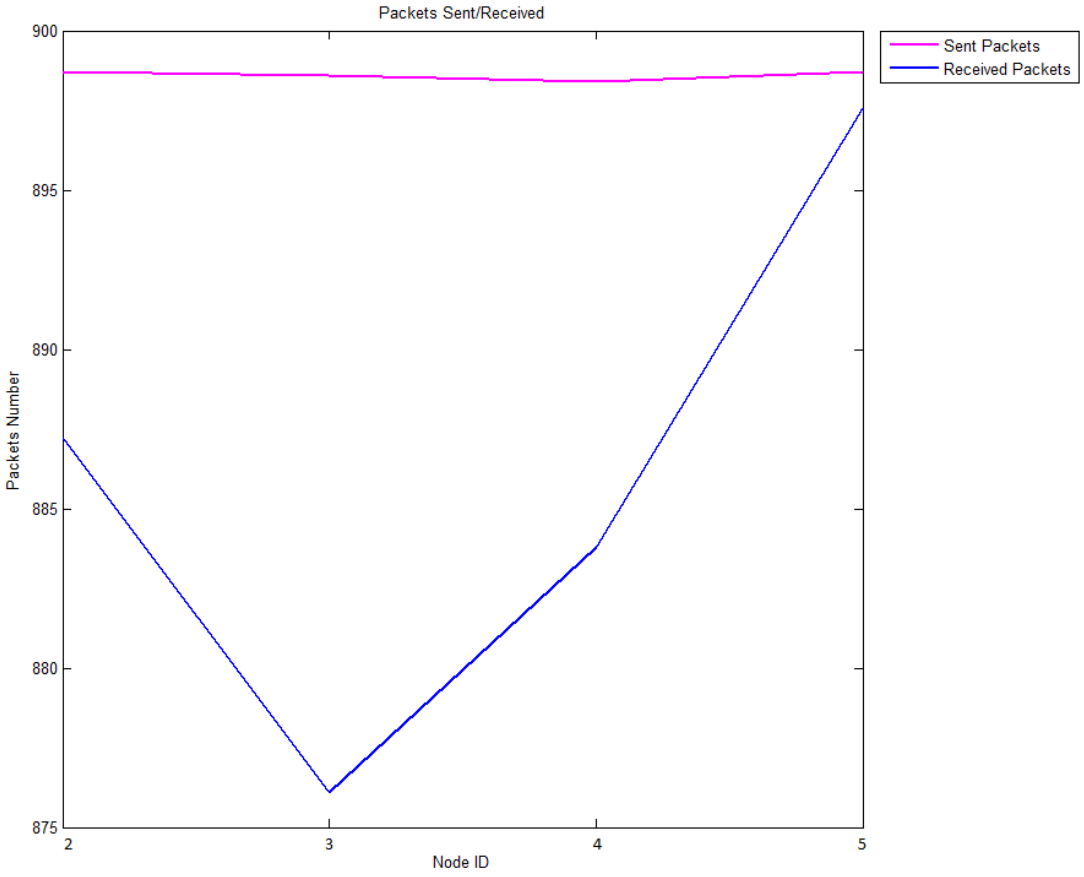
Σε όλα τα πιο κάτω σενάρια χρησιμοποιείται συχνότητα 0,1 και η τοπολογία του δικτύου παραμένει σταθερή.
Ο αριθμός των κακόβουλων και υγειών κόμβων αλλάζει, παραμένει σταθερή όμως η τιμή της συχνότητας μετάδοσης των πακέτων.

Στις παρακάτω γραφικές παραστάσεις, ο άξονας y αναπαριστά τον αριθμό των πακέτων που κινούνται μέσα στο δίκτυο και ο άξονας x δείχνει τον κόμβο στον οποίο αντιστοιχεί ο αριθμός των πακέτων. Σε κάθε μία από αυτές τις προσομοιώσεις αλλάζει μόνο το seed κάθε φορά.

Στις τοπολογίες που παρουσιάζονται στα επόμενα σενάρια, οι κακόβουλοι κόμβοι διαφέρουν ως προς το χρώμα με τους υγιείς κόμβους. Συγκεκριμένα οι υγιείς κόμβοι ξεχωρίζουν με χρώμα πράσινο ενώ οι μολυσμένοι παρουσιάζονται με πορτοκαλί χρώμα.

Ο λόγος που γίνεται αυτή η προσομοίωση είναι για χρησιμοποιηθούν μετά οι γραφικές παραστάσεις που προκύπτουν ως μέτρο σύγκρισης.
Συγκρίνοντας δηλαδή τις γραφικές οι οποίες αντιπροσωπεύουν δίκτυα με κακόβουλους κόμβους με την γραφική ενός δικτύου με υγιείς κόμβους μπορούν να διεξαχθούν ευκολότερα και ακριβέστερα τα συμπεράσματα.

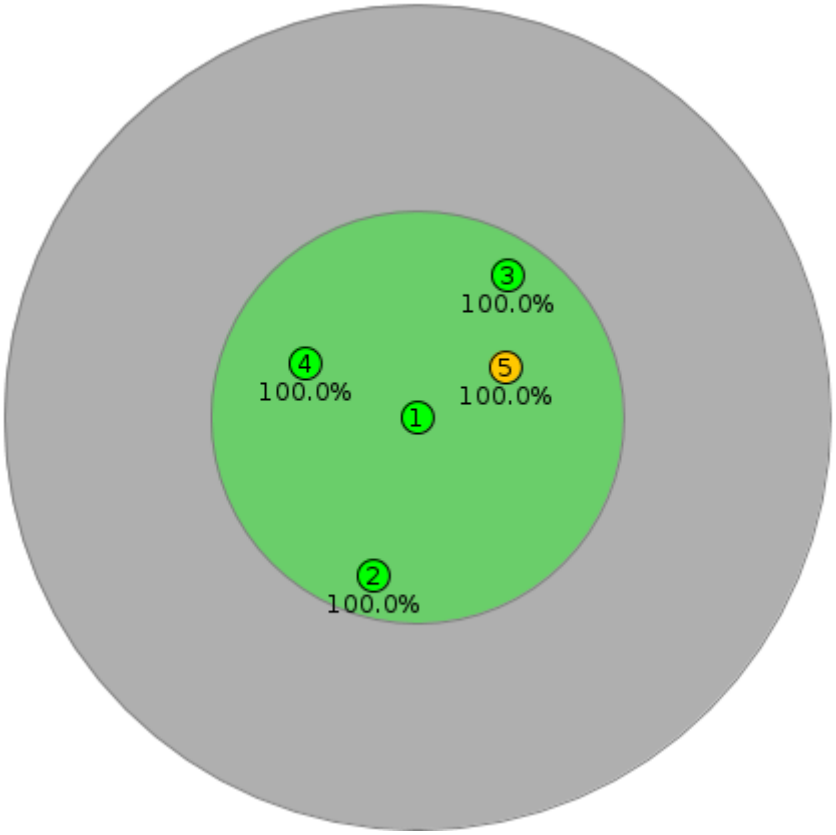
Σενάριο 1.1.1
5 Benign – 0 Malicious Nodes
Τοπολογία 1.1.1



Σε αυτό το σενάριο υπάρχει μόνο ένας κακόβουλος κόμβος ενώ οι υπόλοιποι είναι υγιείς.
Από την γραφική παράσταση, παρατηρείται πως ο αριθμός των πακέτων που στέλνουν όλοι οι κόμβοι κυμαίνεται στις ίδιες τιμές.
Ο κόμβος με τον αριθμό 1, ο οποίος είναι και ο τελικός παραλήπτης (sink node), δεν συμπεριλαμβάνεται μέσα στην γραφική παράσταση αφού στην περίπτωση του Unicast όλοι στέλνουν πακέτα σε αυτόν ενώ ο ίδιος είναι σε θέση μόνο να παραλαμβάνει τα πακέτα που φτάνουν σε αυτόν.

Οι μέσοι όροι των πακέτων που στέλνει ο κάθε κόμβος και που παραλαμβάνει ο κόμβος 1 από τον κάθε κόμβο, είναι παραπλήσιοι.
Υπάρχουν κάποιες απώλειες πακέτων μέσα στο δίκτυο οι οποίες όμως είναι αμελητέες.

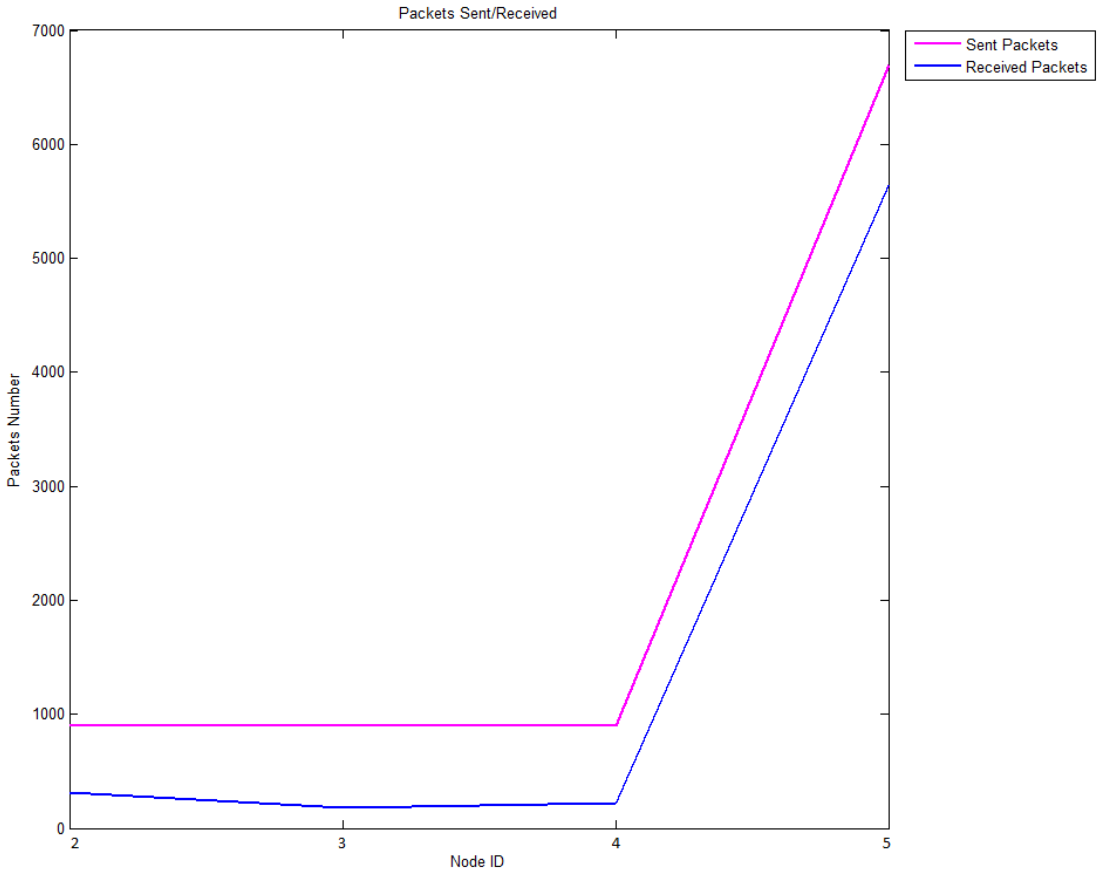
Σενάριο 1.1.2
4 Benign – 1 Malicious Nodes



Τοπολογία 1.1.2

Στην συγκεκριμένη τοπολογία, παρουσιάζεται ένας κακόβουλος κόμβος, ενώ όλοι οι υπόλοιποι κόμβοι του δικτύου είναι καθαροί.

Σενάριο 1.1.2
4 Benign – 1 Malicious Nodes
Τοπολογία 1.1.2

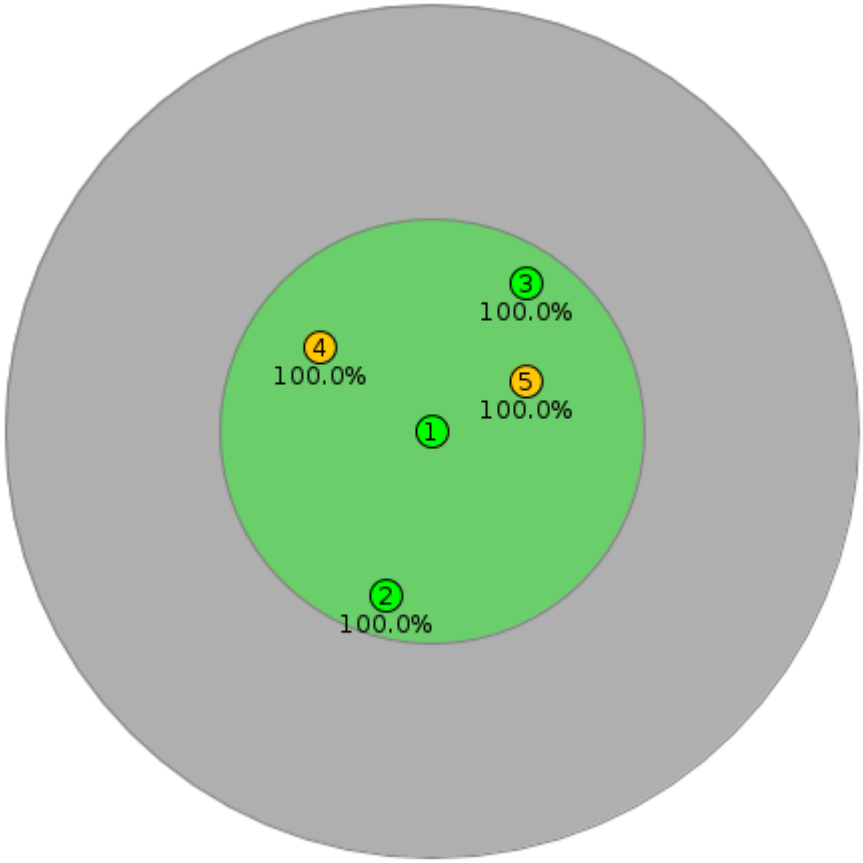


Σε αυτή την περίπτωση μέσα στο δίκτυο υπάρχει ένας "μολυσμένος" κόμβος ο οποίος όπως φαίνεται ξεκάθαρα και από την γραφική παράσταση είναι ο κόμβος 5.

Ο συνολικός αριθμός των πακέτων που στέλνονται τώρα μέσα στο δίκτυο είναι εμφανώς μεγαλύτερος και αυτό οφείλεται στην παρουσία του κακόβουλου κόμβου.

Όσο αφορά την απώλεια των πακέτων μέσα στο δίκτυο, έχει αυξηθεί, τόσο για πακέτα τα οποία φτάνουν από τους "υγιείς" κόμβους όσο και από τον κακόβουλο κόμβο. Ο λόγος που χάνεται μεγαλύτερος αριθμός πακέτων από τους υγιείς κόμβους οφείλεται στο γεγονός ότι το δίκτυο υπερφορτώνεται από τον πολύ μεγάλο αριθμό πακέτων που στέλνει ο κακόβουλος κόμβος μέσα στο δίκτυο. Οπότε ο κόμβος 1 αδυνατεί να εξυπηρετήσει ένα τόσο μεγάλο αριθμό από πακέτα συνεπώς απορρίπτει όλο και περισσότερα.
Από την γραφική φαίνεται πως επηρεάζεται ολόκληρο το δίκτυο με την παρουσία ενός και μόνο κακόβουλου κόμβου.

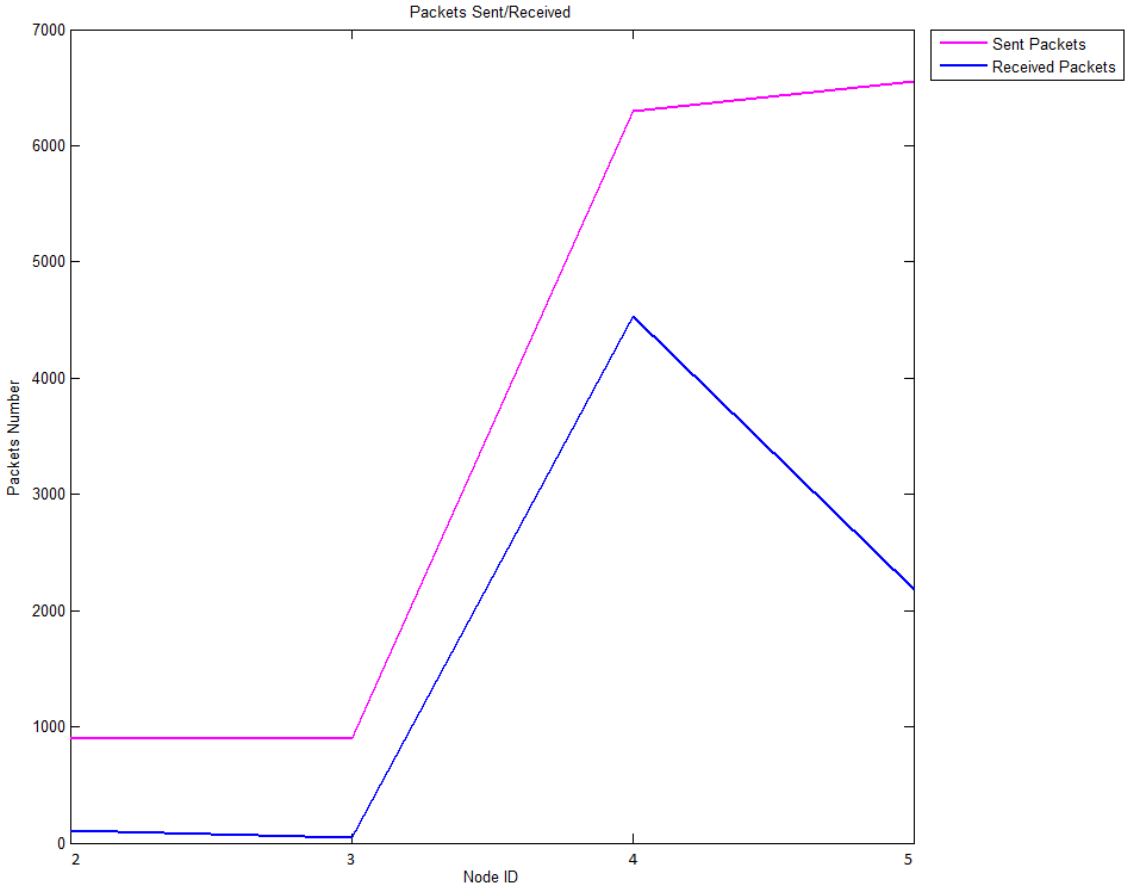
Σενάριο 1.1.3
3 Benign – 2 Malicious Nodes



Τοπολογία 1.1.3

Στην συγκεκριμένη τοπολογία παρουσιάζονται 2 κακόβουλοι κόμβοι ενώ οι υπόλοιποι παραμένουν υγιείς.

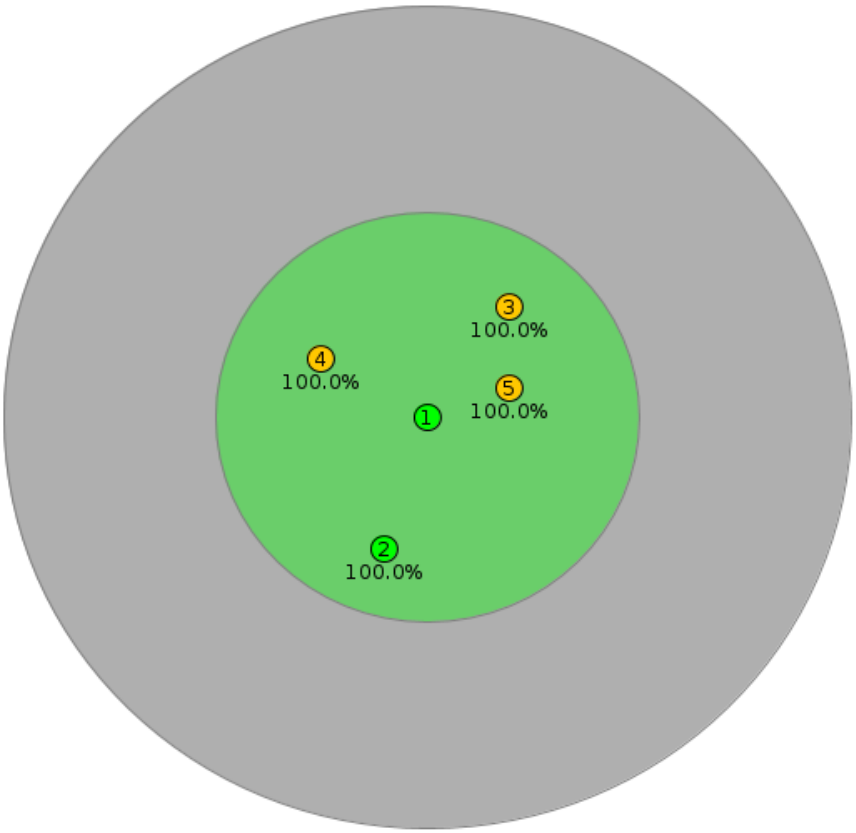
Σενάριο 1.1.3
3 Benign – 2 Malicious Nodes
Τοπολογία 1.1.3



Παρατηρώντας αυτή την γραφική παράσταση βλέπουμε πως οι 2 "μολυσμένοι" κόμβοι αντιδρούν σχεδόν το ίδιο. Ο μέσος όρος της ποσότητας των πακέτων που στέλνουν είναι περίπου ο ίδιος και για τους δύο. Όπως είναι αναμενόμενο, ο αριθμός των πακέτων που στέλνουν οι υπόλοιποι κόμβοι παραμένει σταθερός σε σχέση με το αρχικό σενάριο.

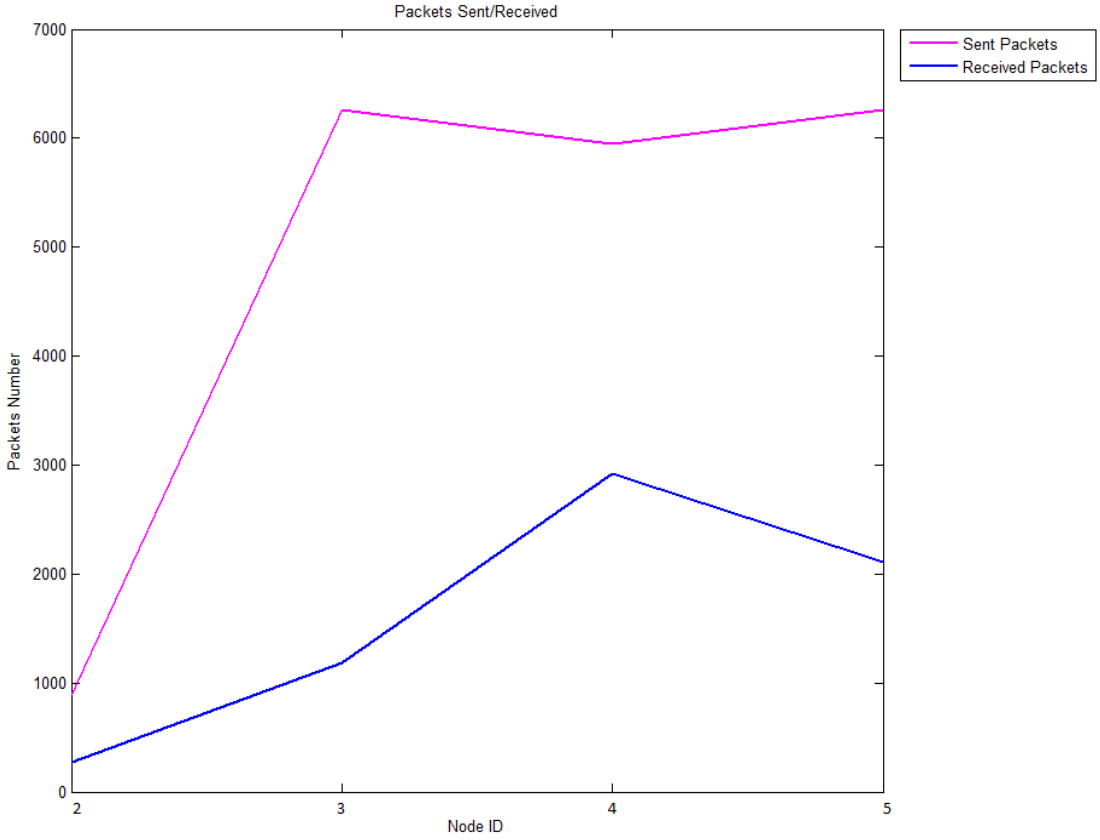
Σε αυτή την περίπτωση ο αριθμός των κακόβουλων κόμβων έχει αυξηθεί και κατά συνέπεια το ίδιο ισχύει και για τον συνολικό αριθμό των πακέτων που κινούνται τώρα μέσα στο δίκτυο.
Η απώλεια των πακέτων έχει αυξηθεί ακόμα περισσότερο για όλους τους κόμβους του δικτύου.

Σενάριο 1.1.4
2 Benign – 3 Malicious Nodes



Τοπολογία 1.1.4
Η τοπολογία αυτή θα χρησιμοποιηθεί για τις επόμενες προσομοιώσεις και αναπαριστά τρεις κακόβουλους κόμβους και 2 υγιείς.

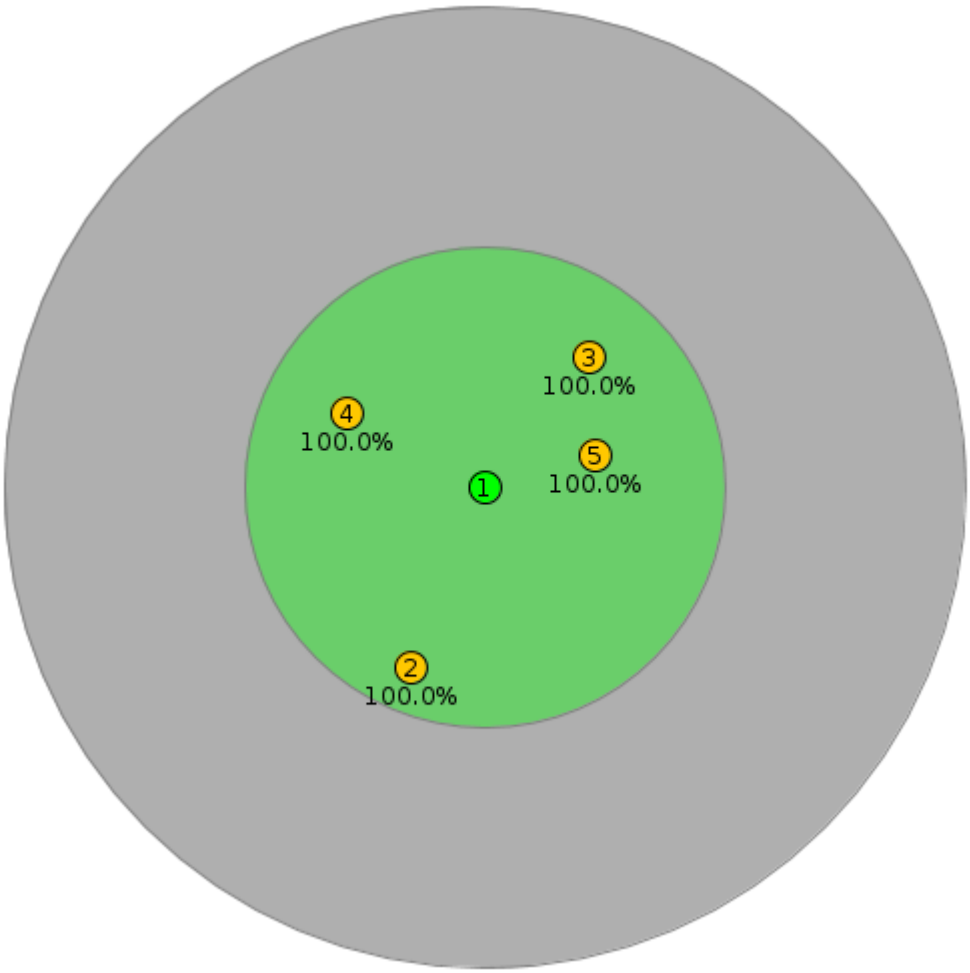
Σενάριο 1.1.4
2 Benign – 3 Malicious Nodes
Τοπολογία 1.1.4



Παρατηρώντας αυτή την γραφική παράσταση και συγκρίνοντας με τις προηγούμενες γραφικές παραστάσεις βλέπουμε ότι ο αριθμός των πακέτων που λαμβάνει από τον καθένα ο κόμβος 1 σε σχέση με τον αριθμό των πακέτων που στέλνονται είναι κατά πολύ μικρότερος.

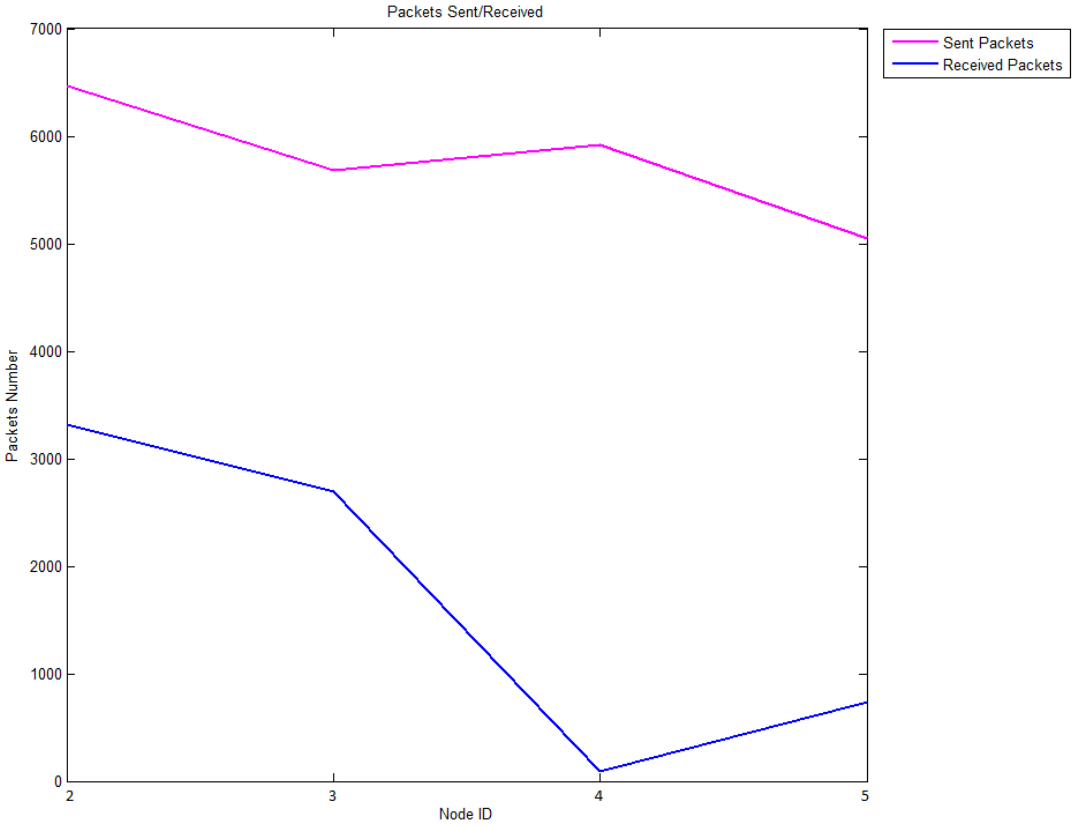
Οπότε παρατηρείται μια απώλεια πακέτων η οποία αυξάνεται με την αύξηση του αριθμού των κακόβουλων κόμβων μέσα στο δίκτυο.

Σενάριο 1.1.5
1 Benign – 4 Malicious Nodes



Τοπολογία 1.1.5
Ο μοναδικός υγιής κόμβος είναι τώρα ο τελικός παραλήπτης.

Σενάριο 1.1.5
1 Benign – 4 Malicious Nodes
Τοπολογία 1.1.5



Σε αυτό το σενάριο έχουμε μόνο “μολυσμένους ” κόμβους. Είναι εμφανές ότι η απώλεια των πακέτων έχει αυξηθεί πολύ περισσότερο σε σχέση με την απώλεια των πακέτων που υπήρχε σε κάθε προηγούμενο σενάριο.

Από την στιγμή που κάθε ένας από τους κόμβους – αποστολέας του δικτύου, στέλνει μια τεράστια ποσότητα από πακέτα, είναι αναμενόμενο ότι θα υπάρχουν ακόμα περισσότερες συγκρούσεις πακέτων από κάθε άλλη προηγούμενη περίπτωση.

Γενικά συμπεράσματα:

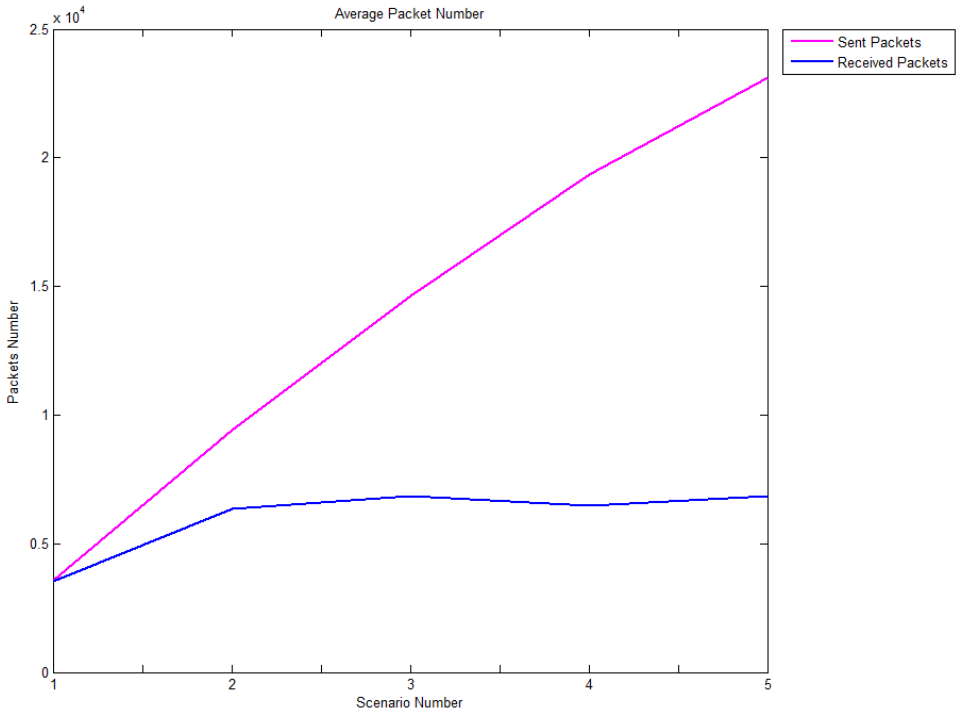
Το ότι χάνεται μεγάλος αριθμός πακέτων μέσα στο δίκτυο, οφείλεται στο ότι η συχνότητα με την οποία οι κακόβουλοι κόμβοι στέλνουν τα πακέτα τους έχει αρκετά μικρή τιμή, δηλαδή στην μονάδα του χρόνου στέλνονται πολλά περισσότερα πακέτα μέσα στο δίκτυο από όσα θα έπρεπε.

Μέσα στο ίδιο χρονικό διάστημα ένας κακόβουλος κόμβος μπορεί να στείλει ένα πολύ μεγαλύτερο αριθμό πακέτων από ένα κανονικό κόμβο.

Όσο περισσότερα πακέτα στέλνει ένας κόμβος στον τελικό προορισμό τότε τόσο περισσότερα πακέτα χάνονται.
Το δίκτυο υπερφορτώνεται και επειδή ο παραλήπτης δεν μπορεί να επεξεργαστεί όλα τα πακέτα λόγω του ότι φτάνει ένας υπερβολικά μεγάλος αριθμός πακέτων μέσα σε πολύ μικρό χρονικό διάστημα, γεμίζοντας το buffer του, τότε αυτά καταστρέφονται.

Γενικότερα, ο τρόπος με τον οποίο προσπαθεί ένας κακόβουλος κόμβος να καταστρέψει το δίκτυο, είναι ότι στέλνοντας πολλά πακέτα στο παραλήπτη αυτός στην προσπάθεια του να επεξεργαστεί όλα τα πακέτα που φθάνουν και μη μπορώντας να ανταποκριθεί σε ένα μεγάλο αριθμό πακέτων σε μικρό χρονικό διάστημα απορρίπτει πακέτα, πολλά από τα οποία προέρχονται και από κόμβους οι οποίοι δεν είναι μολυσμένοι.

Για την λήψη των πιο πάνω μετρήσεων έγιναν προσομοιώσεις, με την ίδια τοπολογία δικτύου, όμως διαφορετικό αριθμό malicious-benign nodes. Για κάθε διαφορετικό σενάριο malicious-benign χρειάστηκαν 10 διαφορετικές προσομοιώσεις με διαφορετικό seed κάθε φορά όμως με την ίδια συχνότητα.
Επιλέγηκε μια συχνότητα η οποία και έμεινε σταθερή για όλες τις επόμενες μετρήσεις.



Scenario Number	1	2	3	4	5
Scenario Name	5Benign – 0Malicious	4Benign – 1Malicious	3Benign – 2Malicious	2Benign – 3Malicious	1Benign – 4Malicious

Σε αυτή την γραφική φαίνεται ο αριθμός των πακέτων σε συνάρτηση με τον αριθμό του σεναρίου στο οποίο αντιστοιχούν.

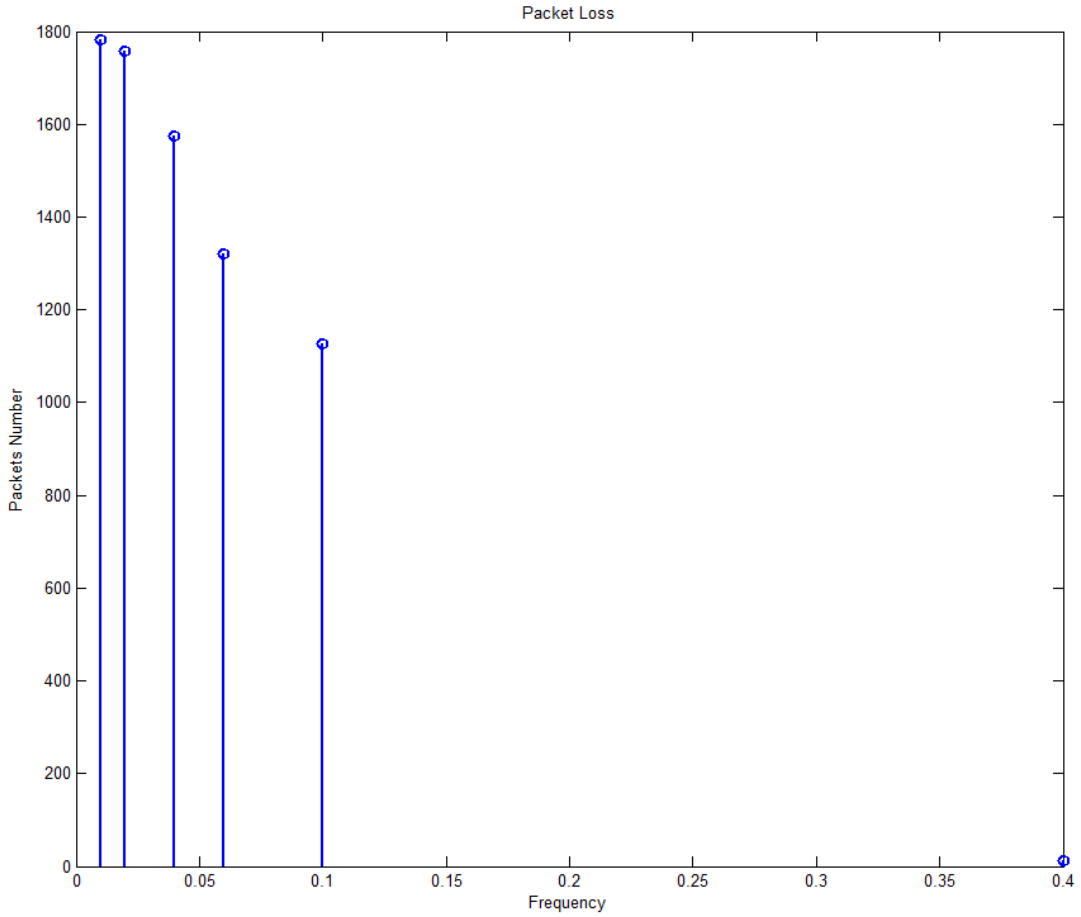
Από την πιο πάνω γραφική παράσταση μπορούμε να δούμε πιο ξεκάθαρα πόσα πακέτα στέλνονται μέσα στο δίκτυο και πόσα παραλαμβάνει στην πραγματικότητα ο τελικός παραλήπτης.

Όπως φαίνεται ξεκάθαρα, όσο αυξάνεται ο αριθμός των μολυσμένων κόμβων, τόσο περισσότερα πακέτα στέλνονται μέσα στο δίκτυο, ενώ υπάρχει ένα σημείο όπου ο αριθμός των πακέτων που παραλαμβάνονται μένει σταθερός (μέχρι τόσα πακέτα μπορεί να επεξεργαστεί ο παραλήπτης).

Όσο λοιπόν αυξάνεται ο αριθμός των κακόβουλων κόμβων τόσο μεγαλώνει η διαφορά του αριθμού των πακέτων που στέλνονται και των πακέτων που παραλαμβάνονται, δηλαδή τόσο αυξάνεται η απώλεια των πακέτων (packet loss).

5.1.2 Runicast

Για τις προσομοιώσεις που έγιναν για την λήψη αποτελεσμάτων με την χρήση Runicast μετάδοσης πακέτων, χρησιμοποιήθηκαν οι ίδιες τοπολογίες που χρησιμοποιήθηκαν στην περίπτωση της Unicast μετάδοσης.



Σε αυτή την γραφική βλέπουμε τον αριθμό των πακέτων που χάνονται μέσα σε ένα δίκτυο ανάλογα με την συχνότητα που χρησιμοποιείται μέσα σε αυτό.
Όσο μικραίνει η τιμή της συχνότητας, τόσο μεγαλύτερη είναι απώλεια των πακέτων. Στον άξονα y είναι ο αριθμός των πακέτων που χάθηκαν και που αντιστοιχούν στην αντίστοιχη συχνότητα που βρίσκεται στον άξονα x.

Για την πιο πάνω γραφική παράσταση χρειάστηκε να δημιουργηθεί ένα δίκτυο κατά το οποίο η τοπολογία δεν άλλαζε όπως ούτε και ο αριθμός των benign-malicious nodes. Τοποθετήθηκαν 5 benign nodes και 0 malicious, όπου για το κάθε σενάριο χρειάστηκε να γίνουν 3 προσομοιώσεις για κάθε διαφορετική συχνότητα όπου για κάθε προσομοίωση άλλαζε το seed.

Για να επιλεγεί η συχνότητα με την οποία θα έτρεχαν τα υπόλοιπα σενάρια, βρέθηκε ο μέσος όρος των πακέτων που δεν έφτασαν στον τελικό προορισμό, για την

συχνότητα η οποία προκαλεί την μικρότερη απώλεια πακέτων μέσα στο δίκτυο και για την συχνότητα που προκαλεί την μεγαλύτερη απώλεια μέσα στο δίκτυο: (packet_loss_freq_0.4 + packet_loss_freq_0.01)/2=897,33

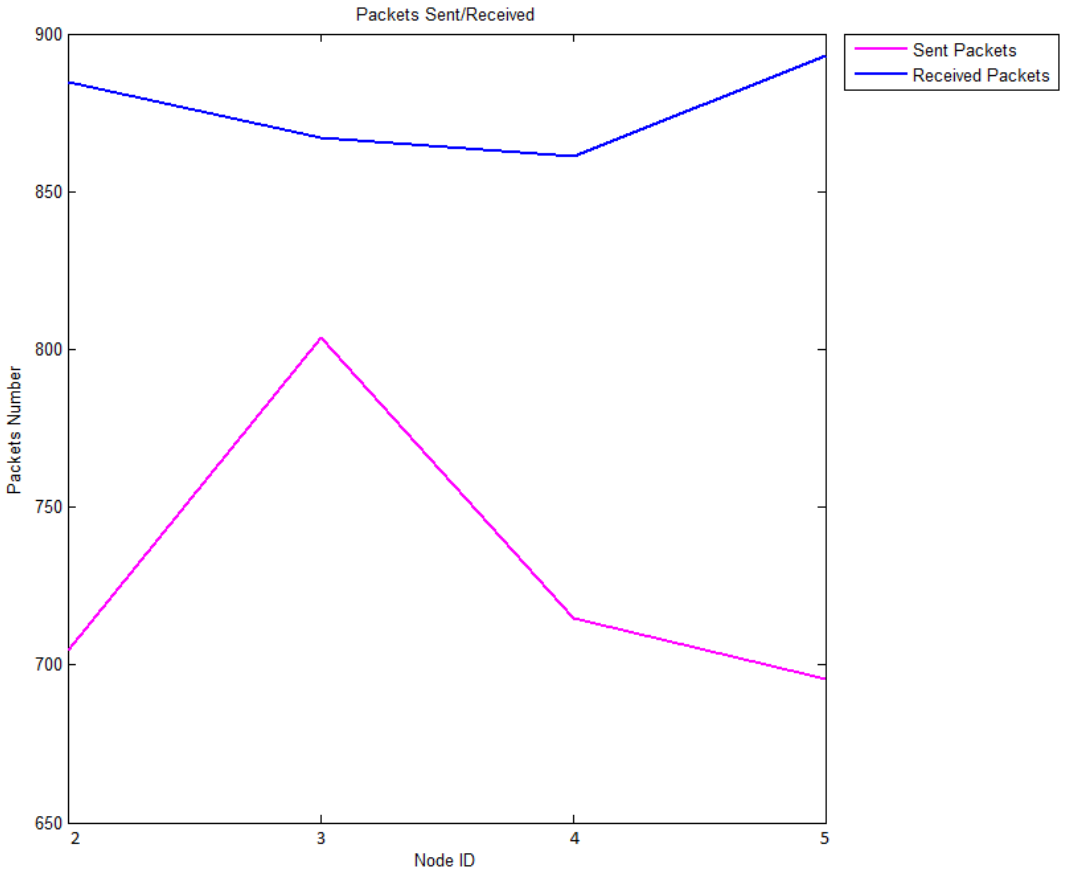
Η πιο κοντινή τιμή Packet loss στον μέσο όρο που βρέθηκε, είναι η τιμή που προκύπτει όταν η συχνότητα είναι 0,1. Οπότε επιλέγεται αυτή την συχνότητα για τις προσομοιώσεις για το runicast.

Σενάρια

Σε όλα τα πιο κάτω σενάρια χρησιμοποιείται συχνότητα 0,1 και η τοπολογία του δικτύου παραμένει σταθερή.

Ο άξονας y αναπαριστά τον αριθμό των πακέτων που κινούνται μέσα στο δίκτυο και ο άξονας x δείχνει τον κόμβο στον οποίο αντιστοιχεί ο αριθμός των πακέτων που έστειλε και που έλαβε από αυτόν ο παραλήπτης. Σε κάθε μία από αυτές τις προσομοιώσεις αλλάζει μόνο το seed κάθε φορά.

Σενάριο 1.2.1
5 Benign – 0 Malicious Nodes
Τοπολογία 1.1.1

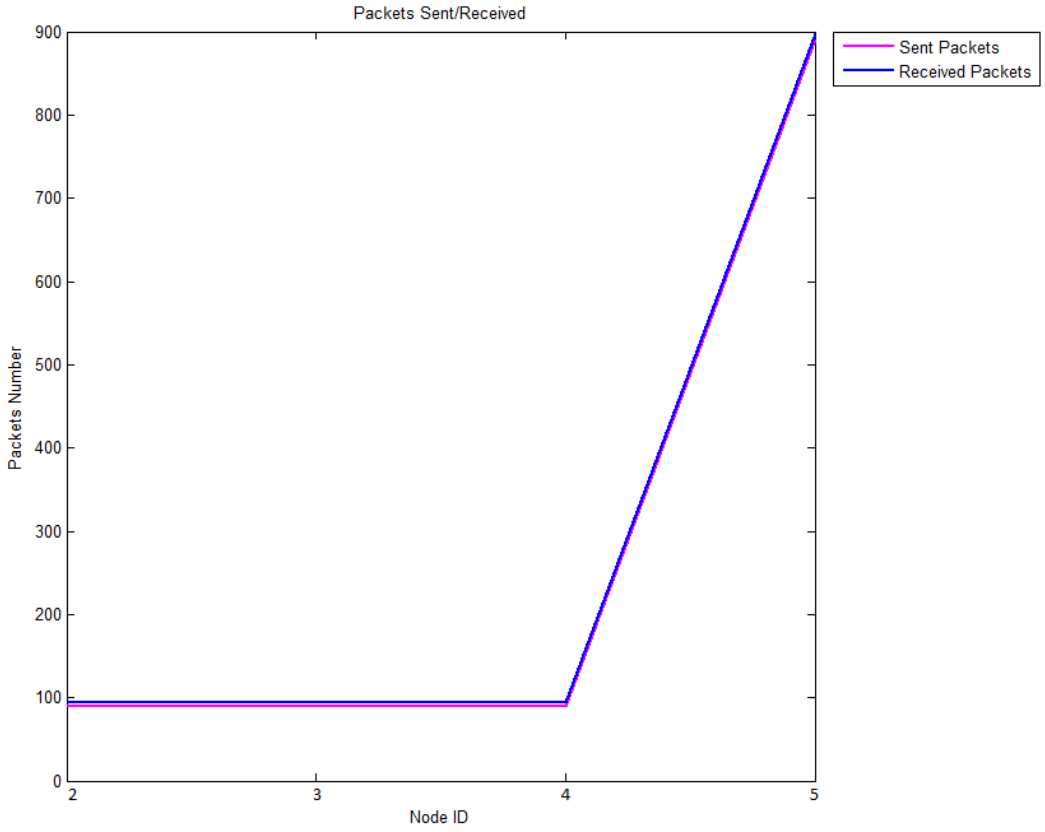


Σε αυτή την γραφική παράσταση δεν υπάρχουν καθόλου κακόβουλοι κόμβοι, και όλοι στέλνουν παραπλήσιο αριθμό πακέτων.

Μέσα στο δίκτυο δεν παρατηρούνται απώλειες πακέτων, αλλά το αντίθετο, τα πακέτα που λαμβάνονται είναι περισσότερα από τα πακέτα που στέλνονται.
Ο λόγος που παρατηρείται αυτό το φαινόμενο, οφείλεται στο γεγονός ότι το runicast αναμεταδίδει κάθε πακέτο το οποίο για κάποιο λόγο είτε δεν φτάνει στον προορισμό του, είτε φτάνει αλλοιωμένο. Επειδή γενικώς μέσα σε ένα δίκτυο, ακόμα και αν αυτό είναι υγιές, υπάρχουν απώλειες, τα πακέτα αναμεταδίδονται από τον αποστολέα τους.

Αυτό επαναλαμβάνεται μέχρι ο παραλήπτης να λάβει το σωστό πακέτο ή μέχρι να πραγματοποιηθεί ένας μέγιστος προκαθορισμένος αριθμός αναμεταδόσεων.

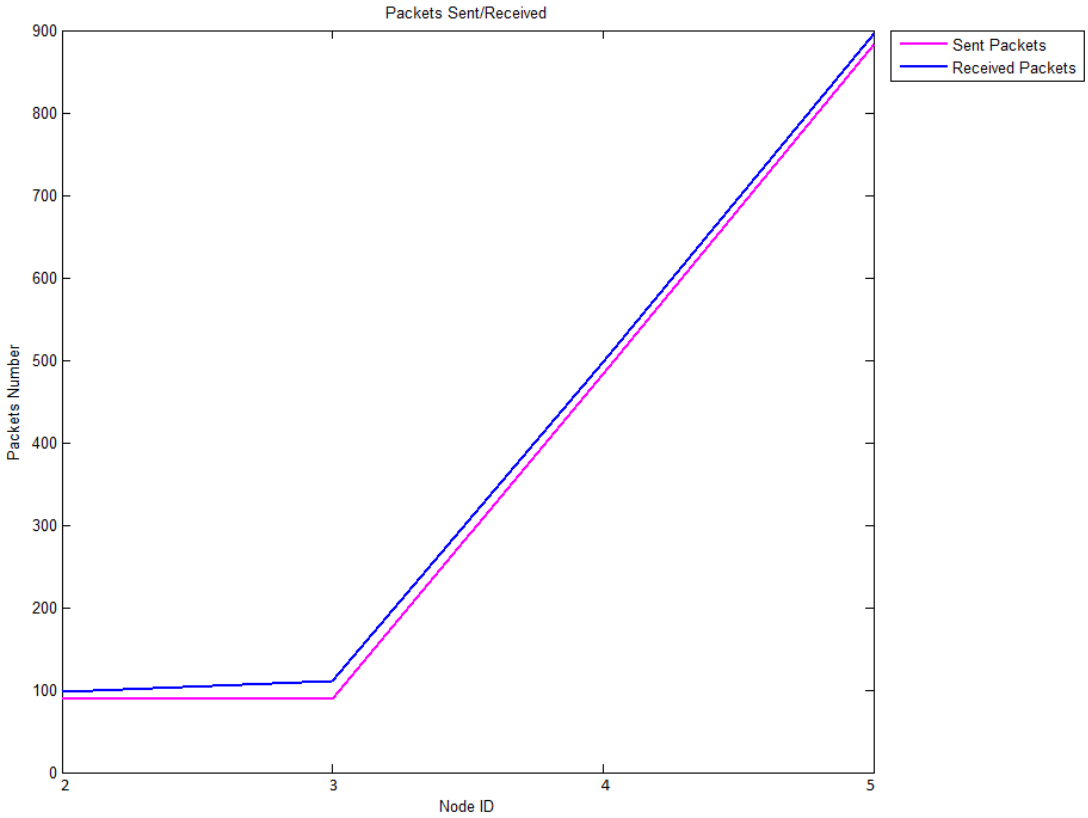
Σενάριο 1.2.2
4 Benign – 1 Malicious Nodes
Τοπολογία 1.1.2



Μέσα στο δίκτυο, σε αυτή την προσομοίωση βρίσκεται ένας κακόβουλος κόμβος, ο οποίος στέλνει εμφανώς πολύ μεγαλύτερο αριθμό από πακέτα μέσα στο δίκτυο.

Αν και δεν φαίνεται, στην πραγματικότητα υπάρχει απώλεια πακέτων μέσα στο δίκτυο. Ο λόγος που ο αριθμός των απεσταλμένων και παραληφθέντων πακέτων είναι ο ίδιος, πολύ πιθανώς να οφείλεται στο γεγονός ότι πολλά από τα πακέτα φτάνουν αλλοιωμένα και αναμεταδίδονται, κάτι το οποίο επεξηγήθηκε πιο πάνω.

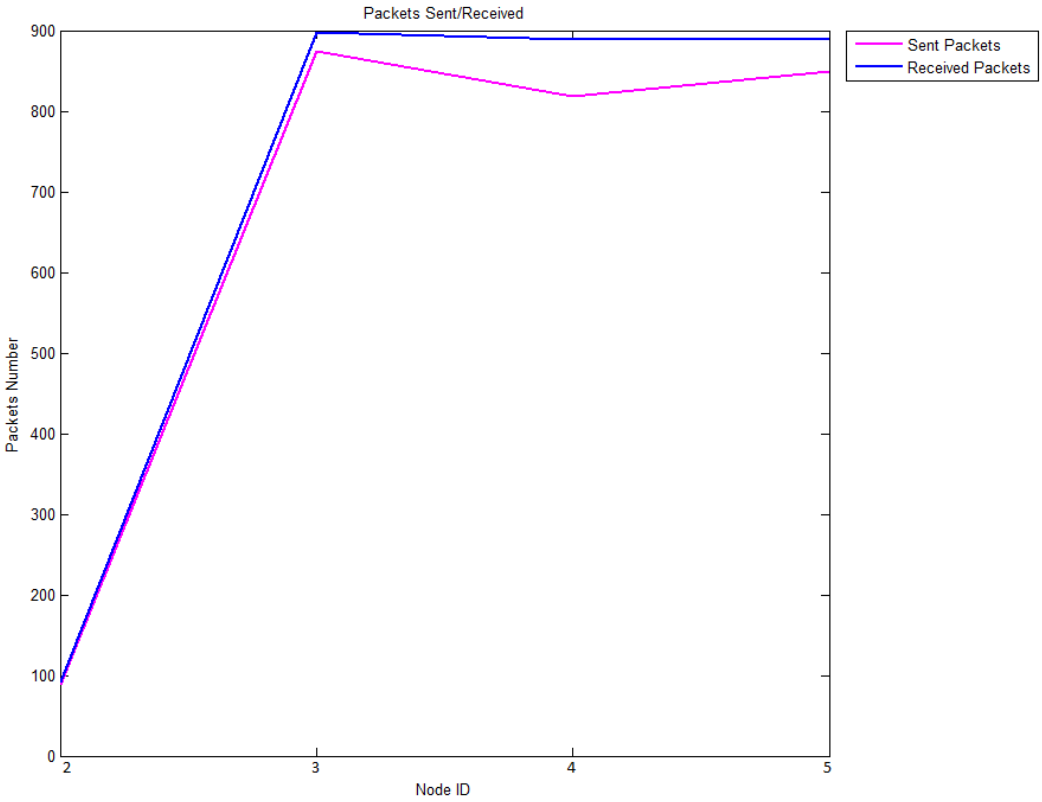
Σενάριο 1.2.3
3 Benign – 2 Malicious Nodes
Τοπολογία 1.1.3



Ο αριθμός των μολυσμένων κόμβων έχει αυξηθεί ακόμα περισσότερο. Συγκρίνοντας με τα προηγούμενα σενάρια φαίνεται πως υπάρχει μεγαλύτερος αριθμός πακέτων μέσα στο δίκτυο όμως σε αντίθεση με το unicast εδώ μαζί αυξάνεται και ο αριθμός των πακέτων που παραδίδονται στον κόμβο 1.

Φαίνεται πως ο αριθμός των πακέτων που λαμβάνονται είναι ανάλογος του αριθμού των πακέτων που στέλνονται. Αυτό εξηγείται στο προηγούμενο σενάριο όπου παρατηρείται το ίδιο φαινόμενο.

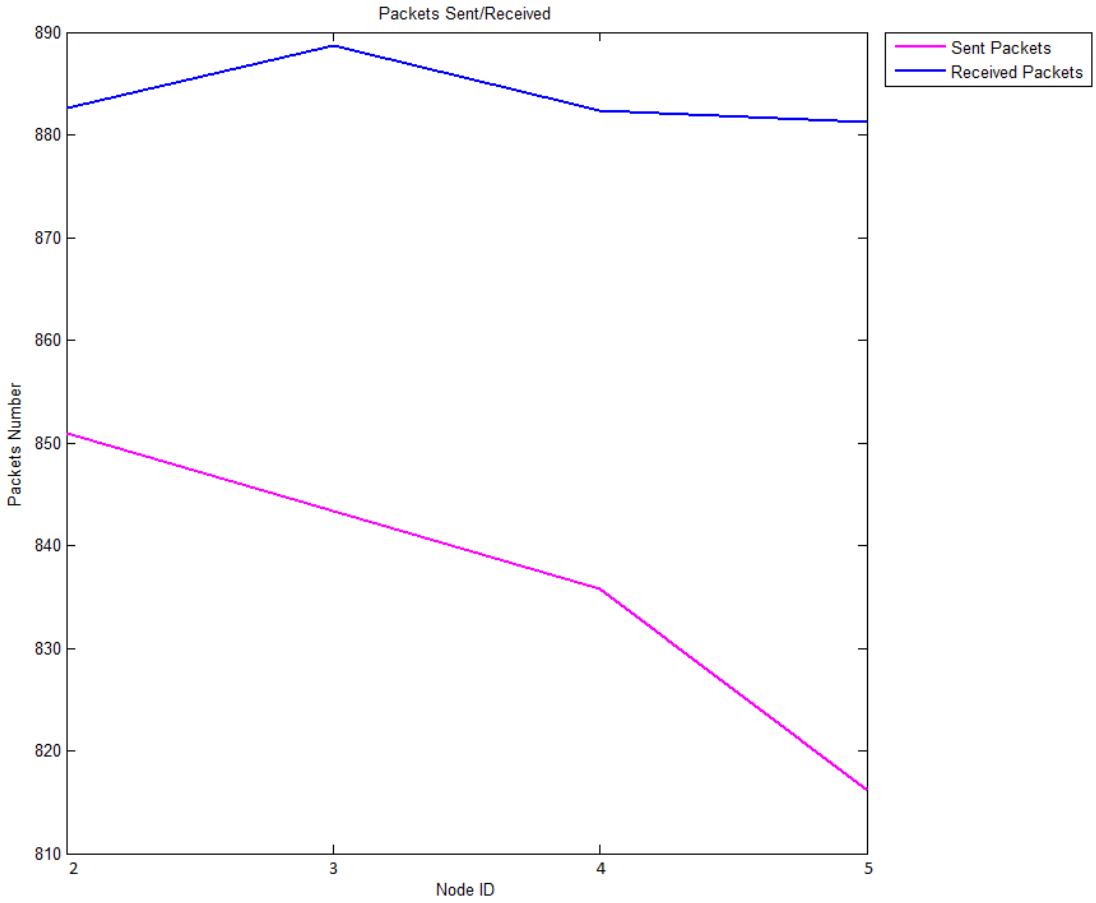
Σενάριο 1.2.4
2 Benign – 3 Malicious Nodes
Τοπολογία 1.1.4



Ισχύει το ίδιο όπως και με τις προηγούμενες περιπτώσεις στο runicast.
Ακόμα περισσότερα είναι τα πακέτα που στέλνονται στον κόμβο 1.

Τα πακέτα που παραλαμβάνει ο κόμβος 1 από τους υπόλοιπους κόμβους, είναι μεγαλύτερος από τον αριθμό των πακέτων που στέλνονται από κάθε κόμβο, και η διαφορά αυτή αυξάνεται σε κάθε σενάριο όπου οι κακόβουλοι κόμβοι αυξάνονται. Αυτό συμβαίνει για τον λόγο που εξηγήθηκε πιο πάνω. Όσο περισσότεροι είναι οι κακόβουλοι κόμβοι μέσα στο δίκτυο, τόσο περισσότερες συγκρούσεις γίνονται μεταξύ των πακέτων, άρα περισσότερα πακέτα φτάνουν αλλοιωμένα στον προορισμό τους οπότε γίνεται μια συνεχής αναμετάδοση τους.

Σενάριο 1.2.5
1 Benign – 4 Malicious Nodes
Τοπολογία 1.1.5



Αυτή είναι η περίπτωση όπου τώρα όλοι οι κόμβοι εκτός από τον παραλήπτη είναι "μολυσμένοι".

Σε αυτό το σενάριο φαίνεται πιο καθαρά ο τρόπος με τον οποίο λειτουργεί ο ιός Flooding χρησιμοποιώντας Runicast μετάδοση πακέτων.

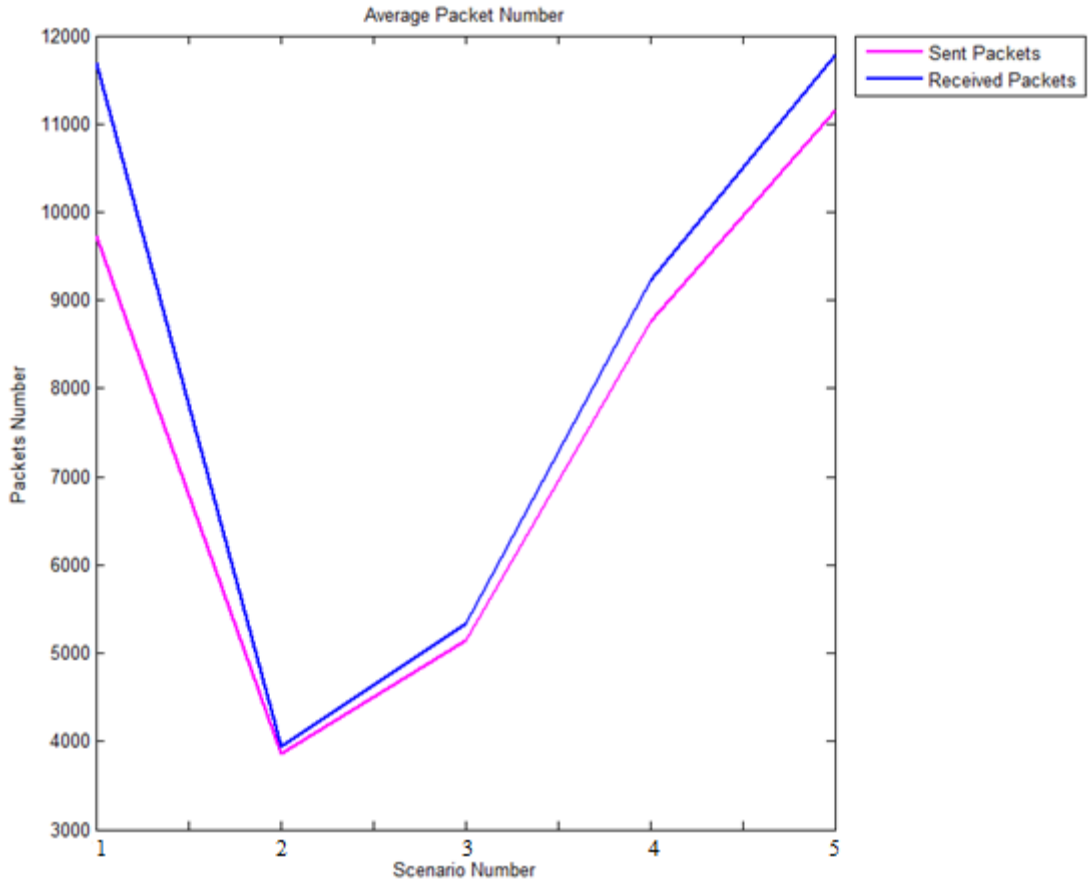
Γενικά Συμπεράσματα:

Παρατηρούμε πως στα πιο πάνω σενάρια που χρησιμοποιείται runicast δρομολόγηση, ο αριθμός των πακέτων που στέλνεται είναι αρκετά μικρότερος από τον αριθμό των πακέτων που λαμβάνει ο κόμβος 1 από τους υπόλοιπους κόμβους.
Αυτό συμβαίνει γιατί ο ρυθμός με τον οποίο οι υπόλοιποι κόμβοι που στέλνουν τα πακέτα τους είναι πολύ μεγαλύτερος από τον κανονικό ρυθμό με τον οποίο μπορεί να δεχτεί ο sink node.
Αφού λοιπόν δεν μπορεί να επεξεργαστεί τα πακέτα τα οποία φθάνουν τα κάνει drop και στην συνέχεια αναμεταδίδονται από τους κόμβους αυτά που χάθηκαν ή που καταστράφηκαν.

Ουσιαστικά η διαφορά του runicast είναι ακριβώς αυτή, ότι δηλαδή ξαναστέλνει τα πακέτα τα οποία δεν έφτασαν στον παραλήπτη.

Για την κάθε μία από τις πιο πάνω γραφικές παραστάσεις χρειάστηκαν δείγματα από 10 διαφορετικές μετρήσεις όπου κάθε φορά άλλαζε το seed όμως αριθμός των benign-malicious nodes έμενε σταθερός, όπως και η συχνότητα και η τοπολογία του δικτύου.

Στην συνέχεια γίνεται μια σύγκριση του αριθμού των πακέτων που προκύπτει από κάθε κόμβο, για κάθε δοκιμή.



Scenario Number	1	2	3	4	5
Scenario Name	5Benign – 0Malicious	4Benign – 1Malicious	3Benign – 2Malicious	2Benign – 3Malicious	1Benign – 4Malicious

Ο άξονας y αναπαριστά τον αριθμό των πακέτων και ο άξονας x αναπαριστά το σενάριο, τον αριθμό των benign-malicious nodes δηλαδή κάθε φορά.
Όπως παρατηρείται, στο σενάριο 2 (4benign-1malicious) ,ο αριθμός των πακέτων που στέλνονται πλησιάζει κατά πολύ τον αριθμό των πακέτων που λαμβάνονται όπου έχουμε και στις δύο περιπτώσεις τις μικρότερες τιμές από όλα τα σενάρια.

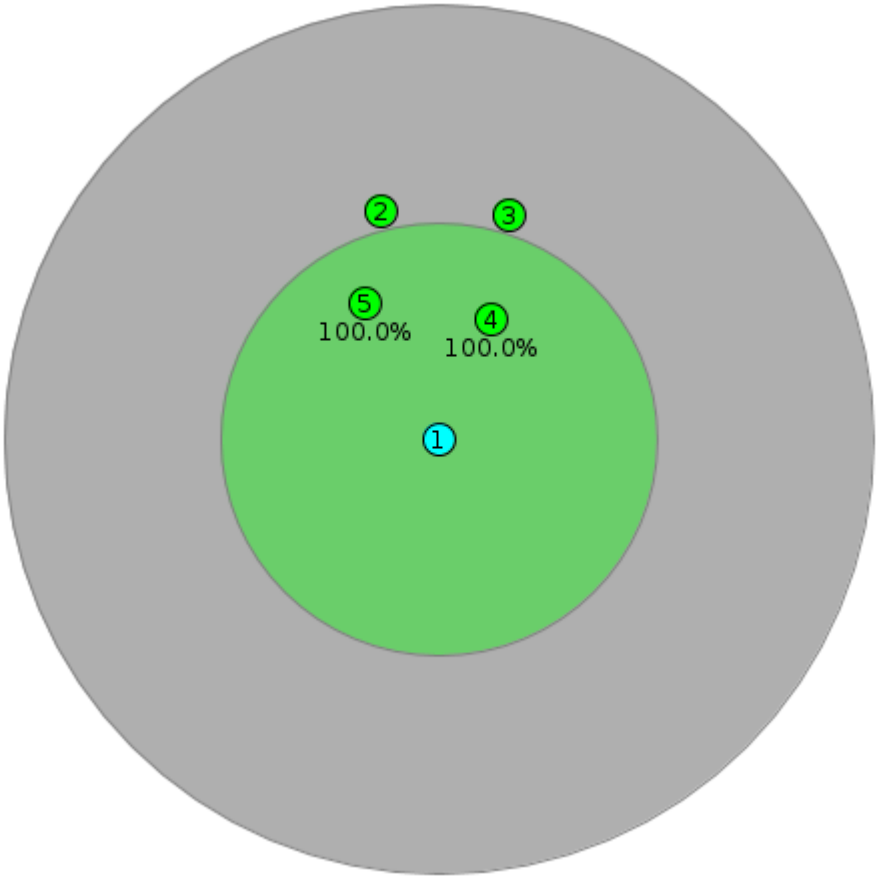
Η περίπτωση κατά την οποία έχουμε τον μέγιστο αριθμό sent και received packets είναι όταν ο αριθμός των malicious nodes είναι μέγιστος, δηλαδή 4.

5.1.3 Multihop

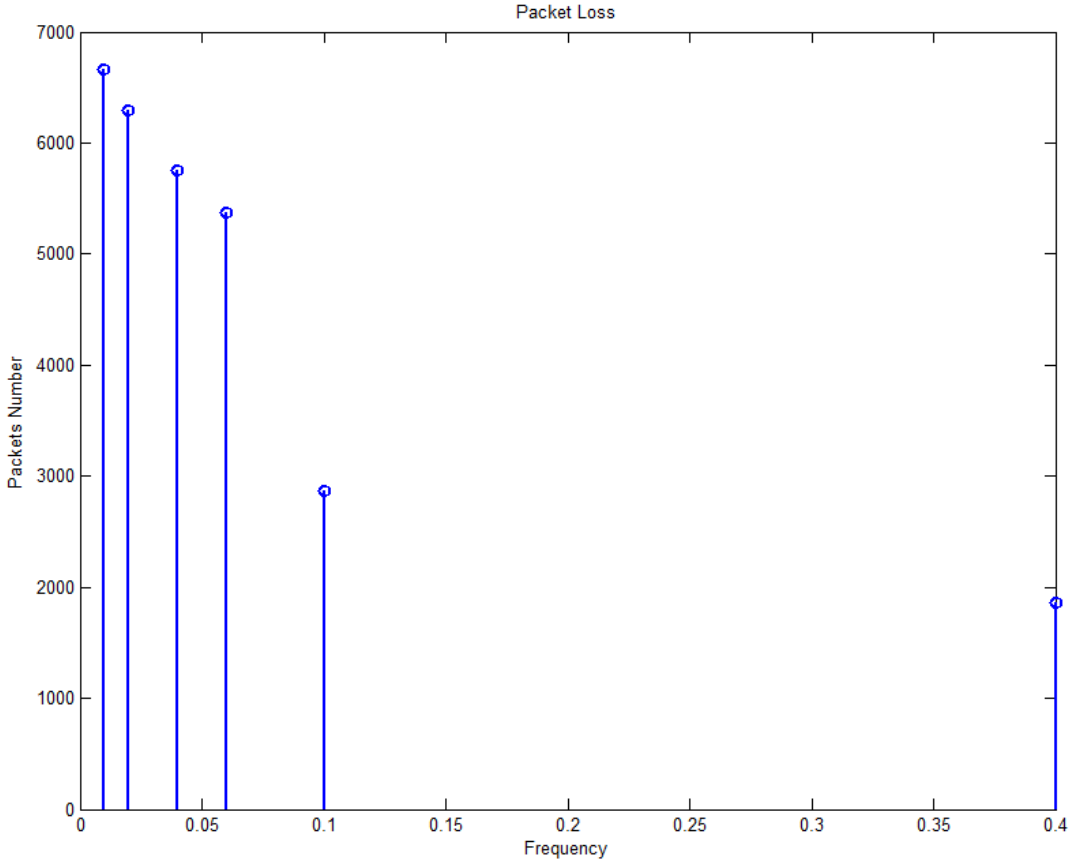
Στην πιο κάτω εικόνα φαίνεται η τοπολογία του δικτύου το οποίο χρησιμοποιείται για την λήψη των μετρήσεων, χρησιμοποιώντας multihop μετάδοση πακέτων.

Στην περίπτωση χρησιμοποιείται το multihop τότε πρέπει και το δίκτυο να έχει κόμβους οι οποίοι απέχουν από τον κόμβο 1, πάνω από 1 hop αλλιώς το δίκτυο δεν δουλεύει σωστά.

Σενάριο 1.3.1
5 Benign – 0 Malicious Nodes



Τοπολογία 1.3.1



Στον άξονα y παρουσιάζεται ο μέσος όρος του αριθμού των πακέτων που χάθηκαν και ο οποίος αντιστοιχεί σε κάθε μία από τις συχνότητες που βρίσκονται στον άξονα x. Για κάθε μία από τις συχνότητες που φαίνονται στην γραφική παράσταση έγιναν 3 προσομοιώσεις με διαφορετικό seed κάθε φορά.

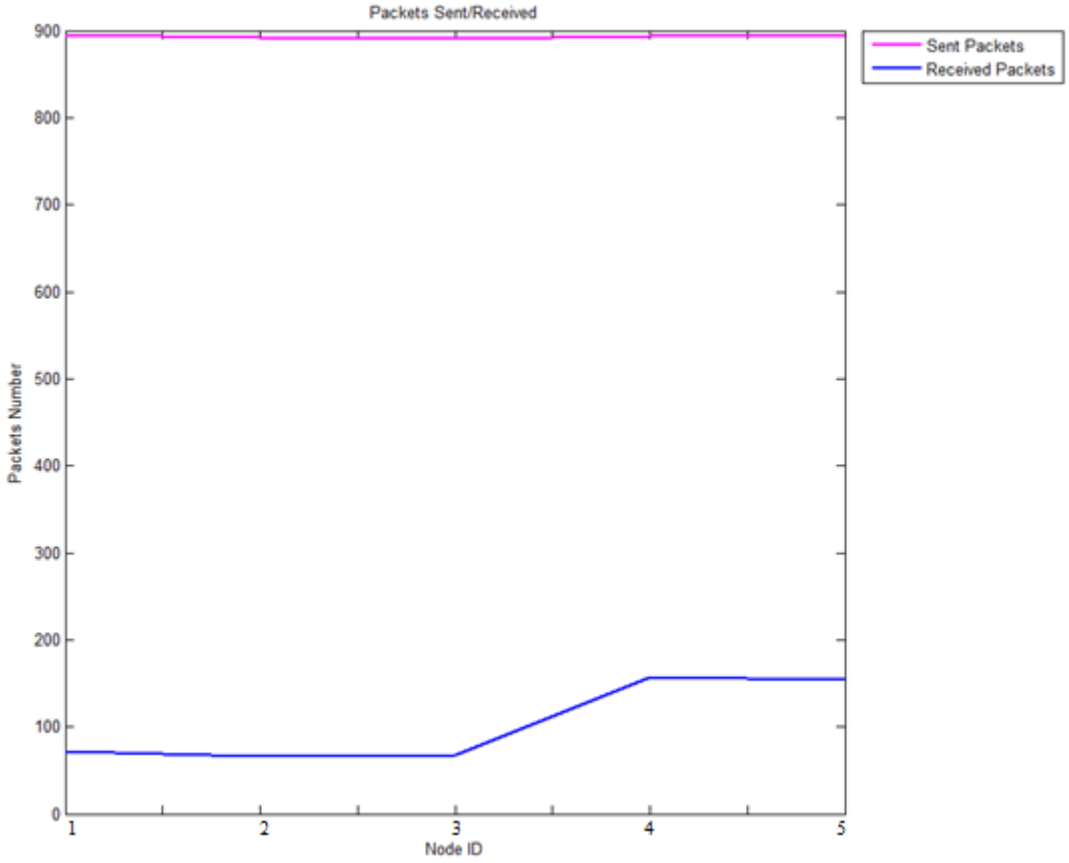
Όπως και στις προηγούμενες δύο περιπτώσεις, με τον ίδιο τρόπο επιλέγηκε και σε αυτή την περίπτωση η συχνότητα η οποία έδειχνε πιο ξεκάθαρα τις αλλαγές που προκαλούσαν οι κακόβουλοι κόμβοι στο δίκτυο. Επιλέγεται λοιπόν η συχνότητα 0.1 για τις υπόλοιπες μετρήσεις που λήφθηκαν.

Σενάρια

Σε όλα τα πιο κάτω σενάρια χρησιμοποιείται συχνότητα 0,1 και η τοπολογία του δικτύου παραμένει σταθερή.

Ο άξονας y αναπαριστά τον αριθμό των πακέτων που κινούνται μέσα στο δίκτυο και ο άξονας x δείχνει τον κόμβο στον οποίο αντιστοιχεί ο αριθμός των πακέτων που έστειλε ο κάθε κόμβος και που έλαβε από αυτόν ο παραλήπτης.
Σε κάθε μία από αυτές τις προσομοιώσεις αλλάζει μόνο το seed κάθε φορά.

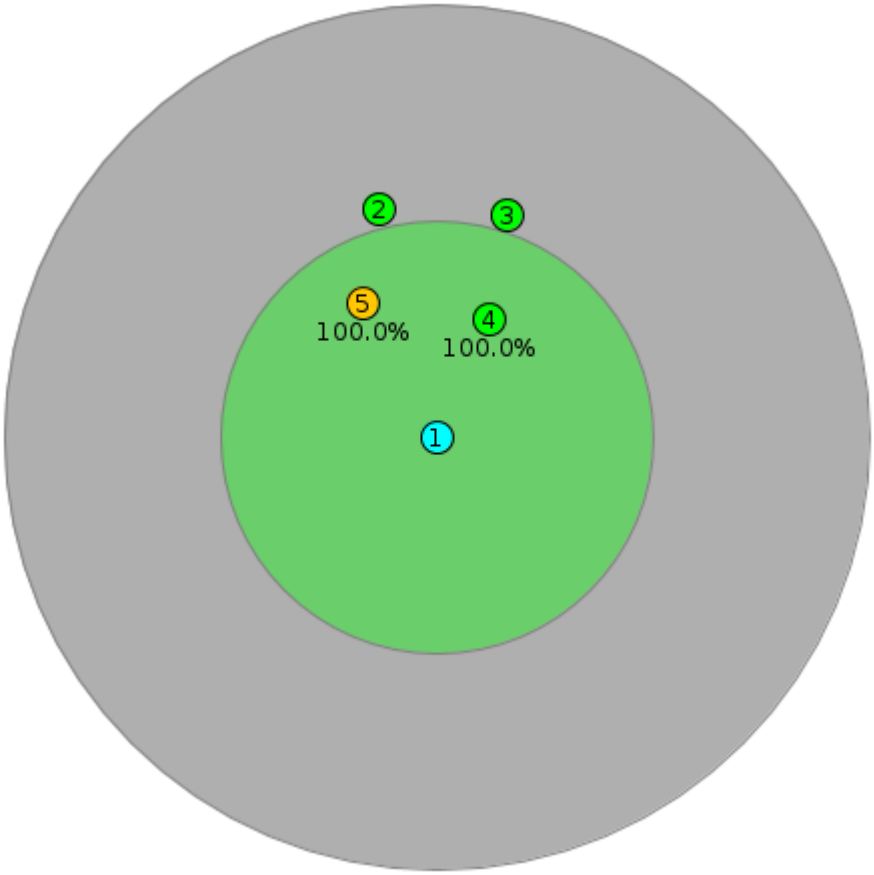
Σενάριο 1.3.1
5 Benign – 0 Malicious Nodes
Τοπολογία 1.3.1



Από το πιο πάνω σενάριο όπου έχουμε μόνο 5 κανονικούς κόμβους και καθόλου κακόβουλους , παρατηρούμε πως στέλνουν κατά προσέγγιση όλοι οι κόμβοι την ίδια ποσότητα πακέτων.

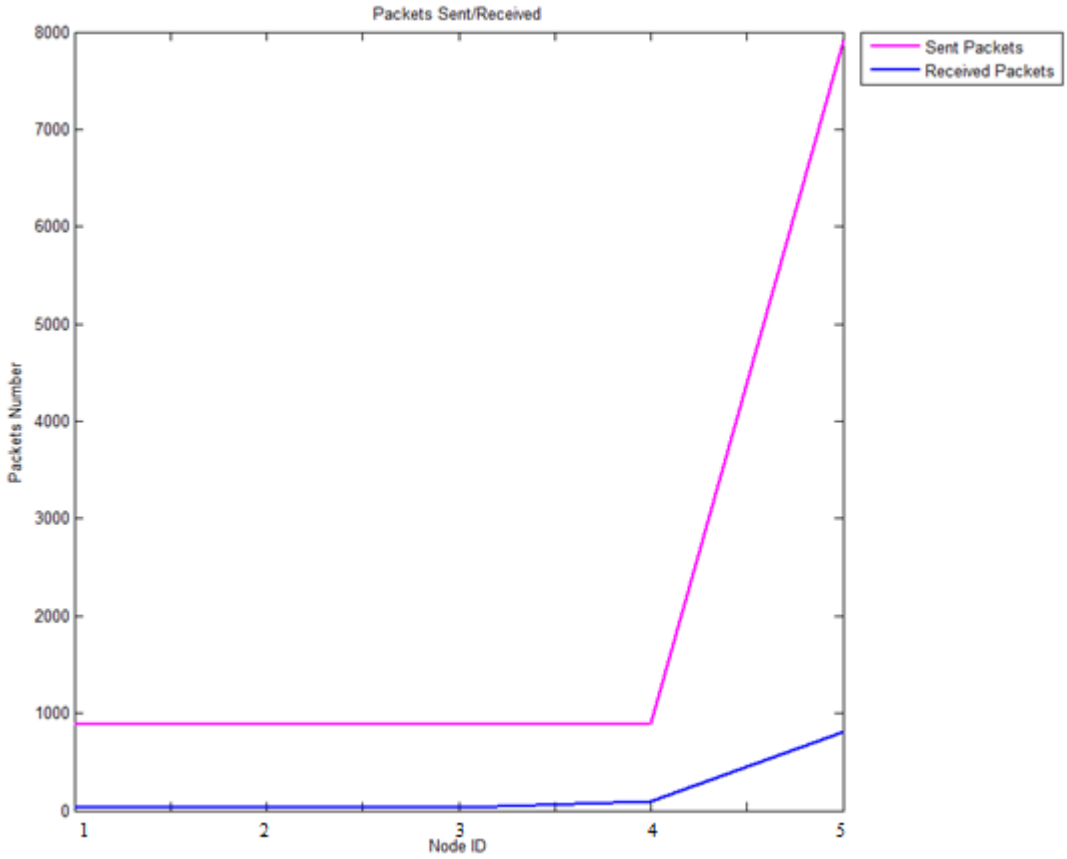
Αν και δεν υπάρχουν καθόλου κακόβουλοι κόμβοι, εντούτοις υπάρχει μεγάλη απώλεια πακέτων μέσα στο δίκτυο, κυρίως από τους κόμβους 2 και 3.
Για τους κόμβους 4 και 5 η απώλεια γίνεται σε πολύ μικρό βαθμό συγκριτικά με τους υπόλοιπους κόμβους.

Σενάριο 1.3.2
4 Benign – 1 Malicious Nodes



Τοπολογία 1.3.2

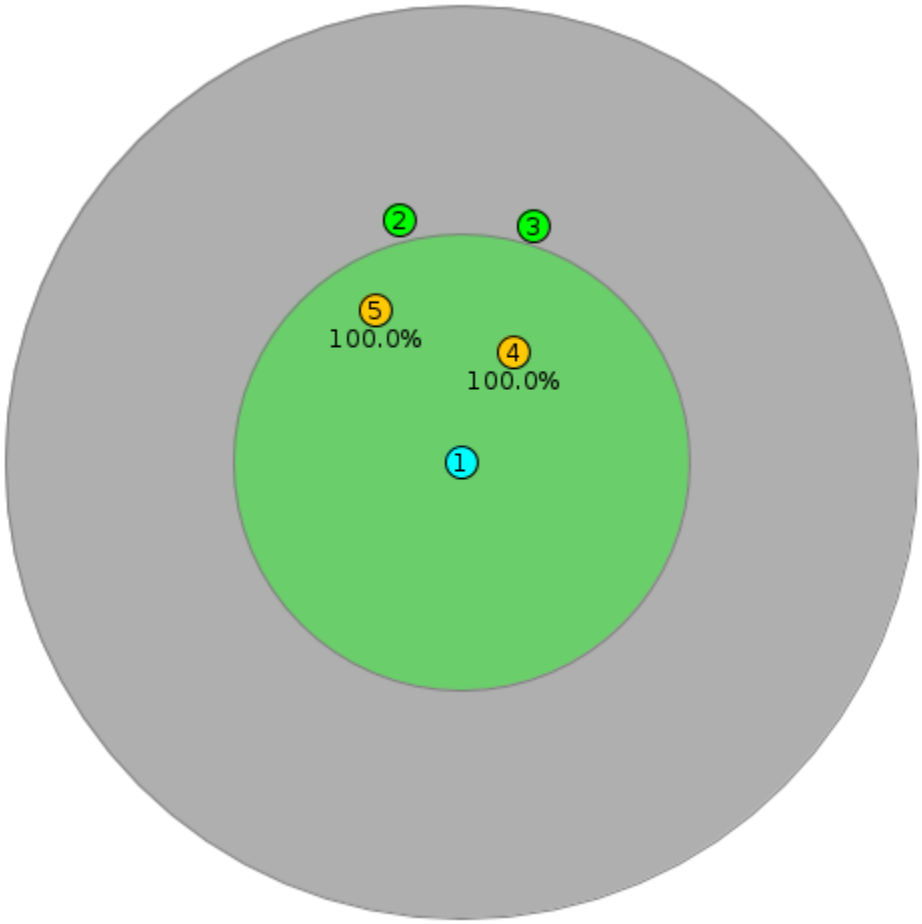
Σενάριο 1.3.2
4 Benign – 1 Malicious Nodes
Τοπολογία 1.3.2



Σε αυτή την γραφική παράσταση παρατηρείται ακόμα μεγαλύτερη απώλεια πακέτων από όλους τους κόμβους.

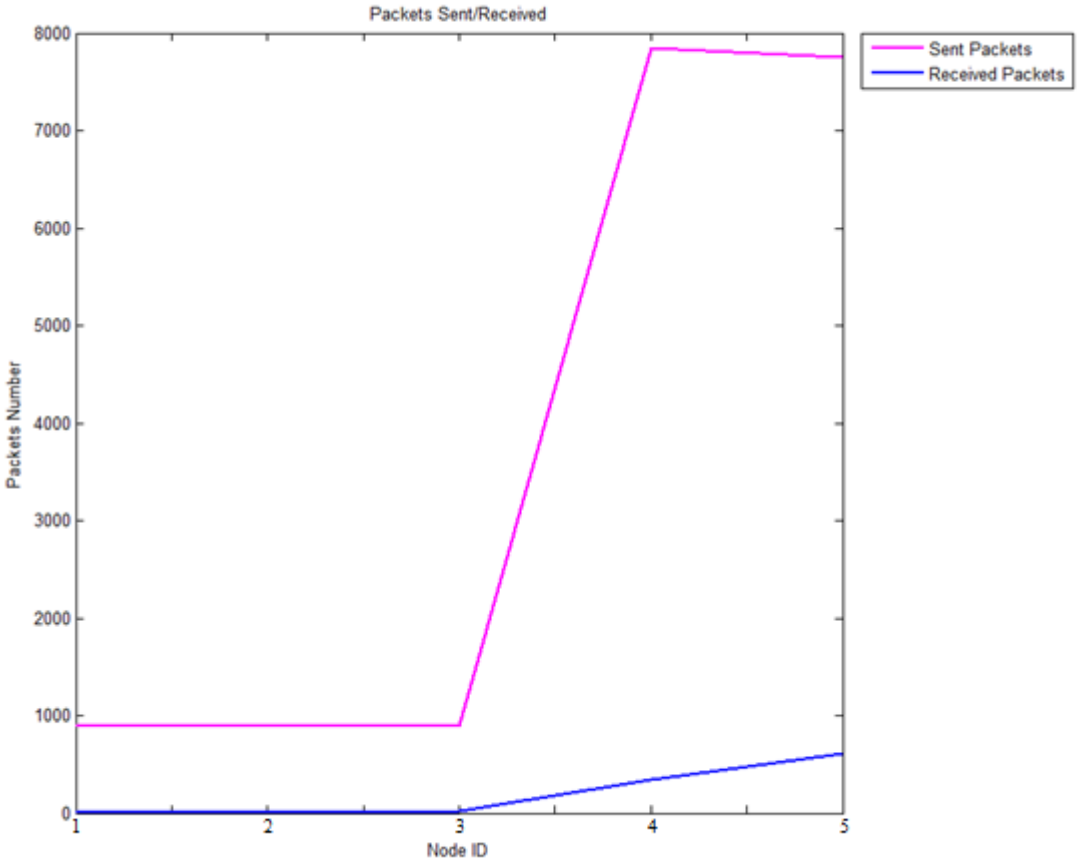
Συγκρίνοντας τα πακέτα που λαμβάνει ο κόμβος 1 από τους 2,3 και 4, αντιλαμβανόμαστε πως ο αριθμός τους έχει μειωθεί αρκετά, παρόλο που είναι "υγιείς" κόμβοι.
Γενικότερα όμως, ολόκληρο το δίκτυο επηρεάζεται με την παρουσία ενός και μόνο κακόβουλου κόμβου, οπότε απώλειες πακέτων οφείλονται και σε αυτό το γεγονός.

Σενάριο 1.3.3
3 Benign – 2 Malicious Nodes



Τοπολογία 1.3.3

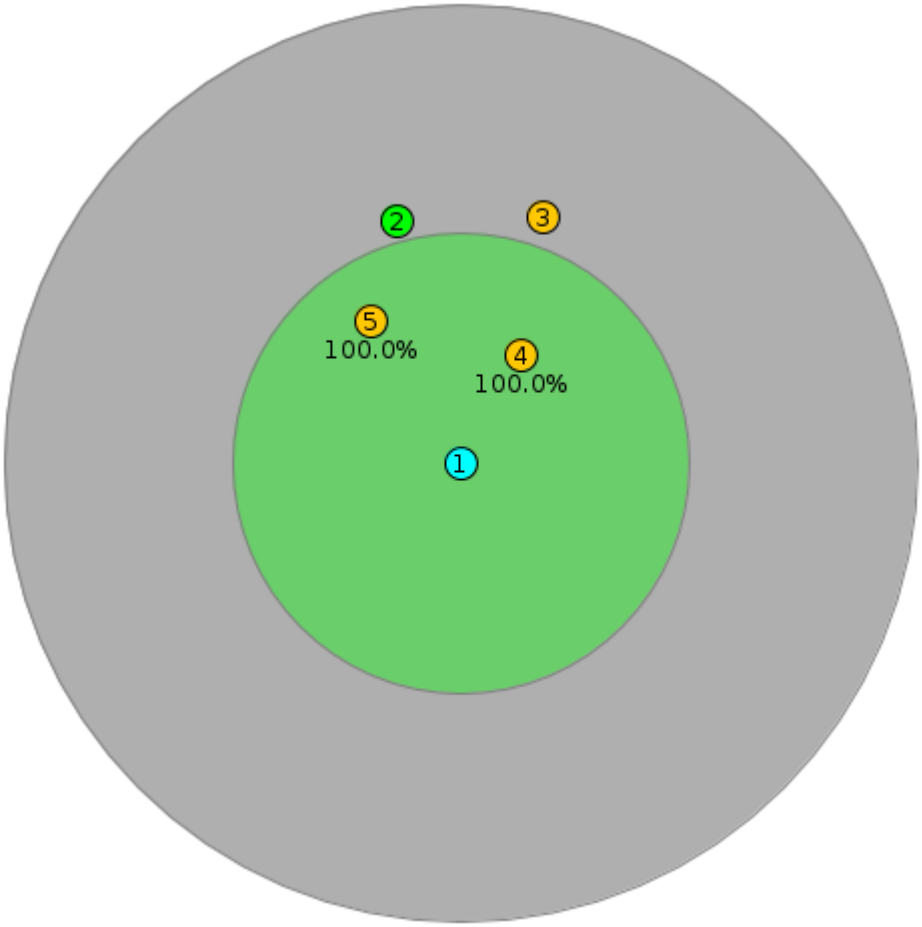
Σενάριο 1.3.3
3 Benign – 2 Malicious Nodes
Τοπολογία 1.3.3



Το ίδιο παρατηρείται και σε αυτή την γραφική παράσταση, όπως και στην προηγούμενη. Τώρα οι κακόβουλοι κόμβοι είναι 2 και στέλνουν παραπλήσιο αριθμό πακέτων. Ο αριθμός των πακέτων που χάνεται είναι ακόμα μεγαλύτερος , τόσο για τους υγιείς όσο και για τους κακόβουλους
Βέβαια λόγω του ότι οι μολυσμένοι στέλνουν μια κατά πολύ μεγαλύτερη ποσότητα πακέτων, καταφέρνουν όντως να παραδώσουν μια σχετικά μεγαλύτερη ποσότητα πακέτων, σε σχέση με τους υπόλοιπους κόμβους, στον τελικό παραλήπτη, ενώ παρουσιάζουν μια πολύ μεγάλου βαθμού απώλεια πακέτων.

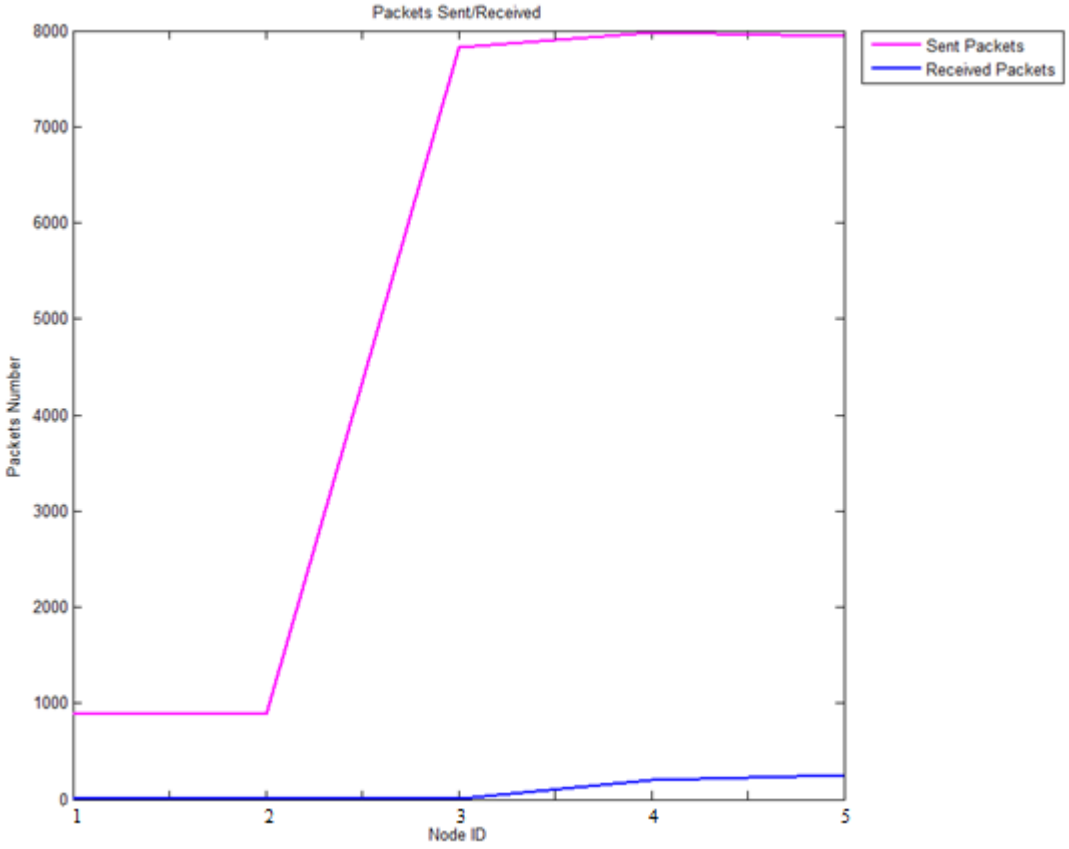
Όσο αυξάνουμε τον αριθμό των "μολυσμένων κόμβων", τα πακέτα που θα λαμβάνονται από τους κανονικούς κόμβους θα μειώνονται συνεχώς πλησιάζοντας το 0.

Σενάριο 1.3.4
2 Benign – 3 Malicious Nodes



Τοπολογία 1.3.4

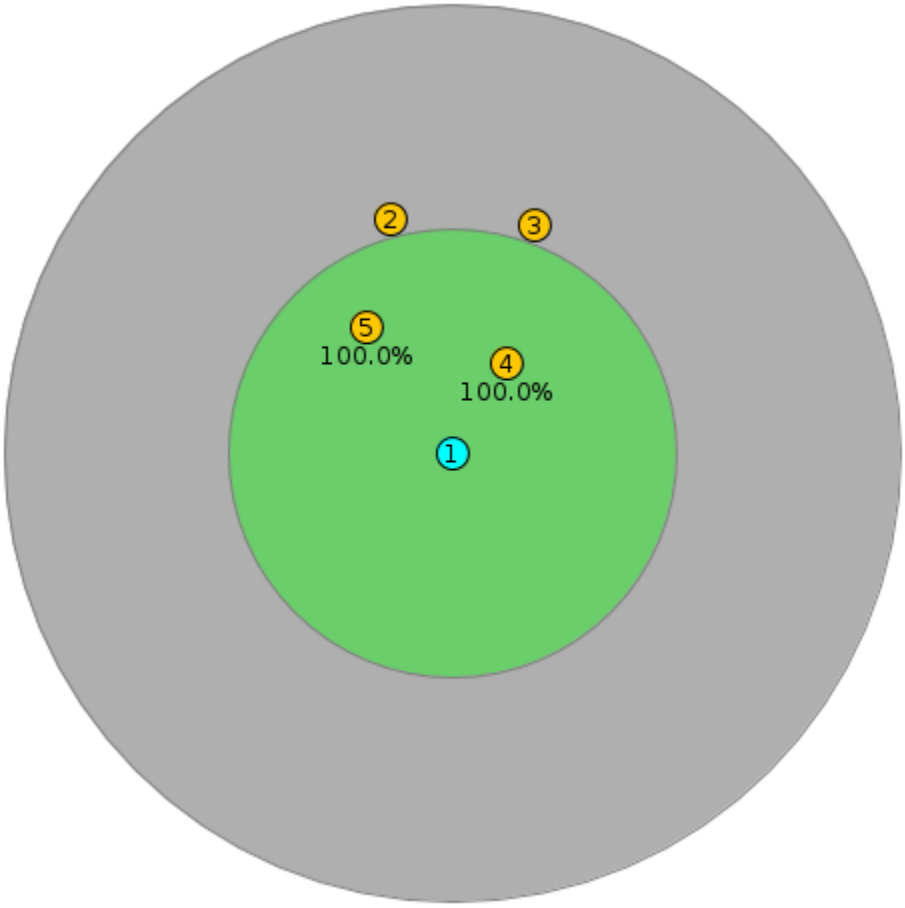
Σενάριο 1.3.4
2 Benign – 3 Malicious Nodes
Τοπολογία 1.3.4



Παρατηρώντας την πιο πάνω γραφική παράσταση μπορούμε να καταλάβουμε ό,τι και στην πιο πάνω, ότι δηλαδή σε κάποιες δοκιμές κανένα από τα πακέτα που έστελνε κάποιος συγκεκριμένος κόμβος, δεν έφτασαν ποτέ στον παραλήπτη τους.

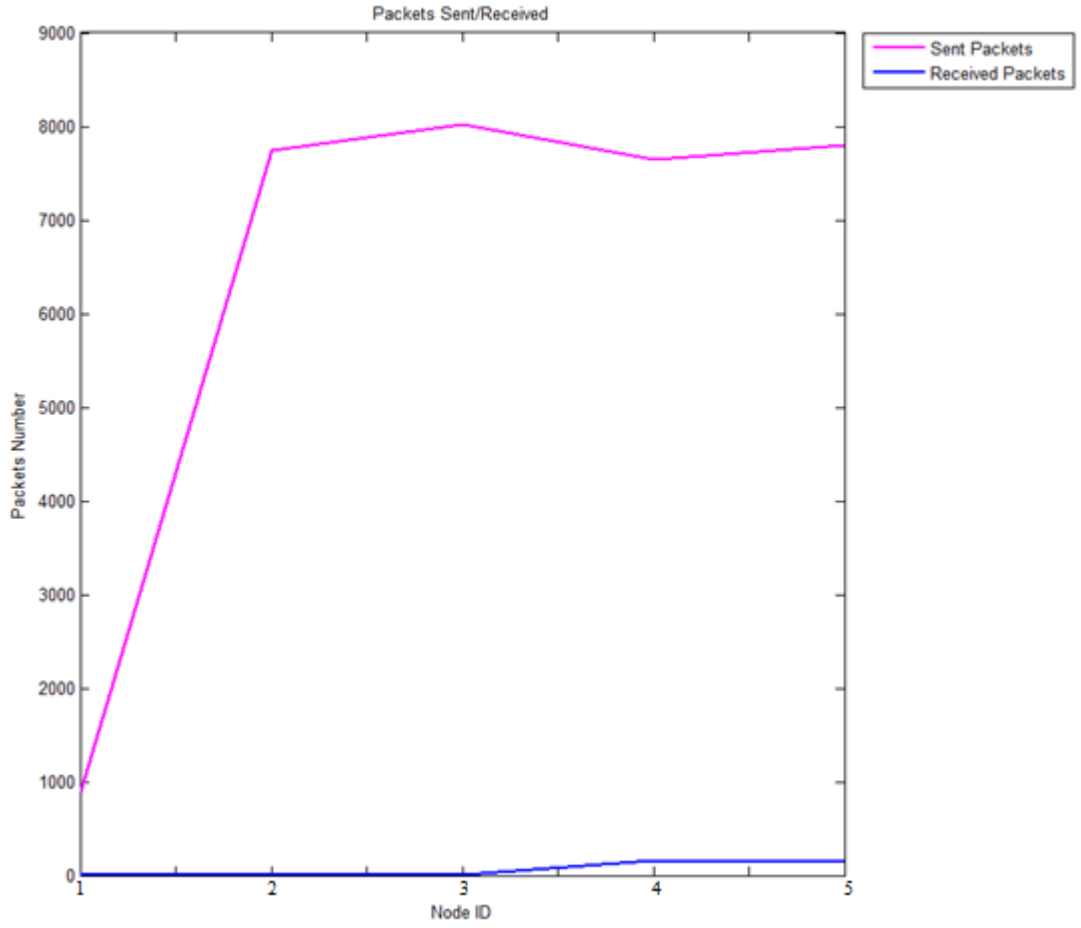
Σίγουρα ο συνολικός αριθμός των πακέτων που στέλνονται μέσα στο δίκτυο είναι ακόμα μεγαλύτερος από τα προηγούμενα σενάρια, ενώ ο αριθμός των πακέτων που καταστρέφονται ή χάνονται είναι κατά πολύ μικρότερος από τον αριθμό των πακέτων που φτάνουν στο κόμβο 1, στα υπόλοιπα σενάρια.

Σενάριο 1.3.5
1 Benign – 4 Malicious Nodes



Τοπολογία 1.3.5

Σενάριο 1.3.5
1 Benign – 4 Malicious Nodes
Τοπολογία 1.3.5



Ο κακόβουλοι κόμβοι τώρα είναι 4 και ο μοναδικός κόμβος που δεν έχει “μολυνθεί ” είναι πλέον ο παραλήπτης όλων των πακέτων.

Ο κόμβος 1 λαμβάνει ένα πολύ μικρό αριθμό από πακέτα τους οποίους ο μέσος όρος πλησιάζει είναι πολύ πιο χαμηλός, κάτι που ήταν βέβαια αναμενόμενο.

Γενικώς παρατηρείται ό,τι και στην προηγούμενη γραφική παράσταση.

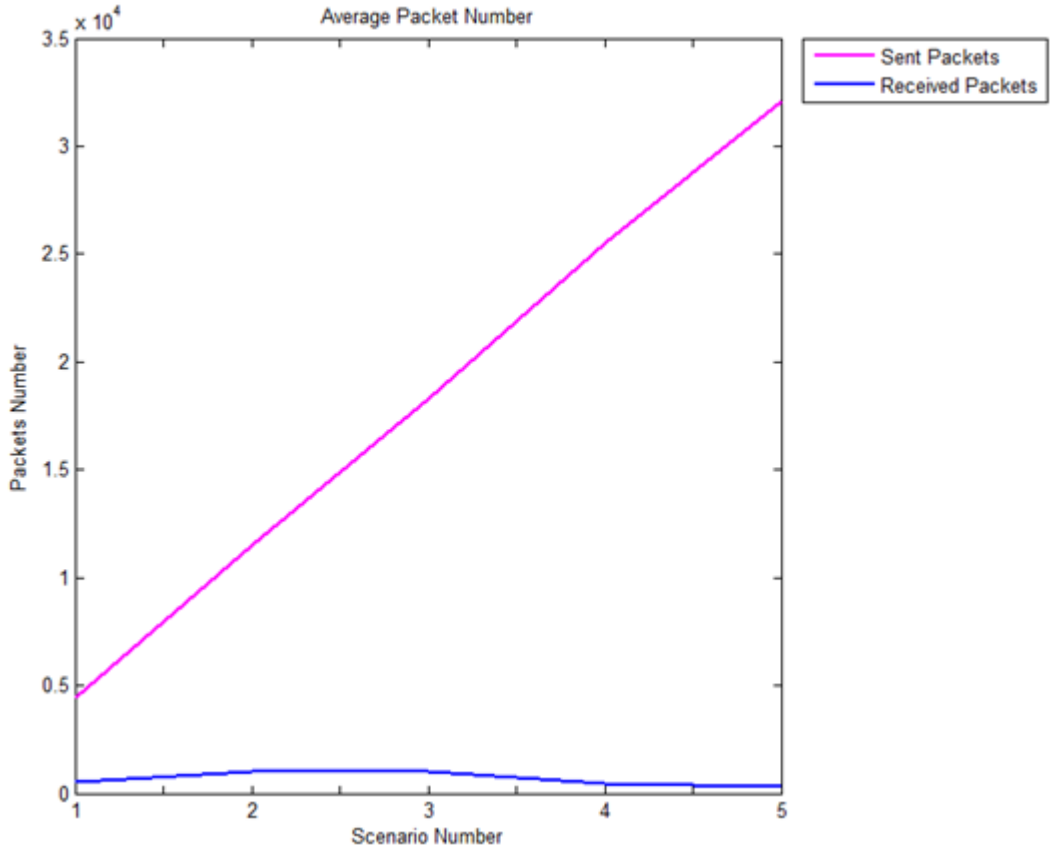
Γενικά συμπεράσματα:

Στην περίπτωση του multihop παρατηρούμε από τις γραφικές πως ο τελικός παραλήπτης λαμβάνει περισσότερα πακέτα από κόμβους οι οποίοι βρίσκονται μέσα στην εμβέλεια του.
Όσα περισσότερα hops δηλαδή μπορεί να διανύσει ένα πακέτο για να φτάσει στον προορισμό του, τόσο πιο πολλές είναι οι πιθανότητες να χαθούν περισσότερα πακέτα σε συνδυασμό με τους malicious nodes οι οποίοι πλημμυρίζουν το δίκτυο με πακέτα.

Οι κόμβοι 4,5 δηλαδή οι οποίοι βρίσκονται μέσα στην εμβέλεια του 1, μπορούν να παραδώσουν τα πακέτα τους απευθείας σε αυτόν μειώνοντας έτσι τις πιθανότητες αυτά να χαθούν. Γι' αυτό και στις περιπτώσεις όπου τόσο οι ίδιοι όσο και κάποιοι άλλοι κόμβοι μέσα στο δίκτυο είναι Malicious, τα πακέτα που λαμβάνονται από αυτούς είναι περισσότερα.

Για να λειτουργήσει το multihop προϋποθέτει ότι υπάρχουν κόμβοι οι οποίοι απέχουν κάποιο αριθμό hops από τον τελικό παραλήπτη.

Όσο περισσότεροι είναι οι κακόβουλοι κόμβοι μέσα στο δίκτυο τόσο πιο πολλά πακέτα πρέπει να επεξεργαστεί ο παραλήπτης οπότε αυξάνονται οι πιθανότητες να χαθούν περισσότερα πακέτα από τον κάθε κόμβο.



Scenario Number	1	2	3	4	5
Scenario Name	5Benign – 0Malicious	4Benign – 1Malicious	3Benign – 2Malicious	2Benign – 3Malicious	1Benign – 4Malicious

Αυτό που φαίνεται από την πιο πάνω γραφική παράσταση είναι πως όσο αυξάνεται ο αριθμός των malicious nodes, τόσο αυξάνεται και ο αριθμός των πακέτων που στέλνονται.

Όσο αφορά τον αριθμό των πακέτων που μπορεί να λάβει ο κόμβος 1, αυτός περιορίζεται σε ένα μικρό σχετικά πεδίο τιμών.

Φαινομενικά ο αριθμός των sent packets αυξάνεται εκθετικά, όπως είδαμε πως συμβαίνει και με τον αριθμό των πακέτων που χάνονται μέσα στο δίκτυο, ενώ ο αριθμός των received παραμένει σχεδόν σταθερός.

5.2 Selective Forwarding Attack

5.2.1 Selective Forwarding Source

Σε αυτό τον ιό, αυτό που κάνει ο κακόβουλος κόμβος είναι να αποκλείει κάποια πακέτα τα οποία φτάνουν από κάποιους συγκεκριμένους κόμβους. Δηλαδή, ένας μολυσμένος κόμβος, έχει την δυνατότητα να καταστρέφει όσα πακέτα φτάνουν από κόμβους οι οποίοι τον χρησιμοποιούν σαν ενδιάμεσο κόμβο, προκειμένου να στείλουν τα πακέτα τους στον προορισμό τους.
Συγκεκριμένα, επιλέγεται για κάποιο χρονικό διάστημα, ένας διαφορετικός κόμβος-παιδί του κακόβουλου κόμβου, του οποίου τα πακέτα θα καταστρέφονται με το που φτάνουν στον μολυσμένο. Γίνεται μια εναλλαγή μεταξύ των κόμβων, έτσι ώστε να μπλοκάρεται διαφορετικό παιδί, για κάποιο χρονικό διάστημα, μέχρι να υπάρχουν απώλειες πακέτων από όλους τους κόμβους.

Κάθε φορά που προωθούνται πακέτα τα οποία φτάνουν από ένα από τα παιδιά του, κάθε άλλο πακέτο που φτάνει από οποιονδήποτε άλλο κόμβο παιδί καταστρέφεται. Δηλαδή για κάποιο χρονικό διάστημα προωθούνται πακέτα τα οποία φτάνουν μόνο από ένα κόμβο παιδί.

Σενάρια

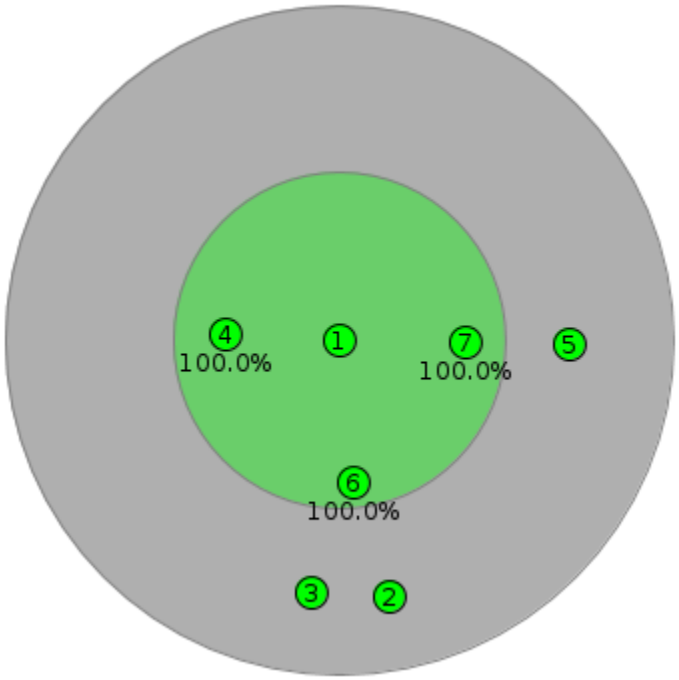
Στις πιο κάτω μετρήσεις που λήφθηκαν, χρειάστηκε να δημιουργηθούν δύο διαφορετικές τοπολογίες, προκειμένου να φαίνονται πιο ξεκάθαρα τα αποτελέσματα και να προκύψουν πιο ορθά συμπεράσματα.

Στην πρώτη τοπολογία, αναπαρίσταται ένα δίκτυο με 7 κόμβους, ενώ στην δεύτερη τοπολογία, παρουσιάζεται ένα δίκτυο με 12 κόμβους.

Για κάθε μία από τις δύο τοπολογίες, δημιουργήθηκαν κάποια σενάρια, τα οποία διέφεραν ως προς τον αριθμό των κακόβουλων κόμβων. Για κάθε ένα από αυτά τα σενάρια, έγιναν 10 προσομοιώσεις, κατά τις οποίες κάθε φορά άλλαζε ο κόμβος από τον οποίο άρχιζε η μετάδοση των πακέτων, είχαν δηλαδή, διαφορετικό seed μεταξύ τους. Με αυτό τον τρόπο φαίνεται καλύτερα πώς αντιδρά το δίκτυο σε πολλές και διαφορετικές περιπτώσεις.

Ο άξονας y αναπαριστά τον αριθμό των πακέτων που κινούνται μέσα στο δίκτυο και ο άξονας x δείχνει τον αριθμό της προσομοίωσης για το συγκεκριμένο σενάριο.

Σενάριο 2.1.1.1
7 Benign – 0 Malicious Nodes



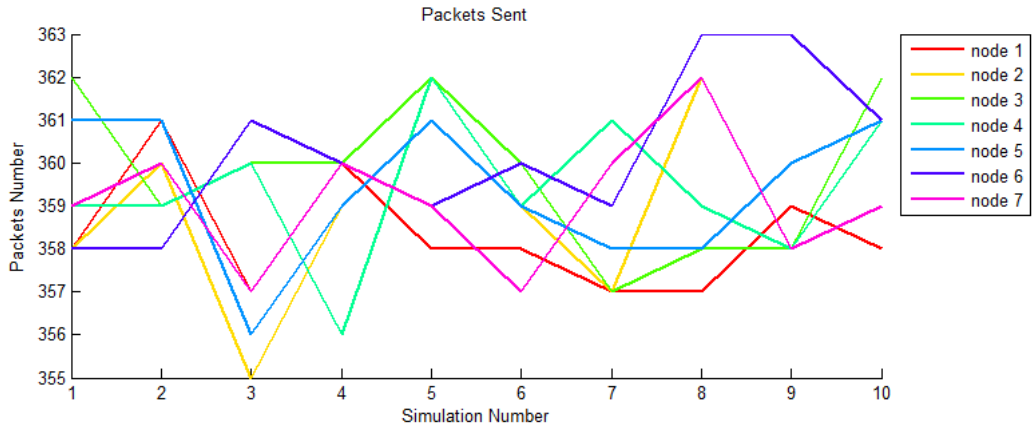
Τοπολογία 2.1.1.1

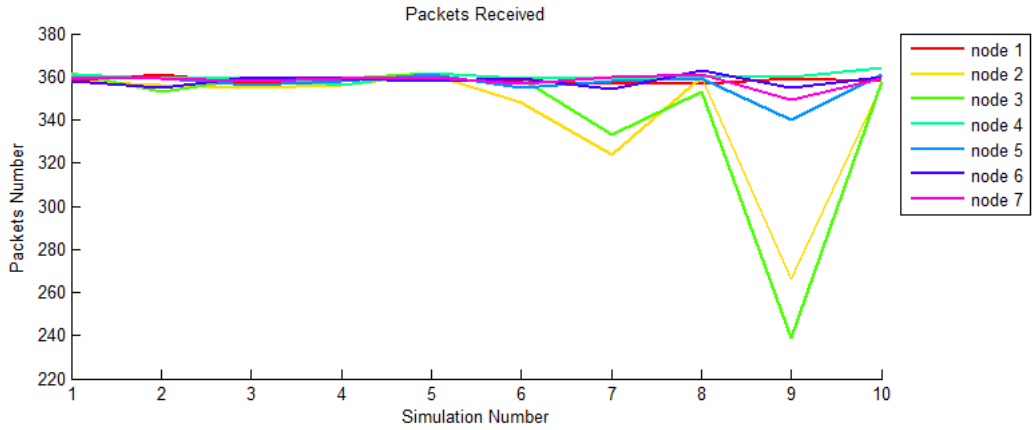
Στην πιο πάνω εικόνα παρουσιάζεται η τοπολογία του δικτύου που χρησιμοποιείται για την λήψη διαφόρων μετρήσεων, έτσι ώστε να φανεί κατά πόσο ένας ιός Selective Forwarding θα μπορούσε να επηρεάσει μια τέτοια διάταξη των κόμβων μέσα σε ένα ασύρματο δίκτυο αισθητήρων.

Εδώ παρουσιάζεται το baseline scenario, όπου ουσιαστικά είναι ένα δίκτυο το οποίο αποτελείται μόνο από ‘υγιείς’ κόμβους, και το οποίο θα χρησιμοποιηθεί στην συνέχεια για σύγκριση των αποτελεσμάτων που θα προκύψουν, με την παρεμβολή κακόβουλου κώδικα.

Για να δουλέψει σωστά ο ιός, απαιτείται multi hop μετάδοση πακέτων, δηλαδή οι κόμβοι που πρόκειται να επηρεαστούν αρνητικά από κάποιο κακόβουλο κόμβο, δεν πρέπει να είναι μέσα στην εμβέλεια του κόμβου 1, προκειμένου να αναγκάζονται να χρησιμοποιήσουν σαν ενδιάμεσο κόμβο για την αποστολή των πακέτων τους, τον κακόβουλο κόμβο. Με αυτό τον τρόπο ο ‘μολυσμένος’ κόμβος, έχει την δυνατότητα να καταστρέψει όσα πακέτα θέλει προερχόμενα από τους κόμβους-παιδιά του.

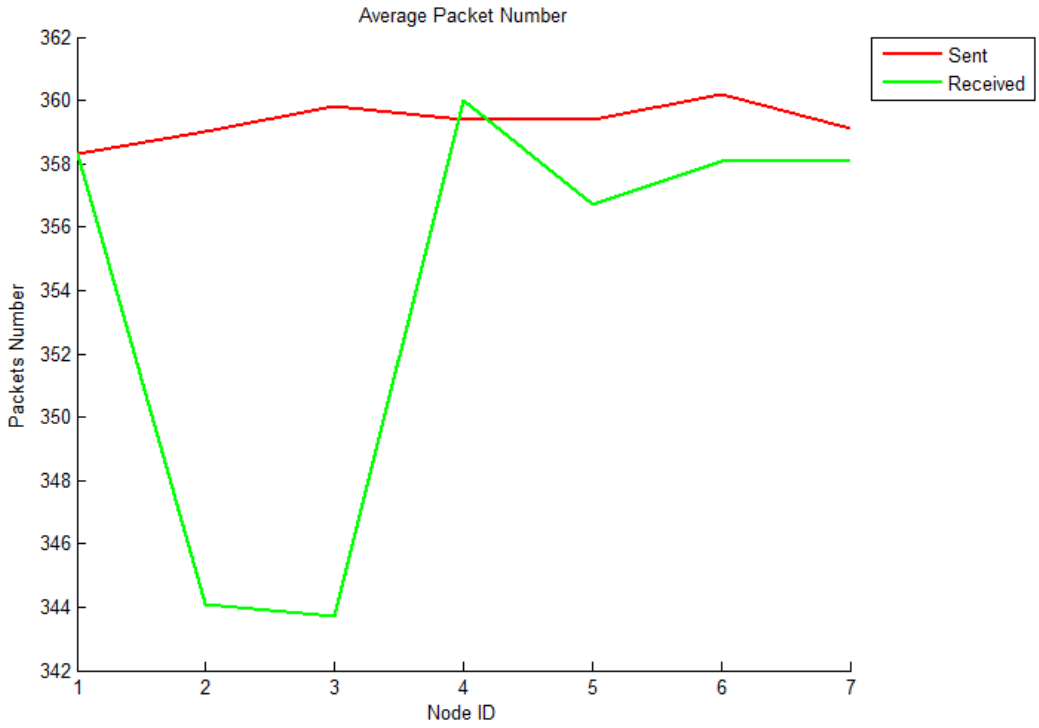
Σενάριο 2.1.1.1
7 Benign – 0 Malicious Nodes
Τοπολογία 2.1.1.1





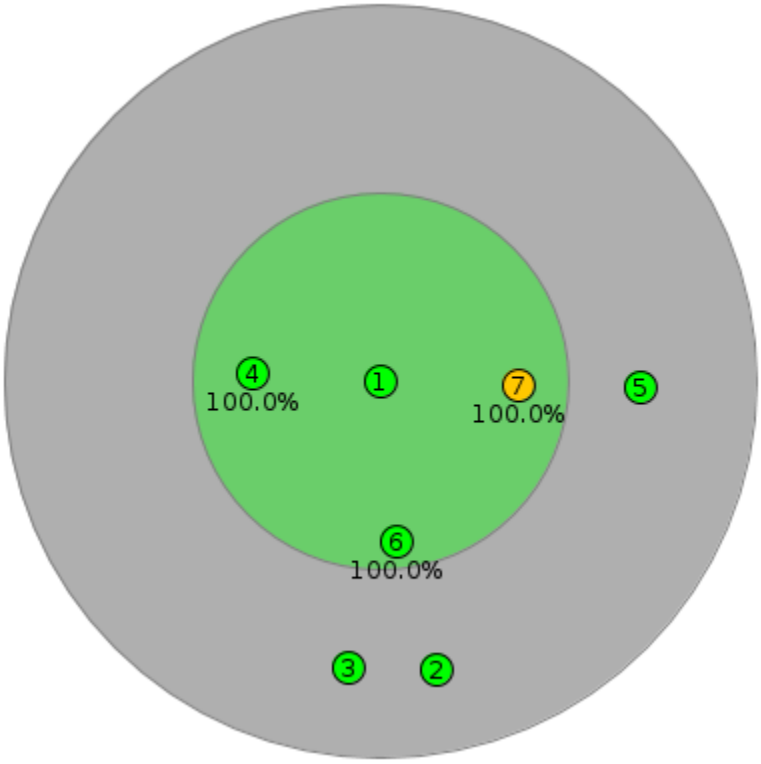
Από την γραφική αυτή παράσταση, φαίνεται πως στην πρώτη περίπτωση, όπου παρουσιάζεται ο αριθμός των πακέτων που στέλνει κάθε ένας από τους κόμβους μέσα στο δίκτυο, είναι περίπου ο ίδιος για όλους.

Στην δεύτερη γραφική παράσταση, παρατηρείται πως αριθμός των πακέτων δεν επηρεάζεται, παραμένει περίπου ο ίδιος με τον αρχικό αριθμό των πακέτων που στάλθηκαν, για κάθε κόμβο. Παρατηρείται μια μικρή απόκλιση, η οποία δεν λαμβάνεται υπόψη, αφού οφείλεται σε ανωμαλίες του δικτύου.



Αυτό είναι το Baseline Scenario, κατά το οποίο φαίνεται ο αριθμός των πακέτων που στέλνει ο κάθε κόμβος μέσα στο δίκτυο και έχει ως τελικό παραλήπτη τον κόμβο 1, όπως και π αριθμός των πακέτων που λαμβάνει ο κόμβος 1 από κάθε ένα από τους υπόλοιπους κόμβους του δικτύου.
Παρατηρείται ότι τα πακέτα που στέλνει ο κάθε κόμβος είναι όσα και τα πακέτα που παραλαμβάνει ο τελικός κόμβος από τον καθένα, με ίσως κάποια μικρή απόκλιση.

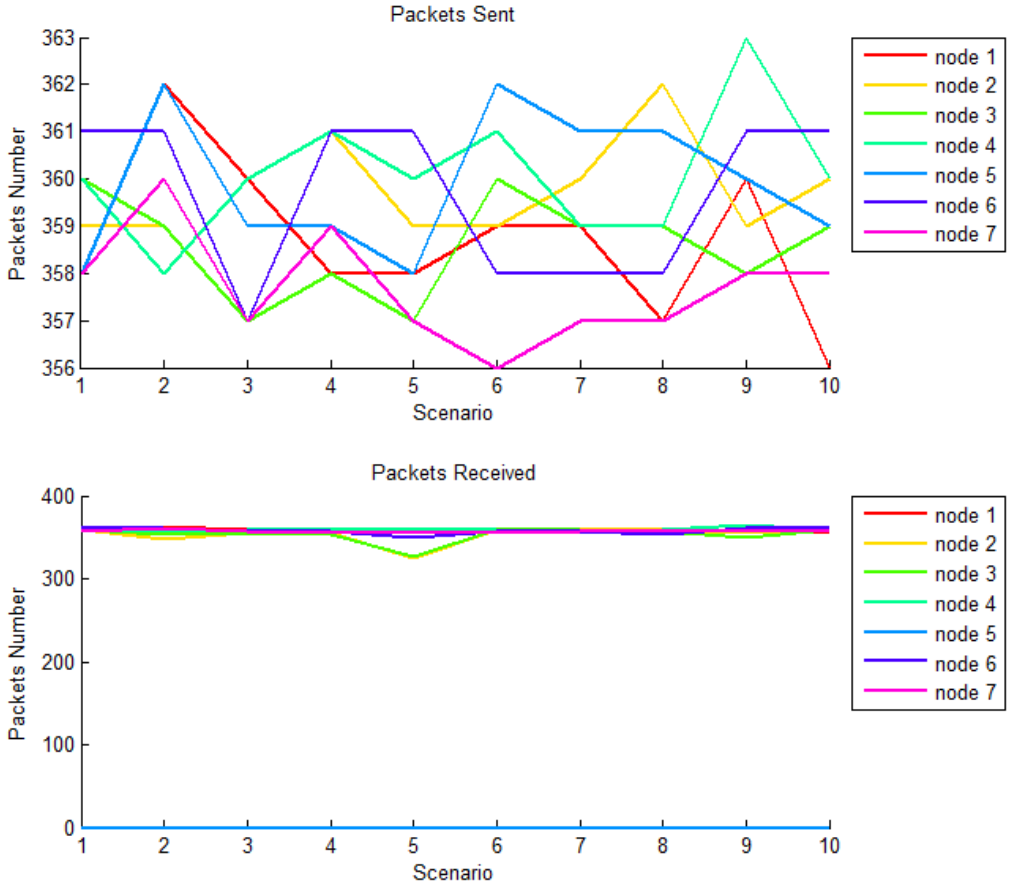
Σενάριο 2.1.1.2
6 Benign – 1 Malicious Nodes



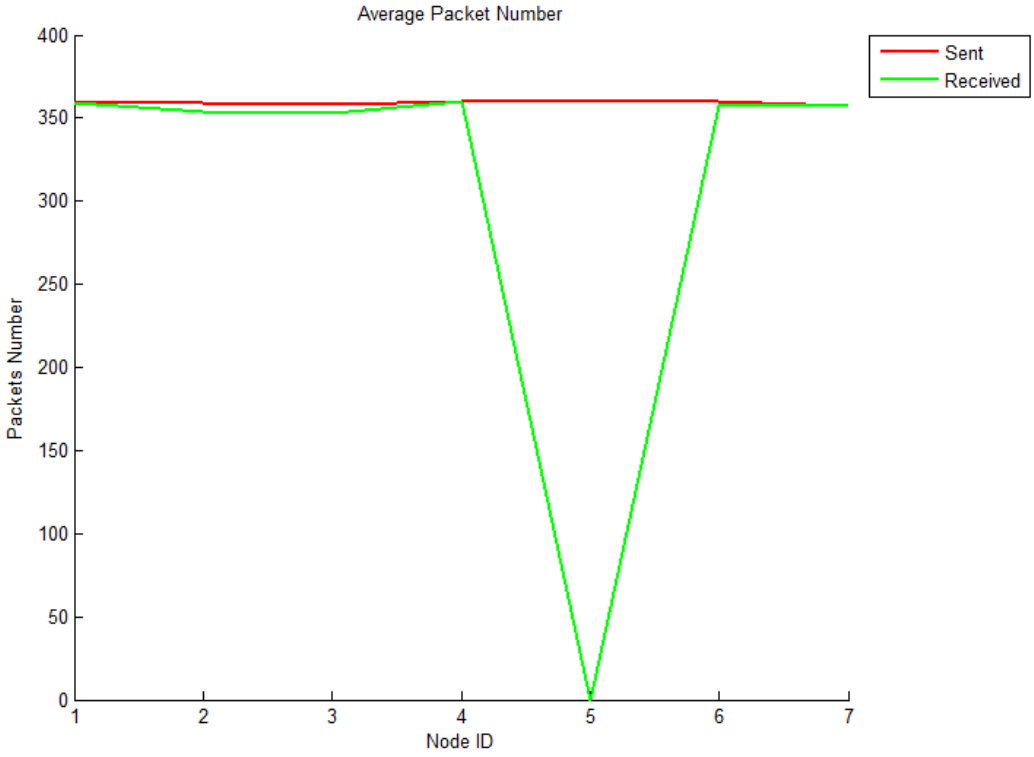
Τοπολογία 2.1.1.2

Στην πιο πάνω τοπολογία, εμφανίζεται ένας κακόβουλος κόμβος μέσα στο δίκτυο, ενώ οι υπόλοιποι παραμένουν υγιείς.
Όπως ξεκάθαρα φαίνεται από την εικόνα, ο κόμβος ο οποίος θα επηρεαστεί από αυτή την αλλαγή, είναι ο κόμβος 5.

Σενάριο 2.1.1.2
6 Benign – 1 Malicious Nodes
Τοπολογία 2.1.1.2

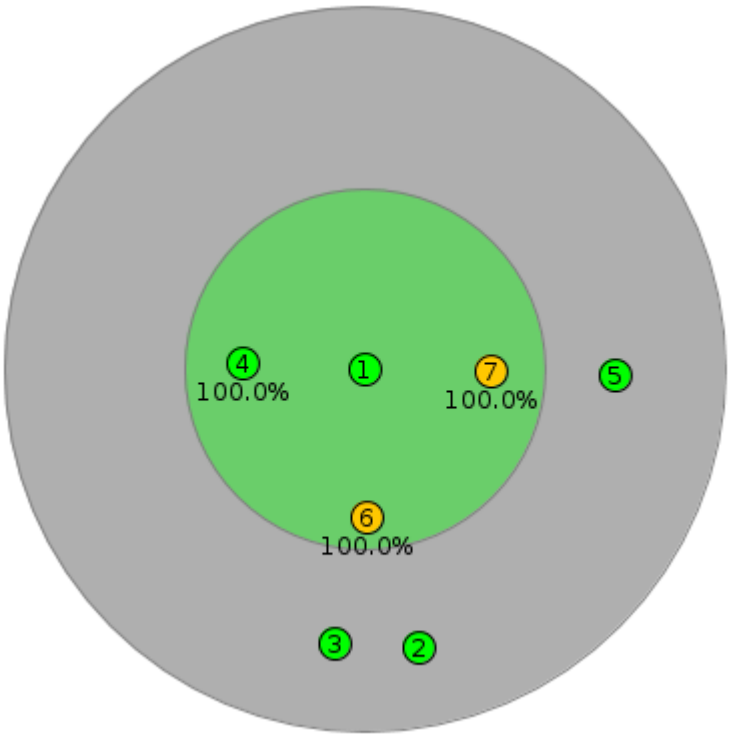


Βλέποντας τις δύο πιο πάνω γραφικές παραστάσεις, παρατηρείται ότι για τον κόμβο 5, παρουσιάζεται πλήρης απώλεια των πακέτων. Ο αριθμός των πακέτων που καταφέρνει ο κόμβος 5 να προωθήσει προς των κόμβο 1, είναι 0, γιατί στην ουσία όλα τα πακέτα καταστρέφονται όταν αυτά φτάσουν στον κόμβο 7. Ο λόγος που συμβαίνει αυτό, οφείλεται στο γεγονός ότι ο 7 λειτουργεί σαν ενδιάμεσος κόμβος, προκειμένου να προωθεί τα πακέτα που στέλνονται από κόμβους που βρίσκονται περισσότερα από 1 hops μακριά από τον τελικό παραλήπτη.
Σε αυτή την περίπτωση τώρα, κανένα από τα πακέτα που φτάνουν από τον κόμβο 5 δεν προωθείται προς τον sink node, και αυτό συμβαίνει γιατί ο 5, είναι το μοναδικό παιδί του μολυσμένου κόμβου. Άρα, μιας και δεν υπάρχουν άλλα παιδιά, δεν είναι δυνατόν να γίνει κάποια εναλλαγή μεταξύ των κόμβων παιδιών, οπότε και αποκλείονται όσα πακέτα φτάνουν από το μοναδικό παιδί.



Σε αυτή την γραφική παράσταση φαίνεται πιο ξεκάθαρα ο τρόπος λειτουργίας του ιού και πώς μπορεί να συμπεριφερθεί το δίκτυο όταν υπάρχει μόνο ένας κόμβος παιδί για τον κακόβουλο κόμβο. Όντως ενώ οι υπόλοιπο κόμβοι καταφέρνουν να προωθήσουν κανονικά τα πακέτα τους παρακάτω, τα πακέτα που φθάνουν από τον κόμβο 5 καταστρέφονται όλα από τον μολυσμένο γονέα του.

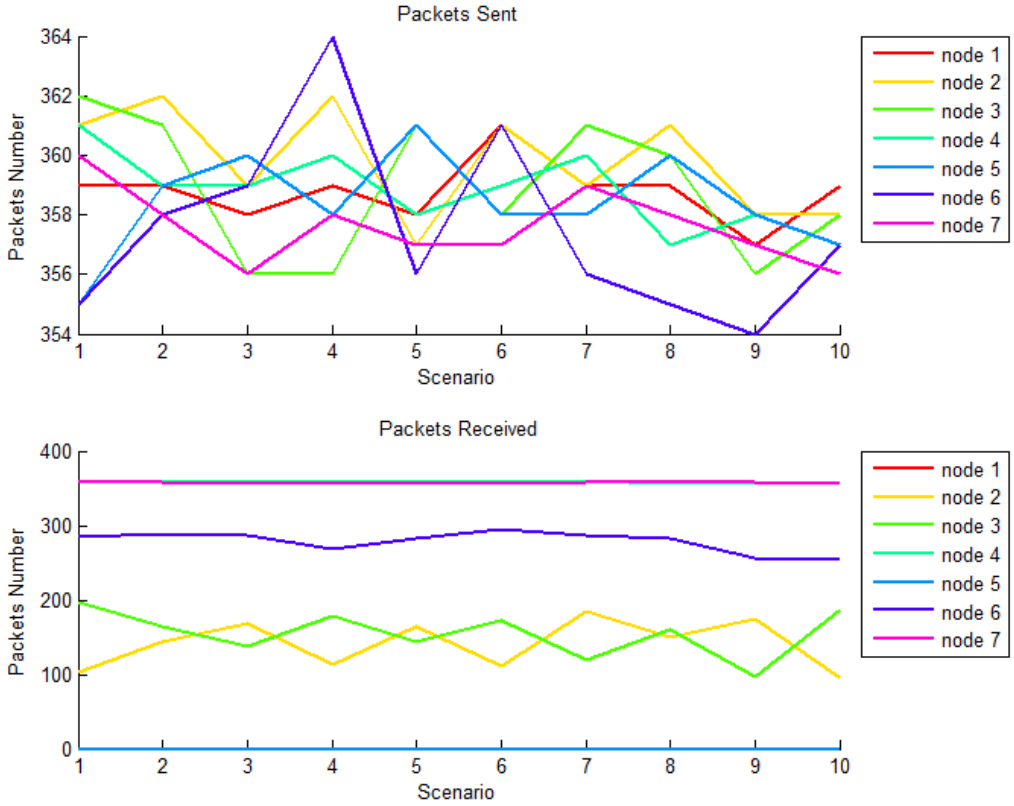
Σενάριο 2.1.1.3
5 Benign – 2 Malicious Nodes



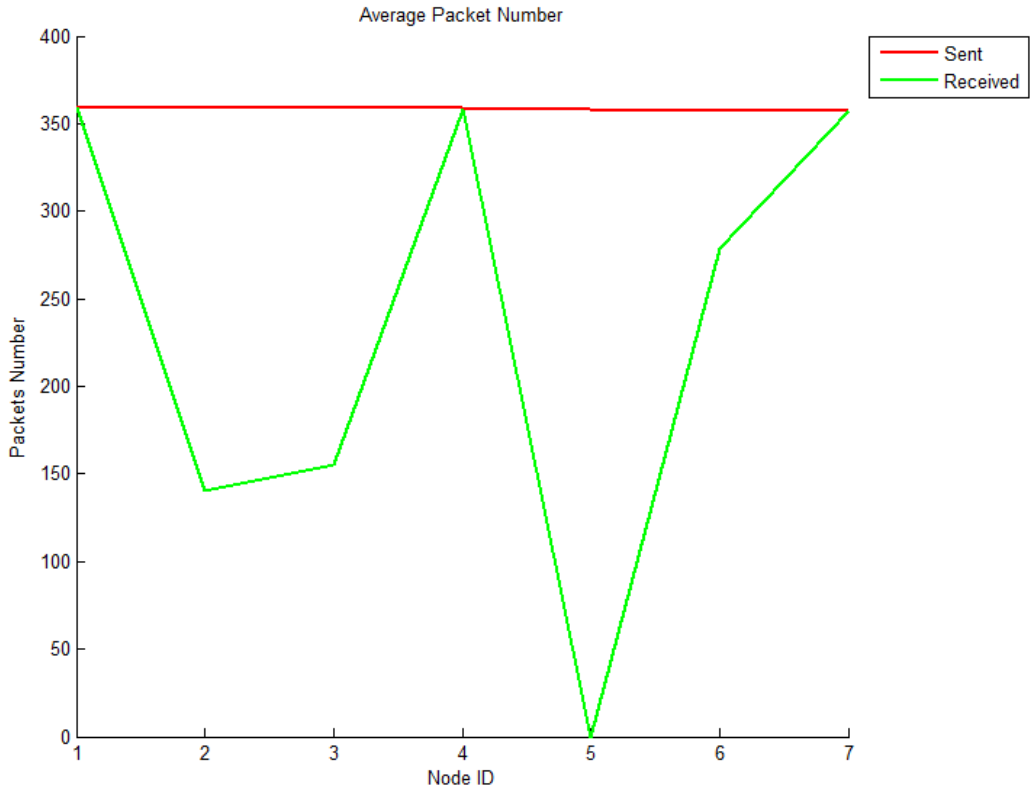
Τοπολογία 2.1.1.3

Πιο πάνω φαίνεται η τοπολογία ενός δικτύου με δύο ‘μολυσμένους’ κόμβους και 5 ‘υγιείς’.
Οι κόμβοι 2 και 3 βρίσκονται μέσα στην εμβέλεια του κόμβου 6, όπως και ο κόμβος 5, στην εμβέλεια του κόμβου 7. Μέσα στην εμβέλεια του κόμβου 1, ο οποίος είναι και ο τελικός παραλήπτης, βρίσκονται οι κόμβοι 4,6 και 7.
Αυτό σημαίνει πως οι κόμβοι 2,3 και 5, επηρεάζονται από τους κακόβουλους κόμβους.

Σενάριο 2.1.1.3
5 Benign – 2 Malicious Nodes
Τοπολογία 2.1.1.3



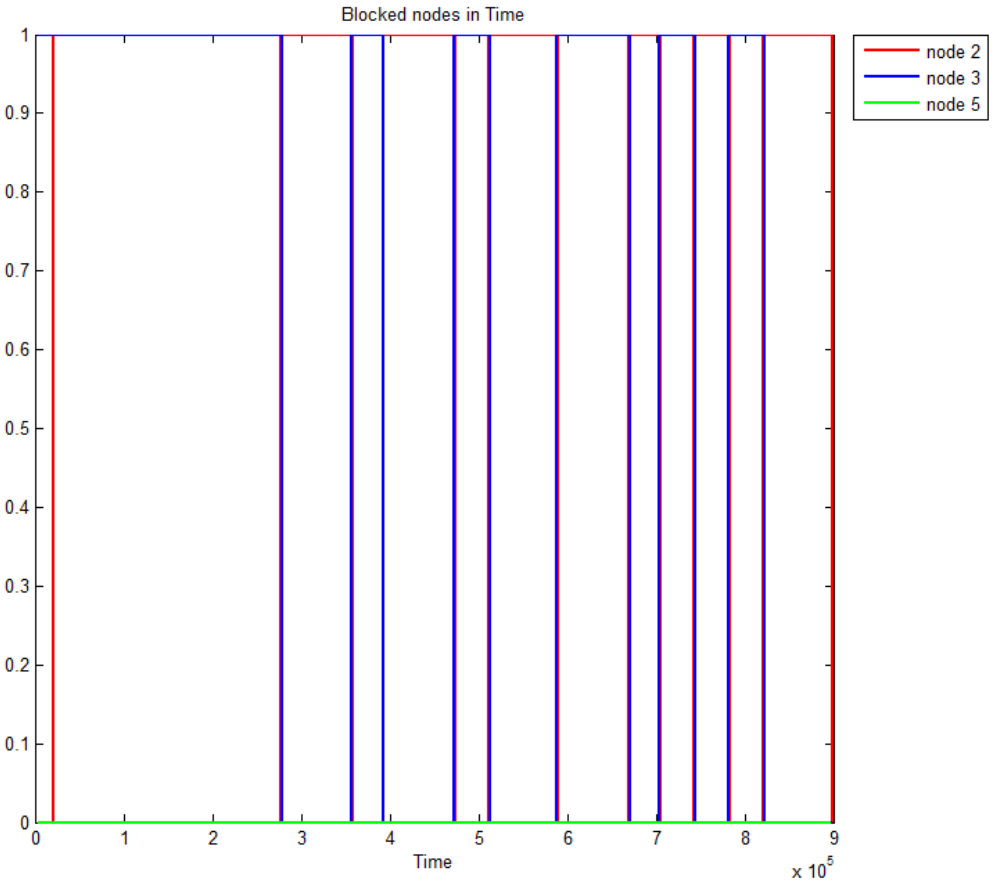
Παρατηρείται πως όλοι οι κόμβοι στέλνουν περίπου τον ίδιο αριθμό πακέτων, για όλες τις διαφορετικές περιπτώσεις. Ο κάθε κόμβος στέλνει τα πακέτα του με τελικό παραλήπτη τον κόμβο 1.
Στην δεύτερη γραφική παράσταση αναπαριστάται ο αριθμός των πακέτων που λαμβάνει ο τελικός παραλήπτης από τον κάθε κόμβο, με τον ίδιο τρόπο όπως και στην πρώτη γραφική παράσταση.
Σε αυτή την περίπτωση φαίνεται ξεκάθαρα η απώλεια των πακέτων από τους κόμβους παιδιά των ‘μολυσμένων’ κόμβων μέσα στο δίκτυο. Συγκεκριμένα παρατηρείται ίδιο ποσοστό απώλειας πακέτων που προέρχονται από τους κόμβους 2 και 3, οι οποίοι είναι παιδιά ενός από τους μολυσμένους κόμβους.
Στην περίπτωση του κόμβου 5, παρατηρείται πως κανένα από τα πακέτα του δεν παραδίνεται στον τελικό προορισμό, αφού είναι ο μοναδικός κόμβος-παιδί του κακόβουλου κόμβου.
Στις γωνιές κάθε γραμμής για κάθε κόμβων είναι ο αριθμός των πακέτων που στάλθηκε στο κάθε σενάριο από τον αντίστοιχο κόμβο και ο αριθμός που παραλήφθηκε από τον συγκεκριμένο κόμβο.



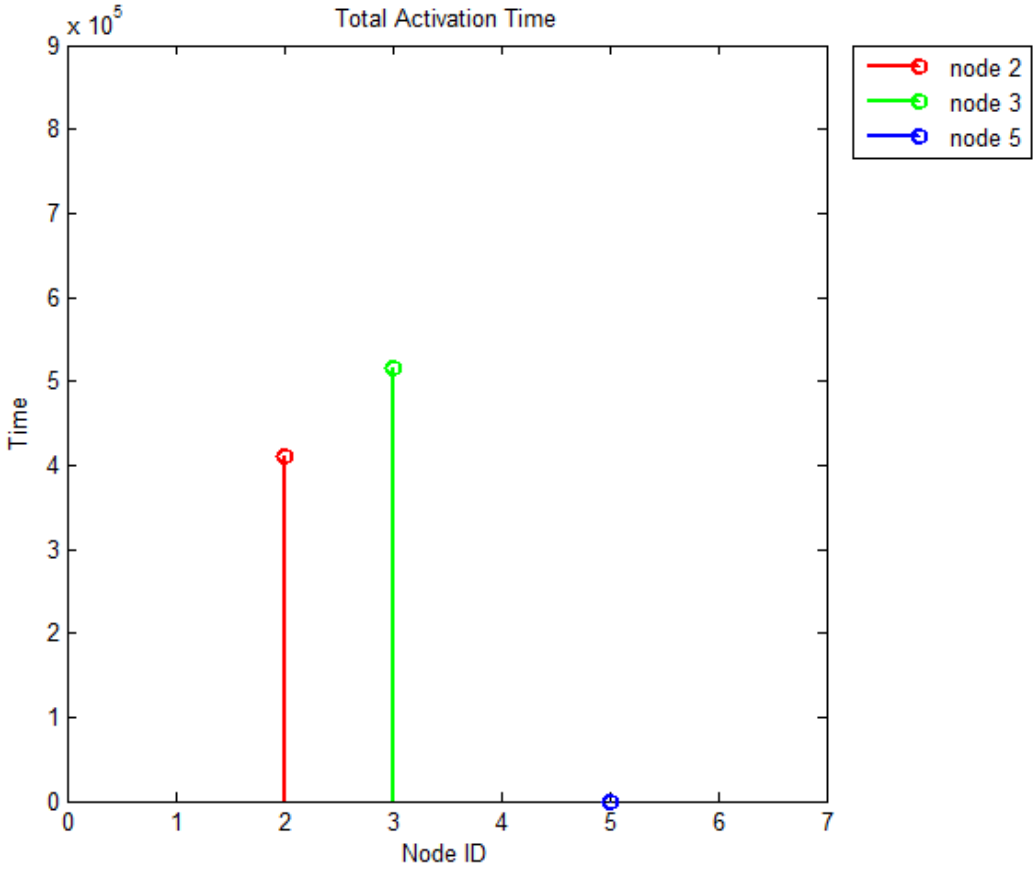
Όπως φαίνεται από την γραφική, ο μέσος όρος των πακέτων που λαμβάνει ο τελικός παραλήπτης από τους κόμβους – παιδιά των μολυσμένων κόμβων, μειώνεται αρκετά, περίπου στο μισό, για κάθε κόμβο. Αυτό οφείλεται στο γεγονός ότι τα πακέτα που φτάνουν από τους κόμβους 2 και 3, οι οποίοι είναι παιδιά του κακόβουλου κόμβου 6, παρεμποδίζονται εναλλάξ για κάποιο χρονικό διάστημα από τον κακόβουλο κόμβο, από το να φτάσουν στον προορισμό τους.

Στην περίπτωση όπου ο κακόβουλος κόμβος είναι ο 7, ο οποίος έχει μόνο ένα παιδί, τότε τα πακέτα αυτού του παιδιού, του 5 δηλαδή, δεν θα φτάνουν ποτέ στον τελικό παραλήπτη, σε καμία χρονική στιγμή. Όταν λοιπόν υπάρχει μόνο ένα παιδί για ένα κακόβουλο κόμβο, τότε τα πακέτα του καταστρέφονται από τον γονέα του επ' αόριστον.

Συγκρίνοντας με το Baseline Scenario φαίνεται καθαρά η διαφορά στην παραλαβή των πακέτων, με την παρουσία του συγκεκριμένου ιού.



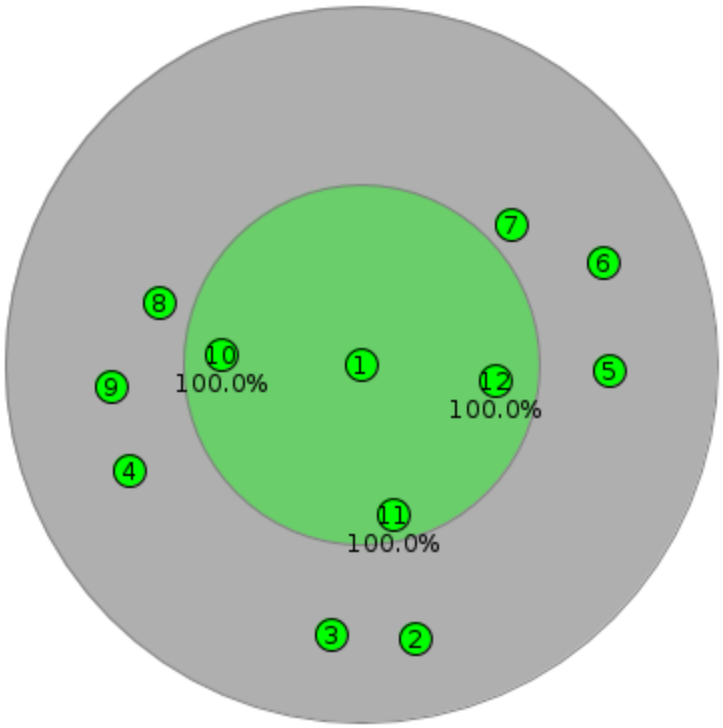
Στην γραφική αυτή παράσταση βλέπουμε σε ποια χρονική στιγμή και για πόσο χρονικό διάστημα, ο τελικός παραλήπτης λαμβάνει πακέτα από τους κόμβους παιδιά των μολυσμένων κόμβων. Στην περίπτωση όπου η τιμή είναι 0, σημαίνει πως αυτό το χρονικό διάστημα ο τελικός παραλήπτης δεν λαμβάνει καθόλου πακέτα από τον κόμβο αποστολέα, το αντίθετο συμβαίνει όταν η τιμή είναι 1.
Ο κόμβος 5 παρατηρούμε πως είναι συνεχώς μπλοκαρισμένος και αυτό οφείλεται στο γεγονός ότι είναι ο μοναδικός κόμβος παιδί του κακόβουλου κόμβου.
Οι κόμβοι 2 και 3 μπλοκάρονται εναλλάξ.



Στην συγκεκριμένη γραφική φαίνεται ο μέσος χρόνος που είναι ενεργός ο κάθε κόμβος, κατά την διάρκεια μιας προσομοίωσης.
Οι τιμές που χρησιμοποιήθηκαν για την πιο πάνω γραφική παράσταση, λήφθηκαν από μια τυχαία περίπτωση προσομοίωσης του σεναρίου.

Παρατηρείται ότι οι κόμβοι 2 και 3, μπλοκάρονται για το μισό χρονικό διάστημα, περίπου της προσομοίωσης και αυτό γίνεται γιατί μπλοκάρονται εναλλάξ. Δηλαδή στο μισό χρονικό διάστημα, τα πακέτα του ενός κόμβου παραδίνονται στον τελικό προορισμό, ενώ το υπόλοιπο συνολικό χρονικό διάστημα, τα πακέτα δεν φτάνουν ποτέ στον sink node.
Όπως και στην πιο πάνω περίπτωση, τα πακέτα από τον κόμβο 5 δεν φτάνουν ποτέ στον προορισμό τους.

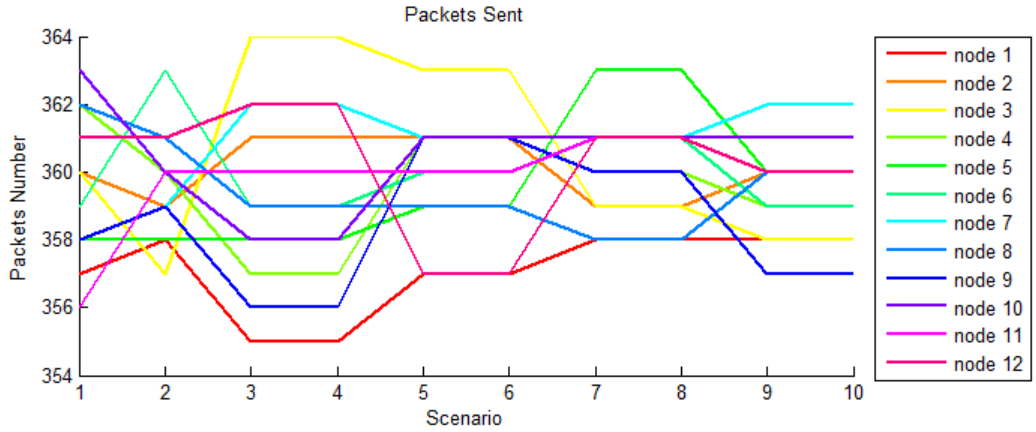
Σενάριο 2.1.2.1
12 Benign – 0 Malicious Nodes

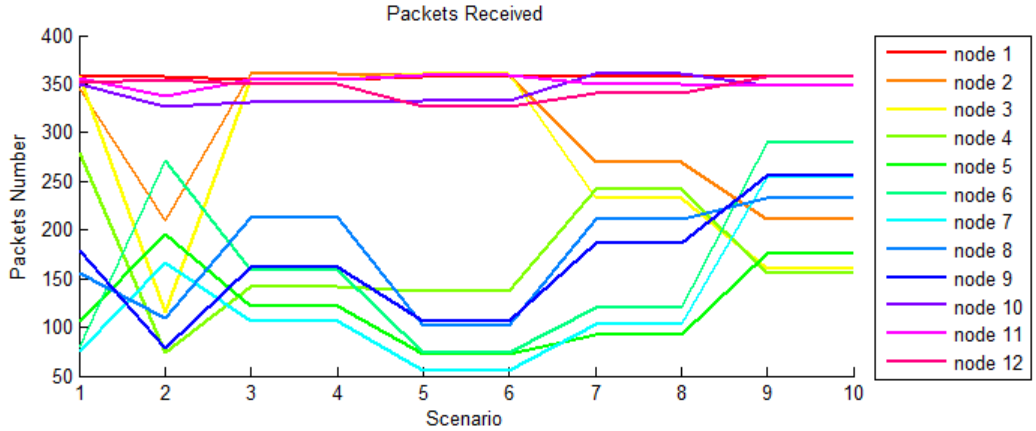


Τοπολογία 2.1.2.1

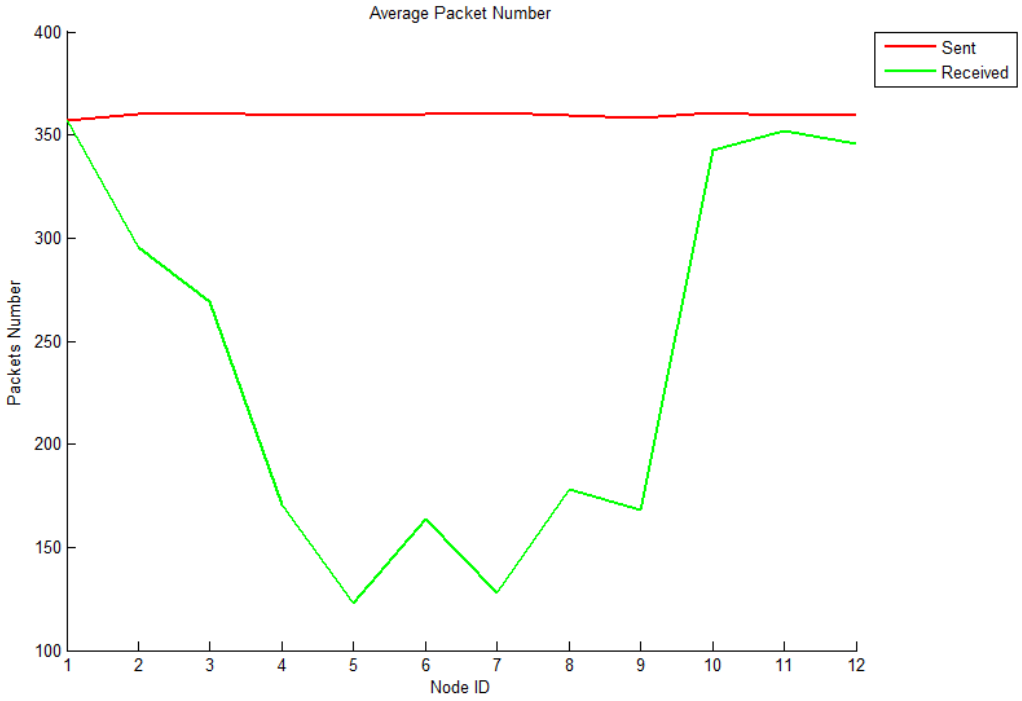
Το σενάριο αυτό, αποτελεί το σενάριο βάση που θα χρησιμοποιηθεί στην συνέχεια για συγκρίσεις με τα σενάρια, τα οποία έχουν ένα ή περισσότερους κακόβουλους κόμβους, προκειμένου να παρατηρηθεί πώς αντιδρά το δίκτυο σε περίπτωση επίθεσης.
Όπως φαίνεται από την εικόνα, σχηματίζονται τρία δέντρα, με γονείς τους κόμβους 10, 11 και 12, κάθε ένα από αυτά, οι οποίοι και λειτουργούν σαν ενδιάμεσοι κόμβοι, προκειμένου να προωθήσουν τα πακέτα των παιδιών τους στον τελικό παραλήπτη.

Σενάριο 2.1.2.1
12 Benign – 0 Malicious Nodes
Τοπολογία 2.1.2.1



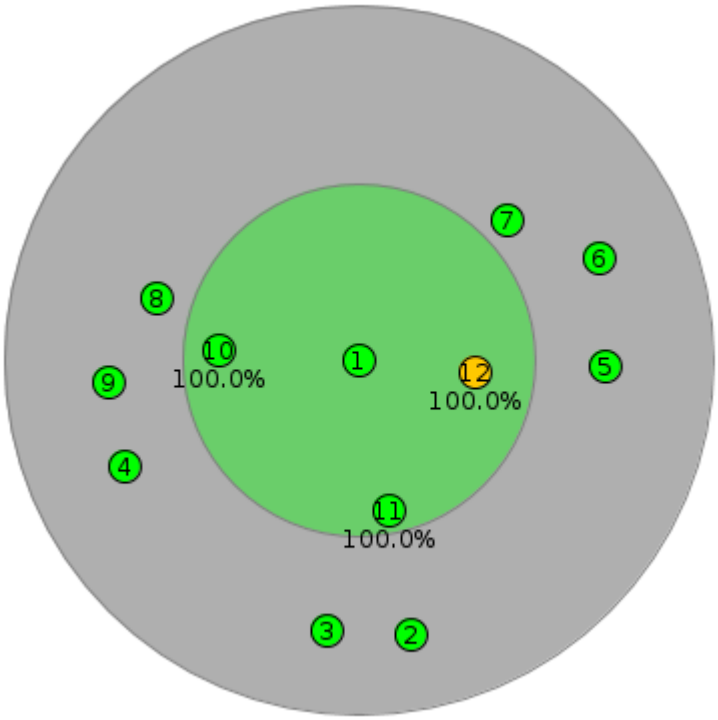


Η γραφική αυτή παρουσιάζει τα αποτελέσματα που προέκυψαν από το σενάριο όπου δεν υπάρχουν καθόλου κακόβουλοι κόμβοι μέσα στο δίκτυο. Εντούτοις παρατηρούνται κάποιες απώλειες πακέτων οι οποίες ίσως οφείλονται σε συγκρούσεις μεταξύ των πακέτων που κινούνται μέσα στο δίκτυο.
Λόγω βέβαια και του μεγάλου αριθμού κόμβων που βρίσκονται μέσα στο δίκτυο και στέλνουν τα πακέτα τους είναι λίγο πολύ αναμενόμενο να υπάρχει κάποια απώλεια πακέτων χωρίς να υπάρχει κάποιος μολυσμένος κόμβος.



Σε αυτή την γραφική παράσταση φαίνονται πιο ξεκάθαρα οι παρατηρήσεις που έγινα προηγουμένως. Φαίνεται δηλαδή πως όντως ενώ δεν υπάρχει κάποιος κακόβουλος κόμβος μέσα στο δίκτυο, εντούτοις υπάρχουν απώλειες μέσα στο δίκτυο.

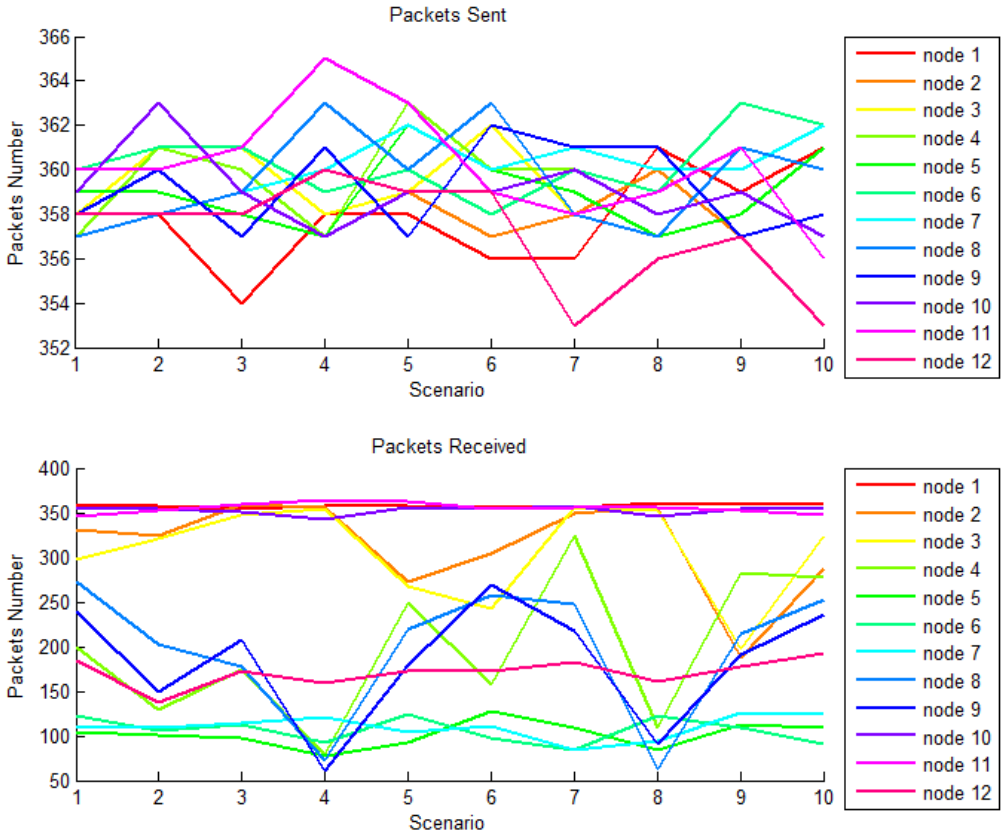
Σενάριο 2.1.2.2
11 Benign – 1 Malicious Nodes



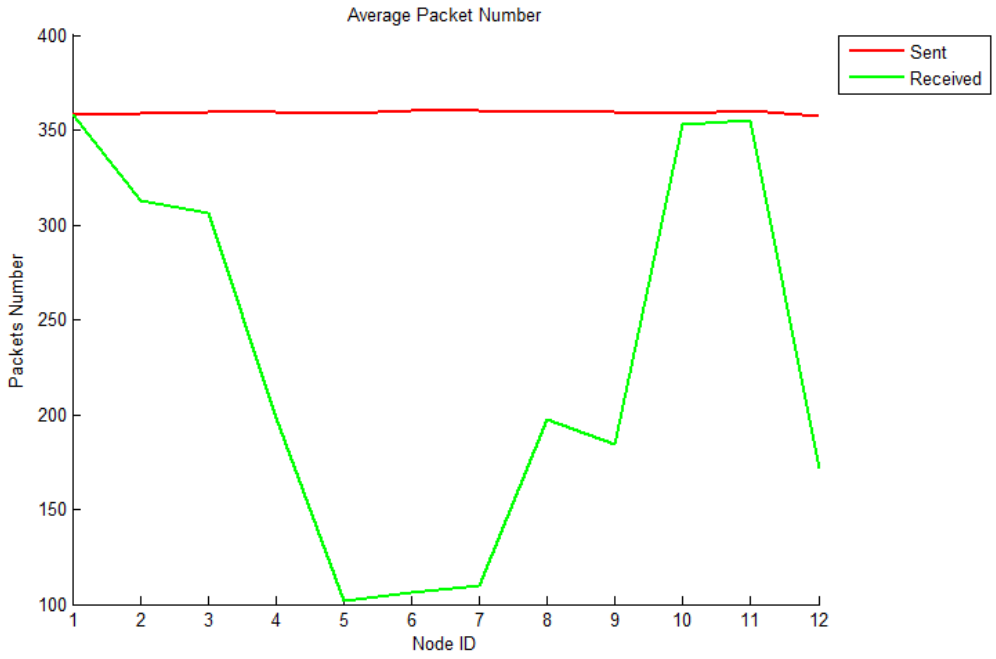
Τοπολογία 2.1.2.2

Στο δίκτυο πιο πάνω, υπάρχει τώρα ένας κακόβουλος κόμβος, ο οποίος επηρεάζει τους κόμβους 5,6 και 7 οι οποίοι βρίσκονται μέσα στην εμβέλεια του, και προωθούν τα πακέτα τους σε αυτόν, αφού είναι ο μοναδικός τους γονέας.

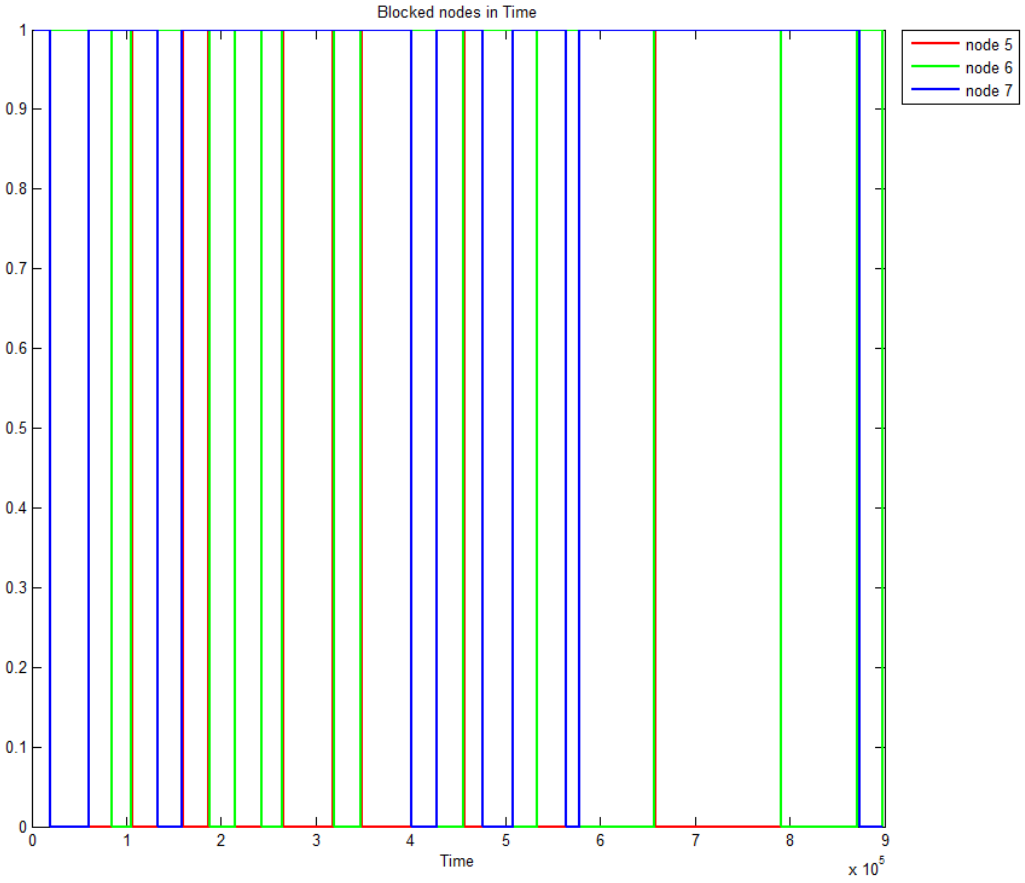
Σενάριο 2.1.2.2
11 Benign – 1 Malicious Nodes
Τοπολογία 2.1.2.2



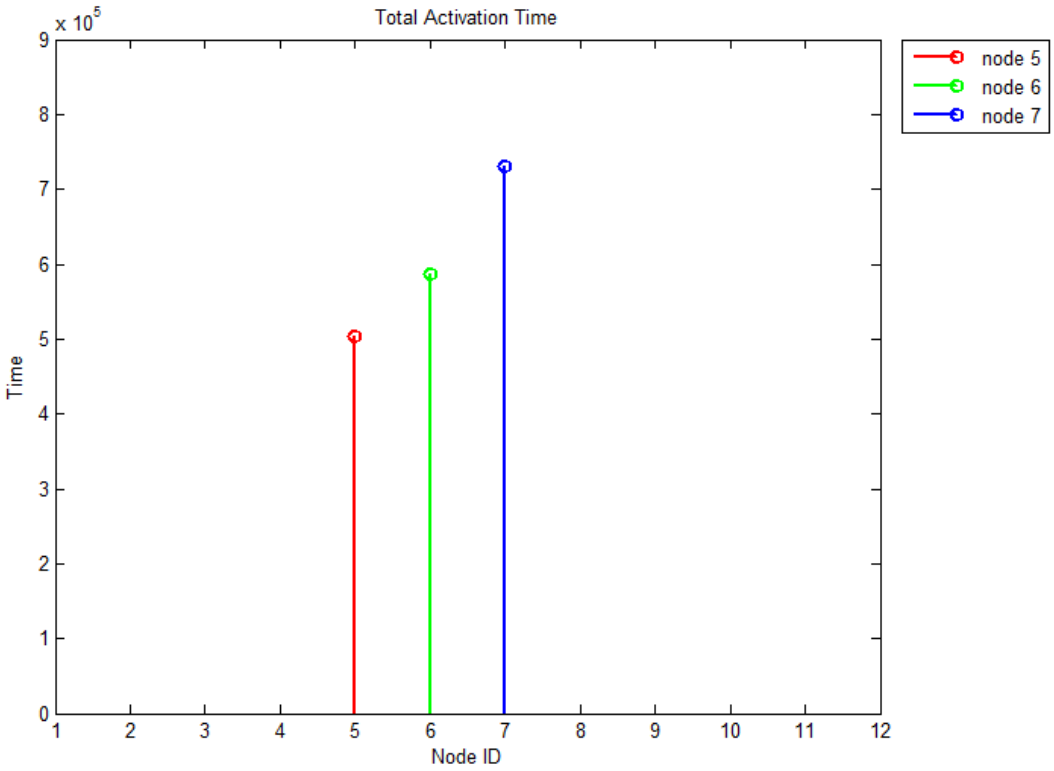
Σε αυτή την γραφική, φαίνονται τα πακέτα που στέλνουν οι κόμβοι μέσα σε ένα δίκτυο, μέσα στο οποίο υπάρχει ένας κακόβουλος κόμβος.
Αρχικά όλοι οι κόμβοι, στέλνουν περίπου τον ίδιο αριθμό πακέτων, προς τον sink node.
Όπως όμως φαίνεται από την δεύτερη γραφική παράσταση, χάνεται ένας μεγάλος αριθμός πακέτων από τους κόμβους 5,6 και 7, κάτι το οποίο οφείλεται στο γεγονός ότι αυτοί οι τρεις χρησιμοποιούν σαν ενδιάμεσο κόμβο τον μολυσμένο, ο οποίος αντί να προωθεί κανονικά τα πακέτα τους, τα καταστρέφει σε διαφορετικές χρονικές στιγμές, εναλλάξ.



Εδώ και πάλι απεικονίζονται καλύτερα τα αποτελέσματα που εξαχθήκαν από την προσομοίωση αυτού του σεναρίου.
Παρατηρείται πιο ξεκάθαρα πως οι κόμβοι 5,6 και 7 οι οποίοι είναι κόμβοι παιδιά του κακόβουλου χάνουν περισσότερα πακέτα, σε σύγκριση με τους υπόλοιπους αν και υπάρχουν γενικώς απώλειες πακέτων μέσα στο δίκτυο.
Το χρονικό διάστημα για το οποίο μπλοκάρονται τα πακέτα του κάθε ενός από τους κόμβους – παιδιά του κακόβουλου κόμβου, μοιράζεται, και καταστρέφει τα πακέτα που προέρχονται από τον καθένα, κατά διαστήματα.

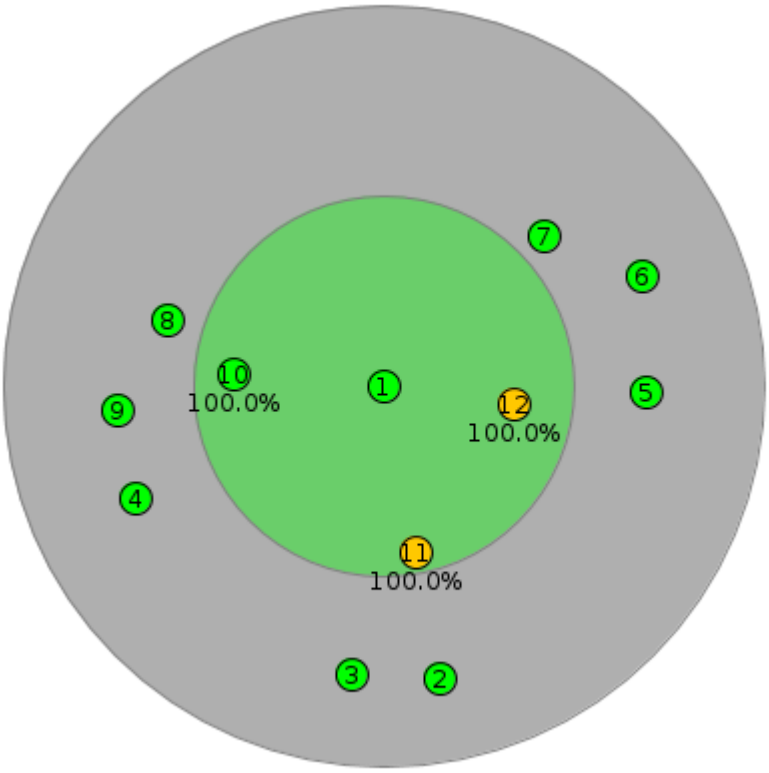


Σε αυτή την γραφική, παρουσιάζεται το χρονικό διάστημα κατά το οποίο είναι ενεργοποιημένοι οι κόμβοι 5,6 και 7, σε ποιες χρονικές στιγμές δηλαδή επιτρέπει ο κακόβουλος κόμβος, τα πακέτα του κάθε ενός από τα παιδιά του, να φτάσουν στον προορισμό τους.



Στην εικόνα πιο πάνω, παρουσιάζεται το συνολικό χρονικό διάστημα κατά το οποίο οι κόμβοι παιδιά του μολυσμένου κόμβου, καταφέρνουν να παραδώσουν τα πακέτα τους στον τελικό παραλήπτη.

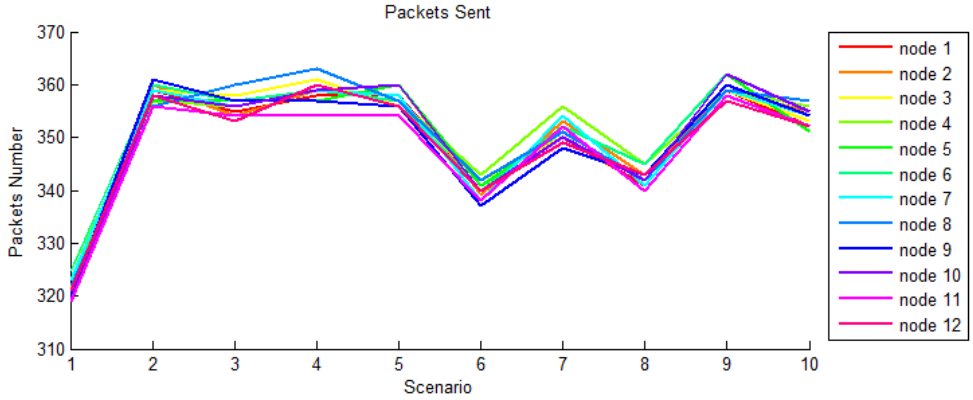
Σενάριο 2.1.2.3
10 Benign – 2 Malicious Nodes

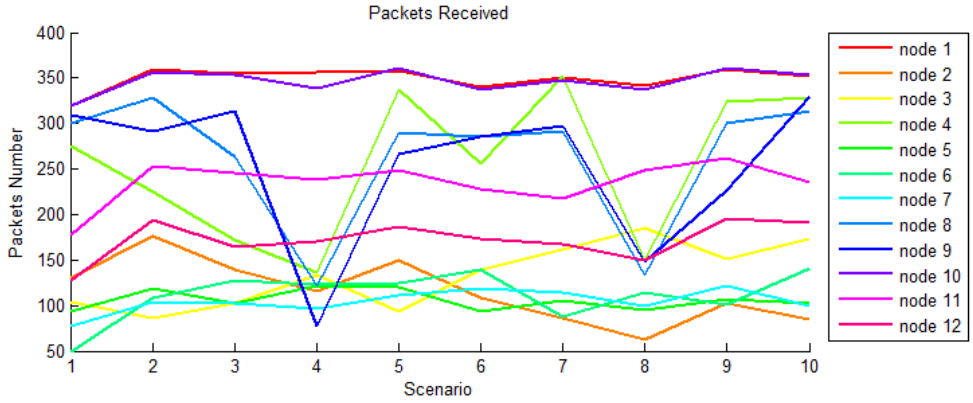


Τοπολογία 2.1.2.3

Σε αυτό το δίκτυο, παρουσιάζονται μόνο δύο κακόβουλοι κόμβοι, οι οποίοι όμως έχουν την δυνατότητα να καταστρέφουν ένα πολύ μεγάλο αριθμό από πακέτα, αφού λειτουργούν ως ενδιάμεσοι κόμβοι για τους κόμβους παιδιά τους, προκειμένου αυτά να μπορέσουν να προωθήσουν τα πακέτα τους στον τελικό παραλήπτη.

Σενάριο 2.1.2.3
10 Benign – 2 Malicious Nodes
Τοπολογία 2.1.2.3

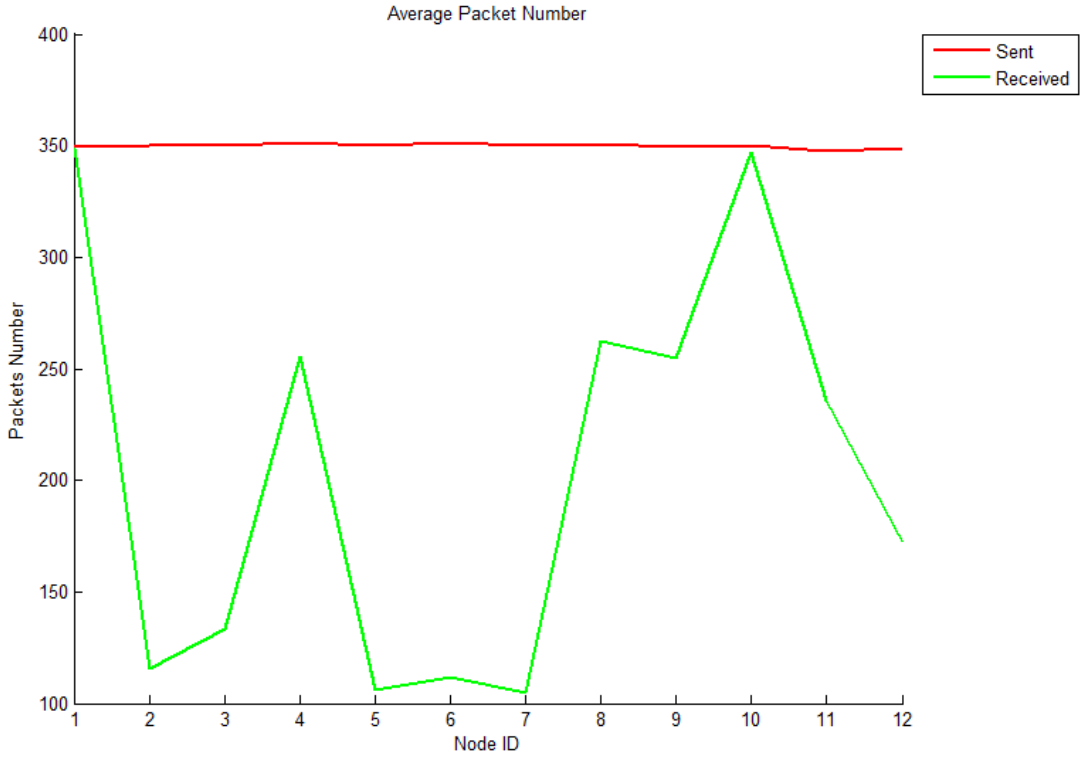




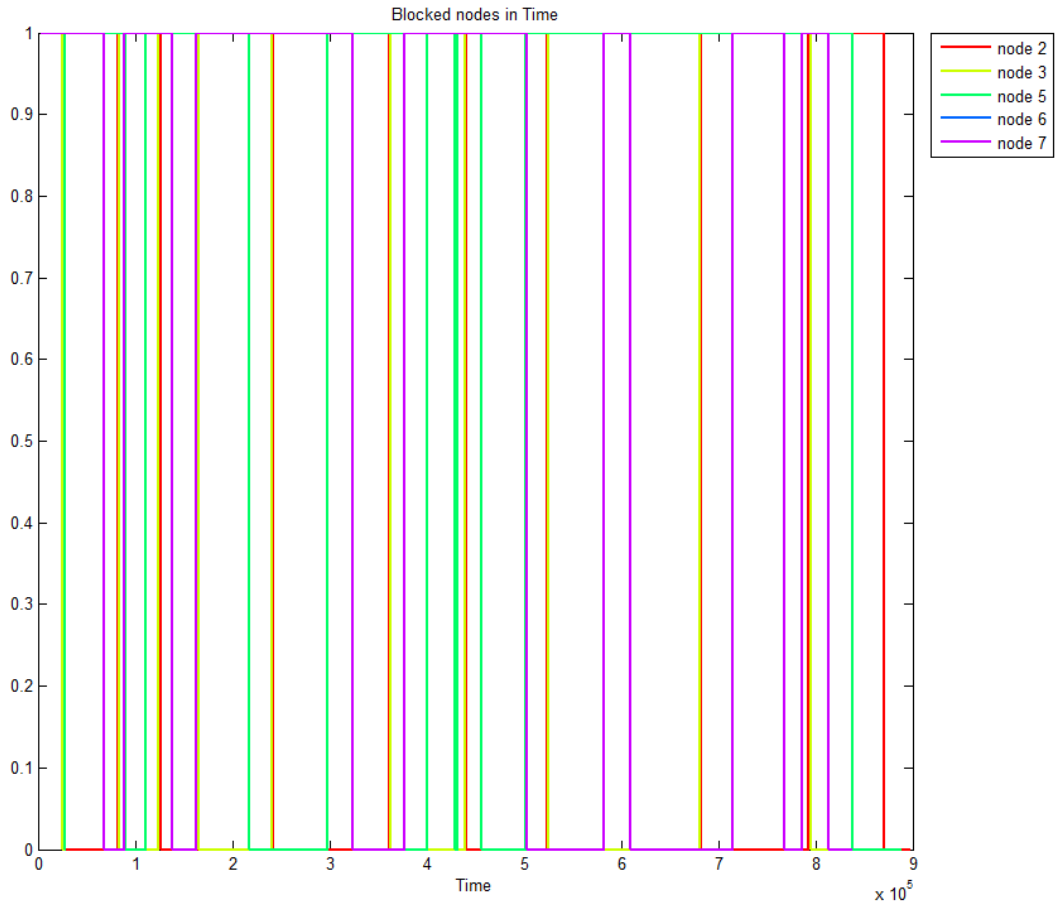
Σε αυτή την γραφική παράσταση παρατηρούμε ότι αρχικά όλοι οι κόμβοι στέλνουν τον ίδιο αριθμό πακέτων, σε κάθε διαφορετική προσομοίωση που γίνεται. Στην γραφική που αναπαριστάται ο αριθμός των πακέτων που λαμβάνει ο τελικός παραλήπτης, παρατηρείται ότι όντως οι κόμβοι – παιδιά των μολυσμένων κόμβων, είναι μπλοκαρισμένοι, δεν μπορούν δηλαδή να παραδοθούν τα πακέτα τους στον sink.

Σε αυτή την τοπολογία, σε αντίθεση με την προηγούμενη, δεν υπάρχει κάποιος κόμβος ο οποίος να είναι μονίμως μπλοκαρισμένος, και αυτό γιατί δεν υπάρχει περίπτωση με ένα και μοναδικό παιδί άλλος μολυσμένου κόμβου.

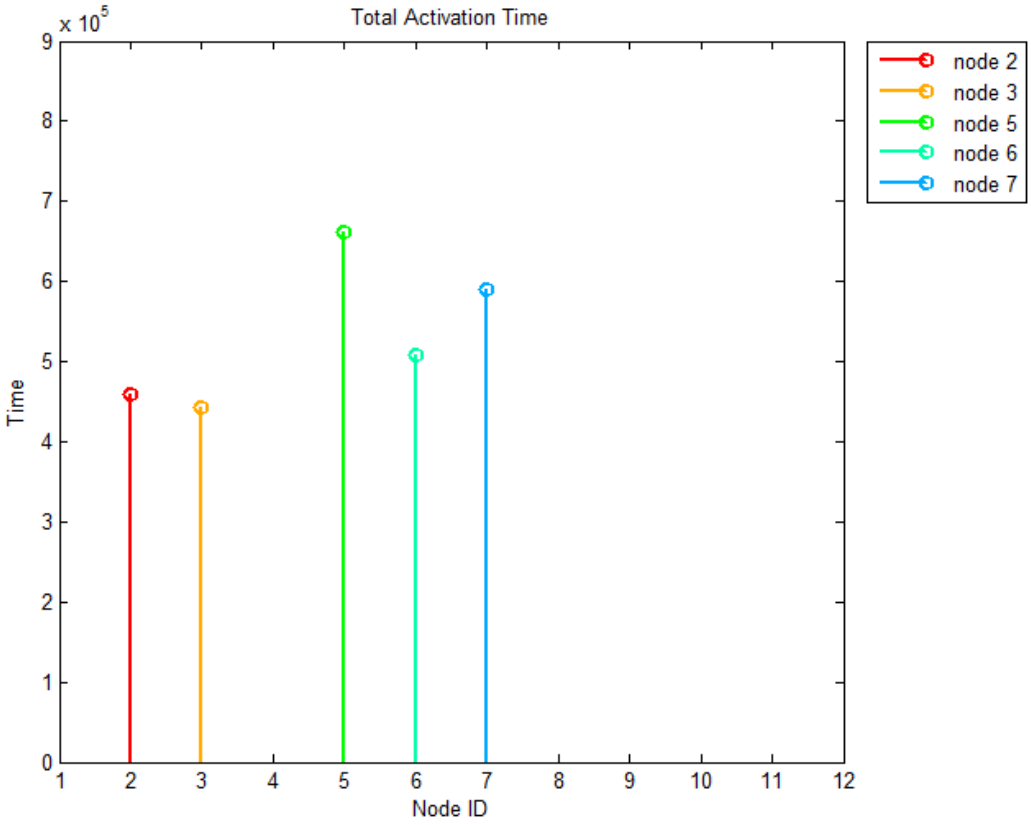
Ο τελικός παραλήπτης, παρατηρούμε ότι λαμβάνει ένα σχετικά μικρότερο αριθμό πακέτων από τους κόμβους παιδιά των μολυσμένων, οι οποίοι είναι οι κόμβοι 2,3,5,6 και 7. Οι υπόλοιποι κόμβοι καταφέρνουν να παραδώσουν κανονικά τα πακέτα τους στον προορισμό τους εκτός από κάποιες περιπτώσεις.



Η πιο πάνω γραφική δείχνει, αρκετά καθαρά, όπως και οι προηγούμενες, ποίοι είναι οι κόμβοι των οποίων τα πακέτα δεν προωθούνται προς τον τελικό παραλήπτη λόγω του μολυσμένου γονέα τους.
Οι κόμβοι 2,3,5,6 και 7, είναι οι κόμβοι οι οποίοι έχουν την μεγαλύτερη απώλεια πακέτων συγκρίνοντας με τους υπόλοιπους κόμβους του δικτύου, όπως επίσης και με την γραφική παράσταση που παρουσιάζει το Baseline Scenario. Συγκρίνοντας με το Baseline Scenario, φαίνεται ότι η απώλεια πακέτων από τους κόμβους – παιδιά είναι αρκετά μεγαλύτερη από την απώλεια πακέτων που υπήρχε όταν μέσα στο δίκτυο δεν παρουσιαζόταν κάποιος κακόβουλος κόμβος.



Σε αυτή την γραφική μπορούμε να δούμε για πόσο χρονικό διάστημα είναι μπλοκαρισμένος ο κάθε κόμβος παιδί κάποιου κακόβουλου.
Όπως παρατηρείται από την γραφική παράσταση, και συγκρίνοντας από την προηγούμενη γραφική η οποία προέκυψε από το σενάριο με 2 μολυσμένους κόμβους, οι αυξομειώσεις των τιμών είναι πολύ περισσότερες. Αυτό γίνεται γιατί ο αριθμός των κακόβουλων κόμβων είναι αυξημένος.
Οι κόμβοι οι οποίοι δεν συμπεριλαμβάνονται στην γραφική παράσταση, είναι συνεχώς ενεργοποιημένοι.

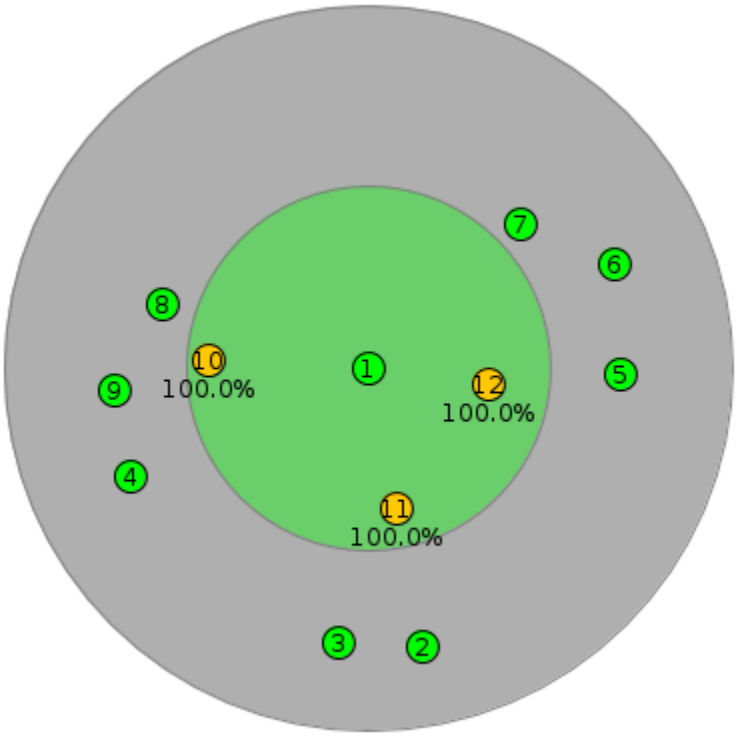


Η πιο πάνω γραφική παράσταση παρουσιάζει το συνολικό χρονικό διάστημα, κατά το οποίο οι κόμβοι που χρησιμοποιούν ως ενδιάμεσο κόμβο κάποιο κακόβουλο, στέλνουν τα πακέτα τους και αυτά όντως παραδίνονται στον τελικό παραλήπτη.

Ουσιαστικά θα μπορούσε να λεχθεί ότι φαίνεται το ποσοστό των πακέτων κάπως, τα οποία φτάνουν όντως στον κόμβο 1, ο οποίος είναι ο sink.
Και σε αυτή την περίπτωση θα μπορούσαμε να πούμε ότι ουσιαστικά όσο περισσότεροι είναι οι κόμβοι παιδιά, τόσο μεγαλύτερο είναι το χρονικό διάστημα κατά το οποίο οι κόμβοι είναι ενεργοποιημένοι.

Ίσως η ποσότητα των πακέτων που καταφέρνει ο κάθε κόμβος να στείλει στον κόμβο 1 αυξάνεται, όμως η συνολική ποσότητα των πακέτων που φτάνουν στον παραλήπτη παραμένει η ίδια.

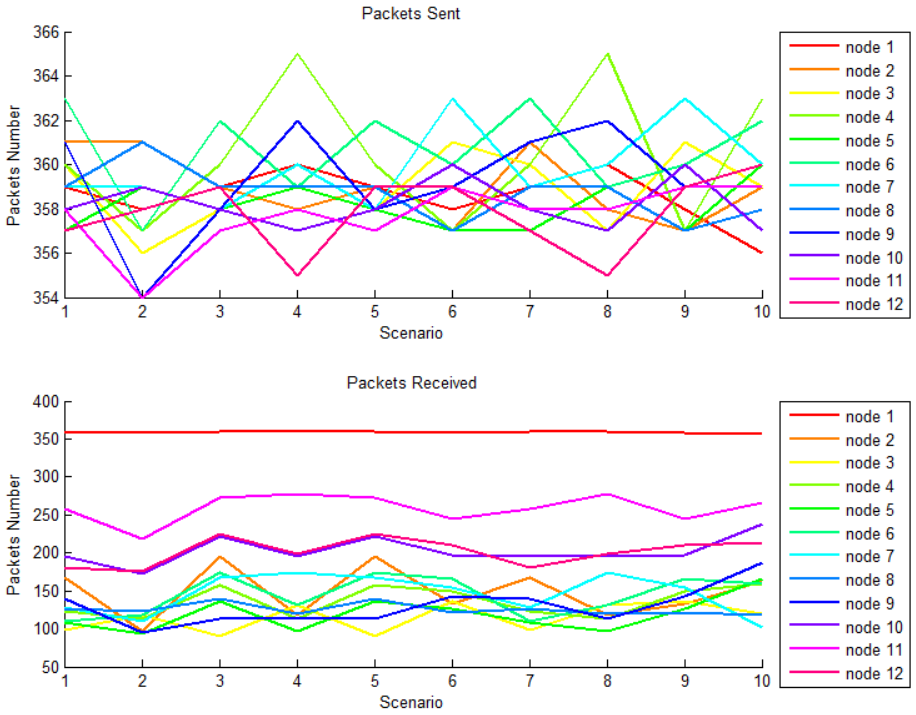
Σενάριο 2.1.2.4
9 Benign – 3 Malicious Nodes



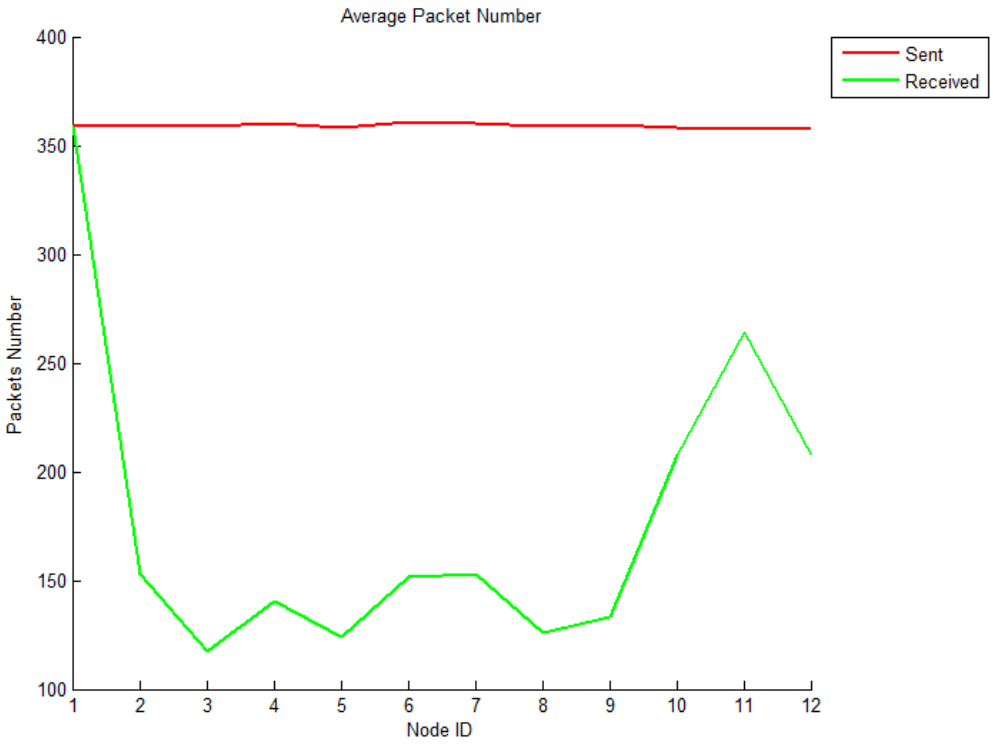
Τοπολογία 2.1.2.4

Σε αυτή την τοπολογία υπάρχουν 3 κακόβουλοι κόμβοι, οι οποίοι είναι γονείς κάποιων άλλων κόμβων.
Μπορεί λοιπόν κάθε ένας από αυτός τους κακόβουλους κόμβους να απορρίψει επιλεκτικά κάποια από τα πακέτα που φτάνουν σε αυτόν από τα παιδιά του.
Ουσιαστικά το δίκτυο αυτό, αποτελείται από 3 δέντρα, και το κάθε ένα έχει ως ρίζα ένα κακόβουλο κόμβο.
Οι κόμβοι 5,6 και 7 βρίσκονται μέσα στην εμβέλεια του κόμβου 12, οι κόμβοι 2 και 3 είναι μέσα στην εμβέλεια του κόμβου 11 και οι κόμβοι 4,8 και 9 είναι μέσα στην εμβέλεια του 10. Οι κόμβοι 10,11 και 12, βρίσκονται μέσα στην εμβέλεια του κόμβου 1 , ο οποίος είναι και ο τελικός παραλήπτης.

Σενάριο 2.1.2.4
9 Benign – 3 Malicious Nodes
Τοπολογία 2.1.2.4

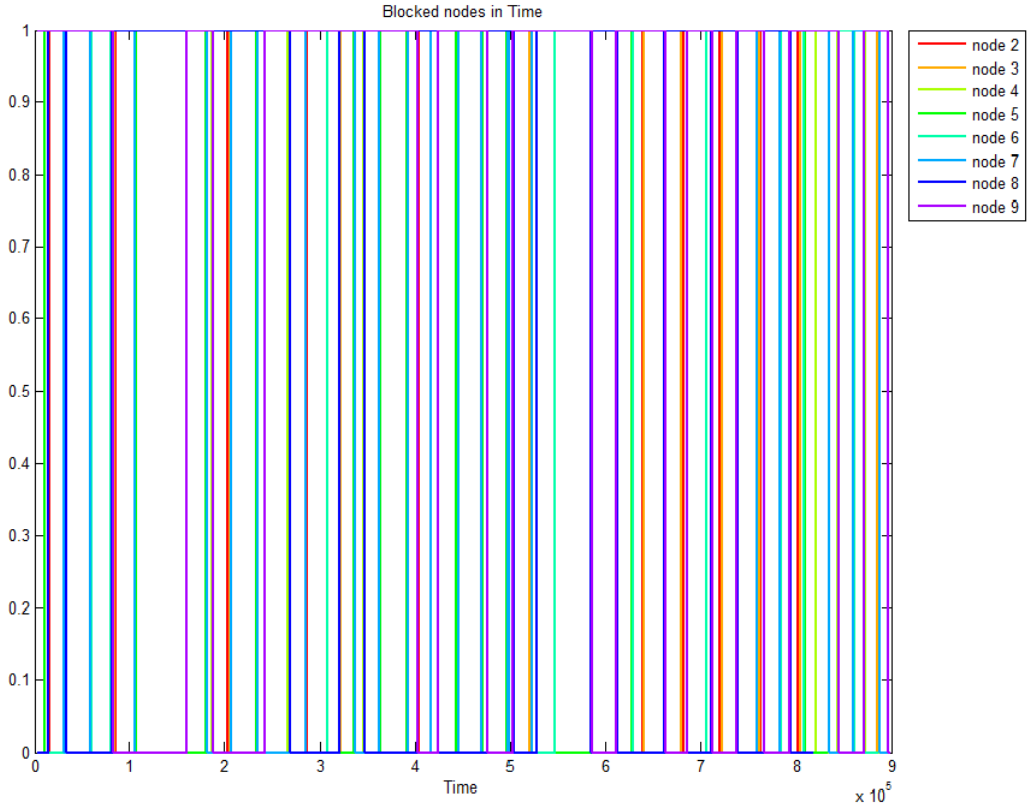


Στην γραφική αυτή παράσταση, φαίνονται τα πακέτα που στέλνει ο κάθε ένας από τους κόμβους μέσα στο δίκτυο, για κάθε σενάριο. Παρατηρείται ότι όλοι οι κόμβοι στέλνουν περίπου τον ίδιο αριθμό πακέτων. Ο κόμβος 1 δεν στέλνει καθόλου πακέτα γιατί είναι ο τελικός παραλήπτης.
Στην δεύτερη γραφική παράσταση, φαίνεται για κάθε κόμβο ο αριθμός των πακέτων που λαμβάνεται από τον τελικό παραλήπτη, σε κάθε σενάριο. Σε αυτή την περίπτωση, ο αριθμός των πακέτων που λαμβάνει ο κόμβος 1 από τους υπόλοιπους κόμβους ,και συγκεκριμένα από τους κόμβους παιδιά των κακόβουλων, είναι κατά πολύ μειωμένος από τον αρχικό αριθμό πακέτων που αυτοί έστελναν.



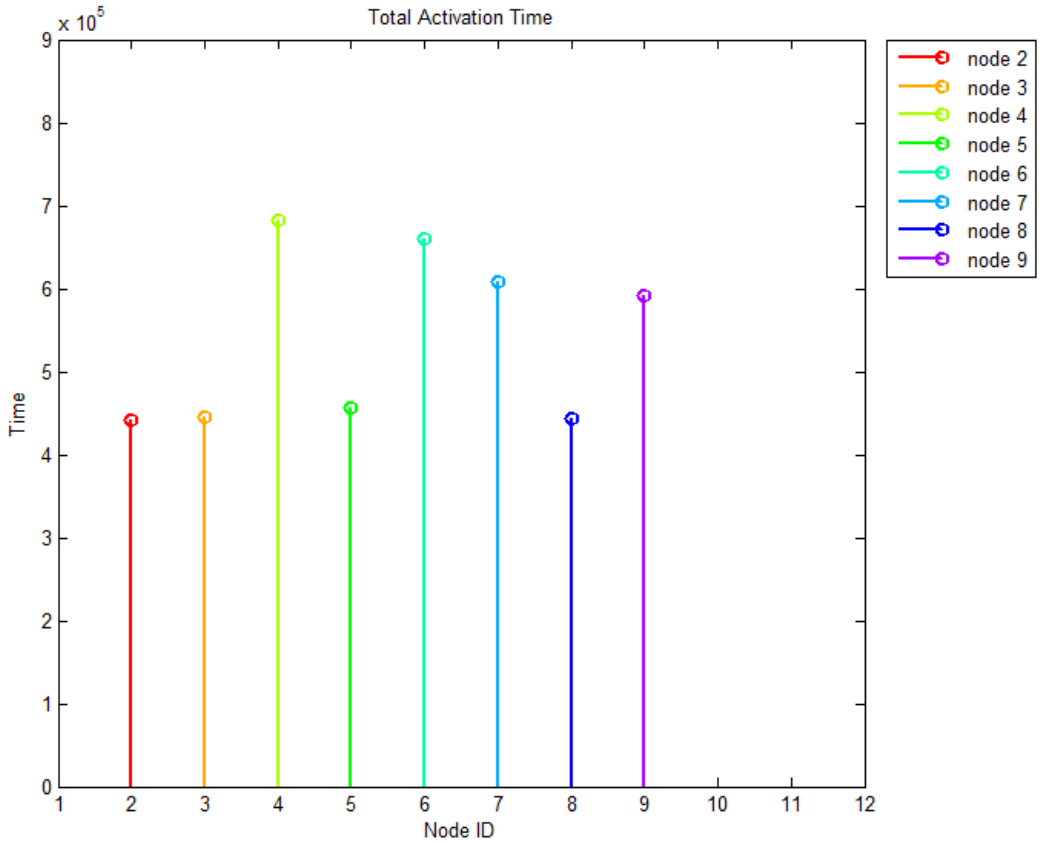
Σε αυτή την γραφική φαίνεται πως όλοι οι κόμβοι μέσα στο δίκτυο, εκτός από τον παραλήπτη που είναι ο 1, και τους κακόβουλους κόμβους οι οποίοι είναι ο 10,11 και 12, παρουσιάζουν μεγάλες απώλειες πακέτων, μεγαλύτερες και από αυτές που υπήρχαν όταν δεν υπήρχαν καθόλου μολυσμένοι κόμβοι μέσα στο δίκτυο.

΄



Στην πιο πάνω γραφική παράσταση φαίνονται τα χρονικά διαστήματα στα οποία είναι ενεργοποιημένοι ή όχι οι κόμβοι.
Συγκεκριμένα η γραφική παράσταση είναι για τους κόμβους οι οποίοι είναι παιδιά των κακόβουλων κόμβων, αφού οι κακόβουλοι κόμβοι είναι πάντα ενεργοί, παραδίνουν πάντα δηλαδή τα δικά τους πακέτα στον τελικό παραλήπτη.

Όσο περισσότεροι είναι οι κόμβοι παιδιά, τότε υπάρχουν βέβαια περισσότερες εναλλαγές ως προς την αποστολή των πακέτων ανά χρονικά διαστήματα.



Σε αυτή την γραφική, παρουσιάζεται το συνολικό χρονικό διάστημα κατά το οποίο είναι ενεργός ο κάθε κόμβος μέσα στο δίκτυο, και συγκεκριμένα οι κόμβοι – παιδιά. Όπως παρατηρείται, οι κόμβοι 2 και 3 που είναι και οι δύο παιδιά ενός από τους τρεις μολυσμένους κόμβους, έχουν τον λιγότερο χρόνο κατά τον οποίο είναι ενεργοί, σε αντίθεση με άλλους κόμβους οι οποίοι είναι ενεργοί για μεγαλύτερο χρονικό διάστημα.

Από την γραφική προκύπτει το συμπέρασμα πως όσο περισσότεροι είναι οι κόμβοι που έχουν ως επόμενο κόμβο ένα κακόβουλο κόμβο, τόσο πιο μεγάλο χρονικό διάστημα αυτοί είναι ενεργοί. Με αυτό εννοούμε πως τόσα περισσότερα πακέτα με αποστολείς αυτούς τους κόμβους φτάνουν στον τελικό προορισμό.

Οι κακόβουλοι κόμβοι είναι συνεχώς ενεργοποιημένοι, δηλαδή τα πακέτα τους φτάνουν κανονικά στον παραλήπτη.

5.2.2. Selective Forwarding Ratio

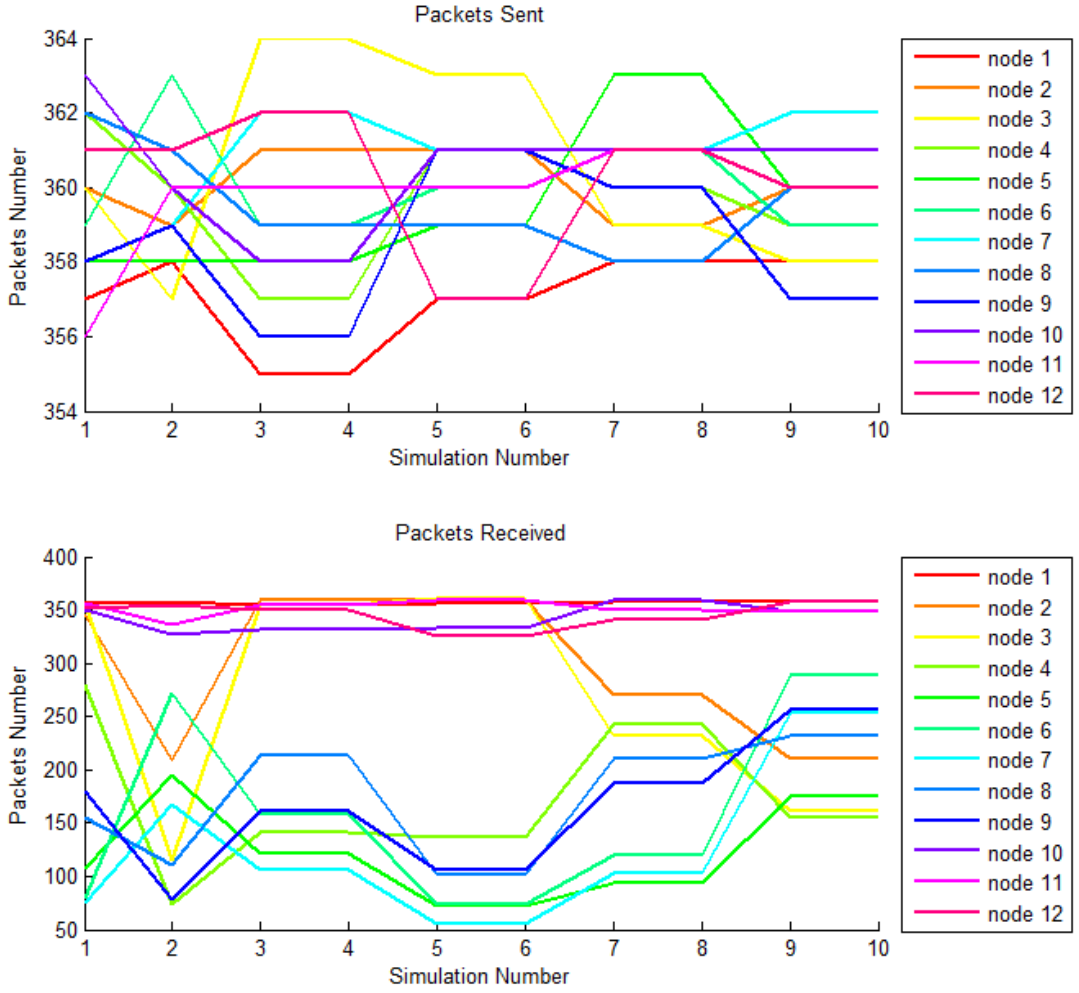
Σε αυτή την επίθεση, και πάλι επηρεάζονται τα πακέτα που φτάνουν από κόμβους οι οποίοι χρησιμοποιούν τον κακόβουλο κόμβο για να στείλουν τα πακέτα τους στον τελικό τους προορισμό.
Τα πακέτα που φτάνουν από άλλους κόμβους, καταστρέφονται σύμφωνα με την τιμή του ratio που παρουσιάζει την δεδομένη χρονική στιγμή ο μολυσμένος κόμβος. Αν αυτό είναι μεγαλύτερο από 50 την στιγμή που φτάνει το πακέτο από κάποιο παιδί, τότε το πακέτο προωθείται κανονικά παρακάτω, αλλιώς απορρίπτεται.

Ουσιαστικά σε αυτή την περίπτωση ιού παρατηρείται κάποια τυχαιότητα ως προς τα πακέτα που προωθούν στον επόμενο κόμβο. Εξαρτάται πάντα από ένα τυχαίο αριθμό που παράγει ο κώδικας του κακόβουλου κόμβου την δεδομένη χρονική στιγμή που φτάνει σε αυτόν το πακέτο. Δεν υπολογίζει ούτε το περιεχόμενο του πακέτου, ούτε την χρονική στιγμή που αυτό φτάνει, ούτε τον κόμβο από τον οποίο αυτό φτάνει.

Σενάρια

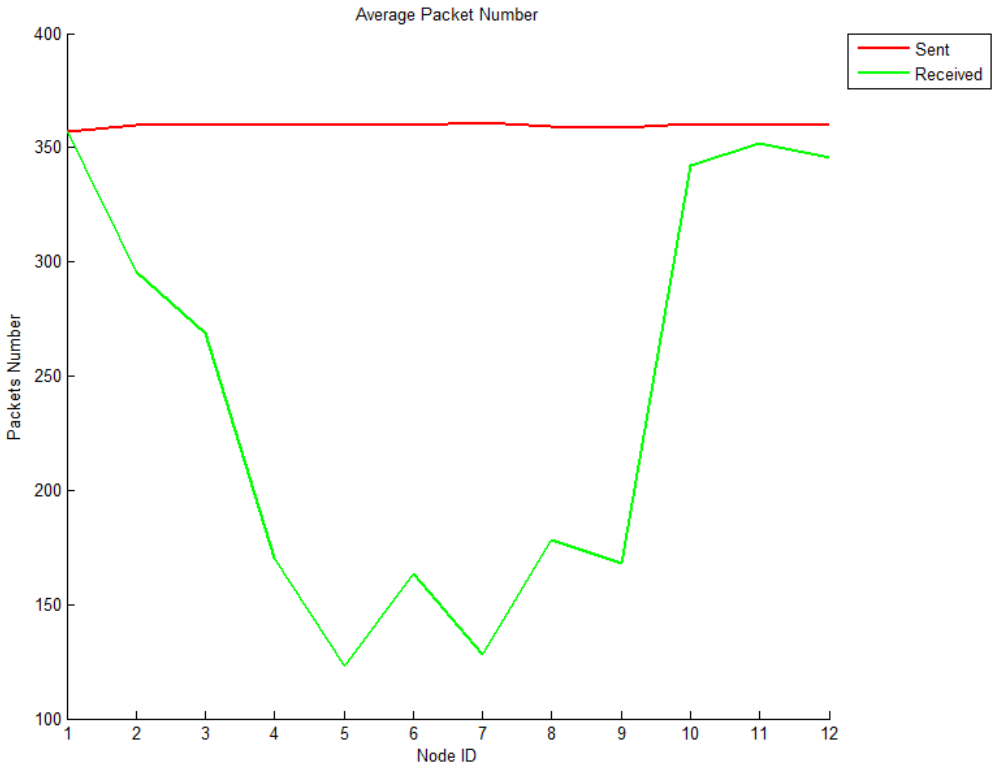
Αρχικά παρουσιάζεται το Baseline scenario, ενώ στην συνέχεια παρουσιάζονται αποτελέσματα και από άλλα σενάρια, με κακόβουλους κόμβους, και των οποίων τα αποτελέσματα συγκρίνονται με το αρχικό δίκτυο, το οποίο περιείχε μόνο καθαρούς κόμβους.
Οι τοπολογίες για τα πιο κάτω σενάρια είναι οι ίδιες με αυτές που χρησιμοποιήθηκαν στην προηγούμενη επίθεση, την Selective Forwarding Source.

Σενάριο 2.2.2.1
12 Benign – 0 Malicious Nodes
Τοπολογία 2.2.2.1



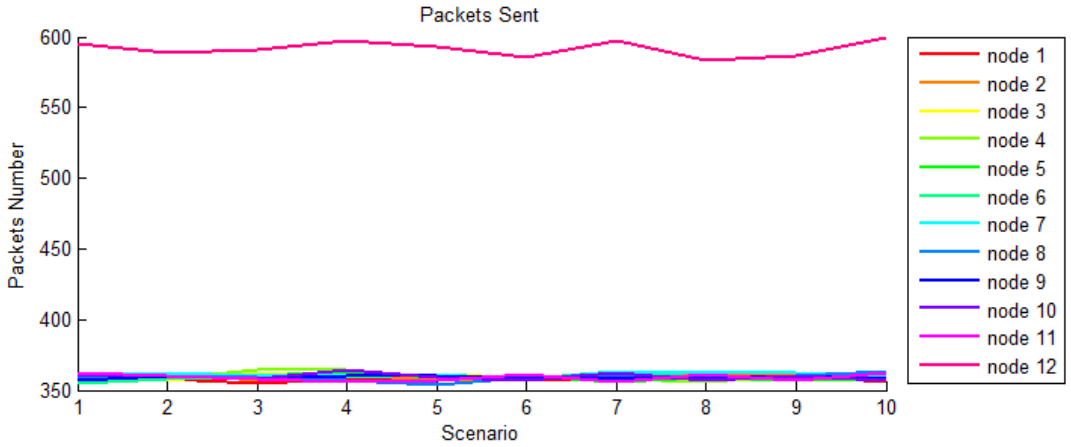
Σε αυτή την γραφική παράσταση , παρουσιάζεται το benign scenario για μια multihop μετάδοση πακέτων. Όλοι οι κόμβοι είναι καθαροί.

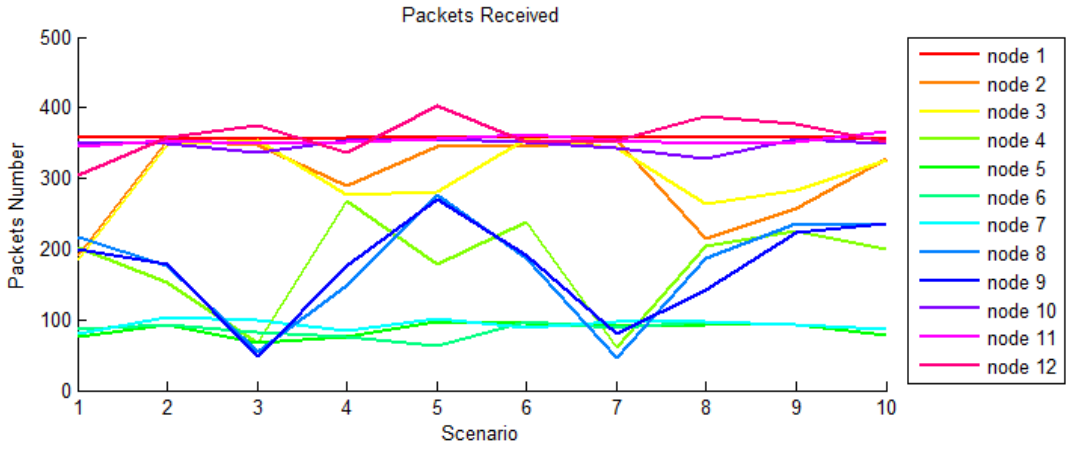
Οι απώλειες πακέτων που παρουσιάζονται όπως αναφέρθηκε και στα προηγούμενα σενάρια, υπενθυμίζεται ότι οφείλονται ίσως σε κάποιες συγκρούσεις που υπάρχουν μέσα στο δίκτυο, λόγω του ότι βέβαια υπάρχει και ένας μεγάλος αριθμός κόμβων οι οποίοι στέλνουν πακέτα μέσα στο δίκτυο.



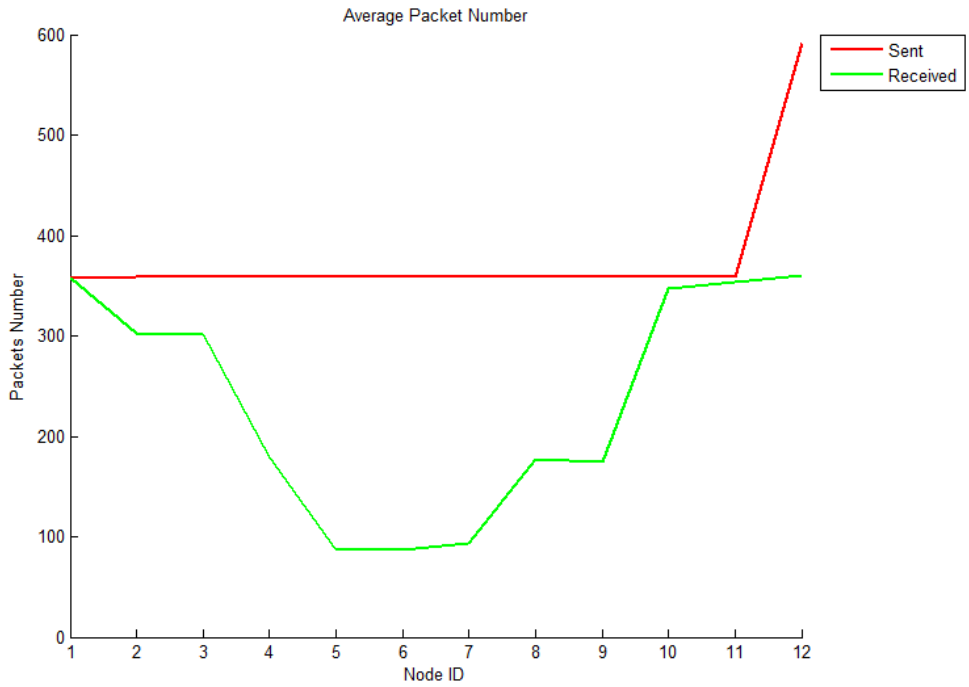
Εδώ παρουσιάζεται το Baseline σενάριο για τον ιό αυτό. Παρατηρείται πως μέσα στο δίκτυο υπάρχουν κάποιες απώλειες πακέτων παρόλο που δεν υπάρχει κάποιος μολυσμένος κόμβος.
Η γραφική αυτή θα χρησιμοποιηθεί στην συνέχεια, όπως και στις προηγούμενες περιπτώσεις, ως μέτρο σύγκρισης μεταξύ των υπόλοιπων σεναρίων.

Σενάριο 2.2.2.2
11 Benign – 1 Malicious Nodes
Τοπολογία 2.2.2.2

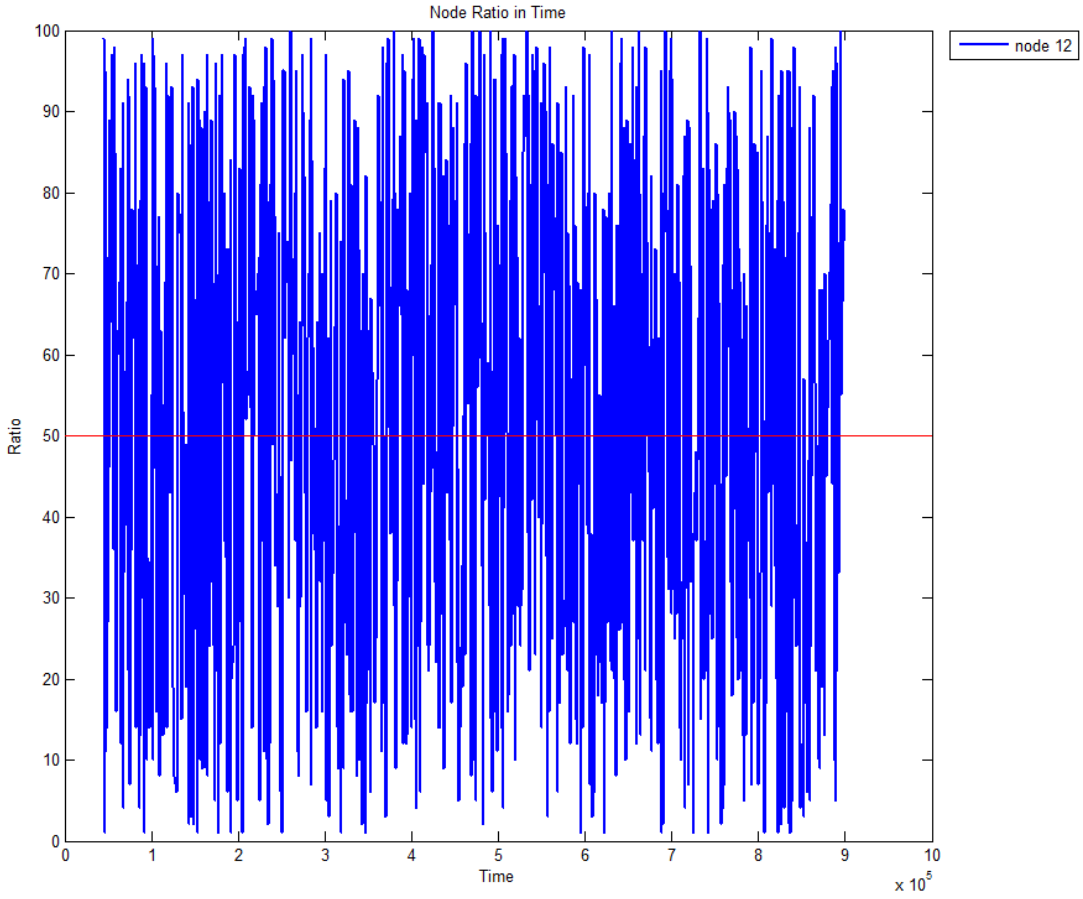




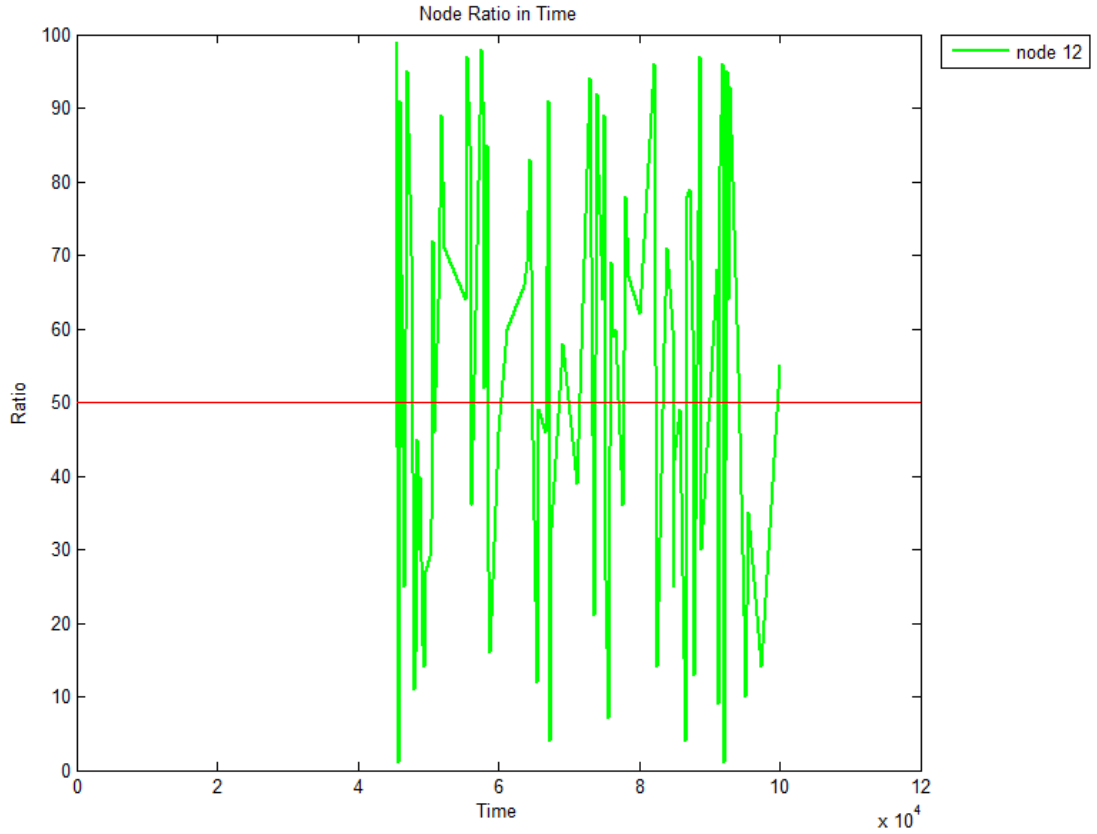
Η πρώτη γραφική παράσταση αναπαριστά τον αριθμό των πακέτων που στέλνει ο κάθε κόμβος μέσα στο δίκτυο. Παρατηρείται πως όλοι οι κόμβοι στέλνουν τον ίδιο αριθμό πακέτων.
Στην δεύτερη γραφική παράσταση, φαίνεται ξεκάθαρα ότι οι κόμβοι 5,6 και 7, επηρεάζονται από τον κακόβουλο κόμβο, ο οποίος είναι γονέας και για τους τρεις. Όπως παρατηρείται λοιπόν, ο αριθμός των πακέτων που προέρχονται από αυτούς τους τρεις και που παραδίνεται στον τελικό παραλήπτη, είναι κατά πολύ μειωμένος, σε σχέση με τον αριθμό των πακέτων που στέλνουν, και που θα έπρεπε να φτάνει στον τελικό παραλήπτη.
Από τις δύο γραφικές παραστάσεις, φαίνεται πως ο κακόβουλος κόμβος, στέλνει όλα τα πακέτα που πρέπει στον τελικό παραλήπτη. Στην πραγματικότητα όμως, ο τελικός παραλήπτης λαμβάνει πολύ λιγότερα πακέτα από αυτά που φαίνεται, τα οποία είναι στην ουσία τα πακέτα που έχουν ως αποστολέα τον κακόβουλο κόμβο.



Συγκρίνοντας αυτό το σενάριο με το Baseline σενάριο, φαίνεται πως ενώ υπήρχαν απώλειες πακέτων ούτως ή άλλως μέσα στο δίκτυο, ο αριθμός των πακέτων που δεν φτάνουν στον τελικό προορισμό αυξάνεται με την παρουσία κάποιου μολυσμένου κόμβου.
Ο μολυσμένος κόμβος σε αυτή την περίπτωση είναι ο 12 και τα παιδιά του είναι οι κόμβοι 5,6 και 7.
Παρατηρείται ότι τα παιδιά του κακόβουλου κόμβου χάνουν σχεδόν τον ίδιο αριθμό πακέτων. Τα πακέτα που φτάνουν από κάθε κόμβο καταστρέφονται σε τυχαίες χρονικές στιγμές.

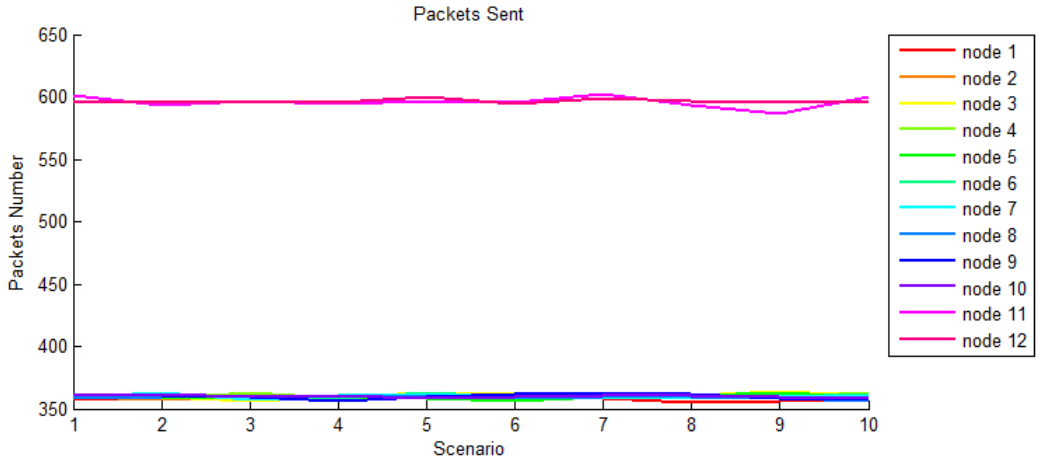


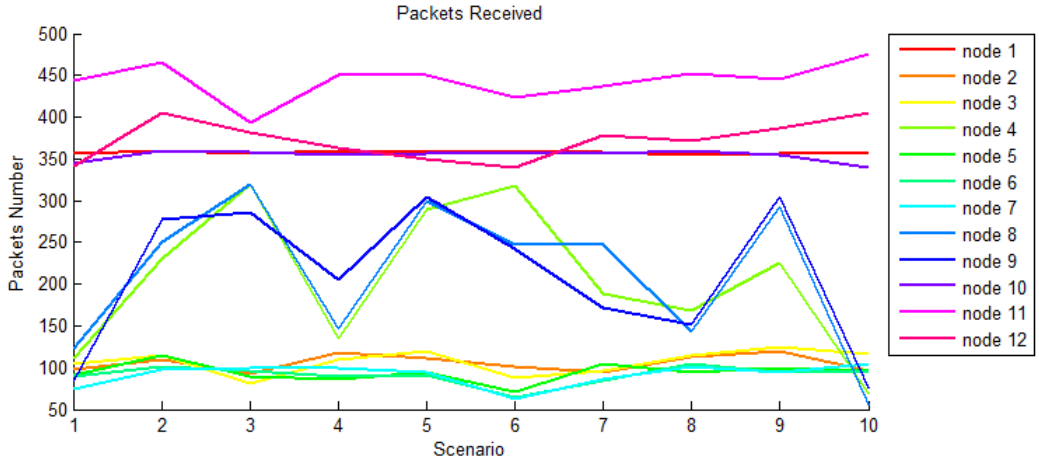
Στην γραφική αυτή παράσταση, φαίνεται η τιμή του ratio ενός συγκεκριμένου κόμβου, του κόμβου 12, ο οποίος είναι ο malicious node, για όλα τα σενάρια, σε συνάρτηση με τον χρόνο.
Για κάθε χρονική στιγμή, όταν η τιμή του ratio είναι μικρότερη ή ίση με 50, τότε ο κόμβος 12 δεν προωθεί κανένα από τα πακέτα των παιδιών του. Από την ευθεία οριζόντια γραμμή στην θέση 50 του άξονα ψ, μπορούμε να διακρίνουμε ανά πάσα χρονική στιγμή πότε ο κόμβος 12 προωθεί κανονικά τα πακέτα, και πότε όχι.
Η κορυφή της κάθε γραμμής στην γραφική παράσταση, δείχνει την τιμή του ratio, την συγκεκριμένη χρονική στιγμή.
Η γραφική αυτή παράσταση είναι παρόμοια για όλα τα σενάρια, γι' αυτό και παρουσιάζεται μόνο η συγκεκριμένη για όλα τα σενάρια.



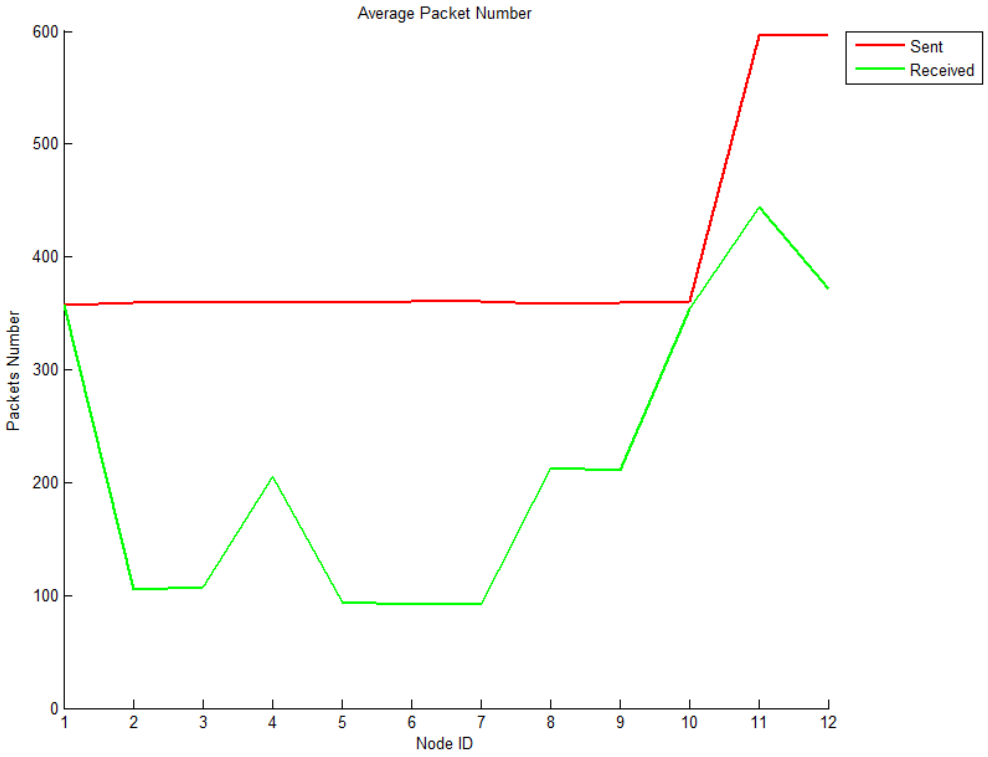
Σε αυτή την γραφική παράσταση τώρα, φαίνονται μέσα σε κάποιο χρονικό διάστημα, από 0 μέχρι 100.000ms οι τιμές του ratio που παρουσιάζει ο κόμβος 12, για κάθε χρονική στιγμή που ένα πακέτο φτάνει σε αυτόν.
Από αυτή την γραφική παράσταση μπορεί να φανεί πιο καθαρά πότε ο κόμβος αυτός αφήνει τα πακέτα από τα παιδιά του να παραδοθούν στον προορισμό τους και πότε όχι. Φαίνεται πως ο αριθμός των πακέτων που παραδίδονται στον προορισμό τους, είναι περίπου ο ίδιος με τον αριθμό των πακέτων που απορρίπτονται, μιας και η τιμή του ratio αυξομειώνεται συνεχώς.

Σενάριο 2.2.2.3
10 Benign – 2 Malicious Nodes
Τοπολογία 2.2.2.3

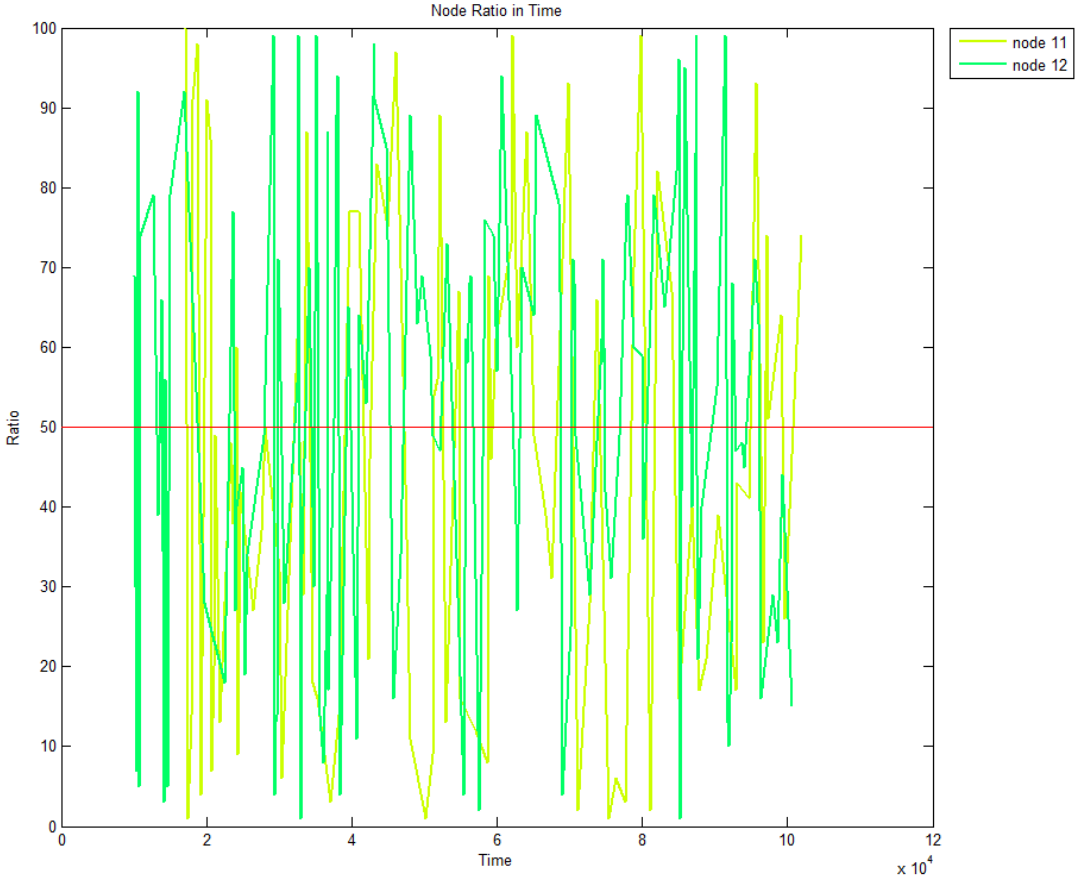




Οι πιο πάνω γραφικές, επίσης παρουσιάζουν τα πακέτα που στέλνονται από τους κόμβους μέσα στο δίκτυο και λαμβάνονται από τον τελικό παραλήπτη, τον κόμβο 1. Οι μολυσμένοι κόμβοι είναι οι κόμβοι 11 και 12, που έχουν ως παιδιά τους κόμβους 2,3,5,6 και 7, και οι οποίοι καταφέρνουν τελικά να παραδώσουν μόνο ένα πολύ μικρό ποσοστό πακέτων στον τελικό παραλήπτη. Συγκεκριμένα ο αριθμός των πακέτων που φτάνουν στον κόμβο 1 από τους κόμβους παιδιά, κυμαίνεται από 50 μέχρι και 100 ενώ ο αρχικός αριθμός των πακέτων που έστελναν οι συγκεκριμένοι κόμβοι, ήταν γύρω στο 350.
Όσο αφορά τους κόμβους 4,8 και 9, καταφέρνουν κανονικά να παραδώσουν τα πακέτα τους εκτός από κάποιες περιπτώσεις, όπου υπάρχει μια μικρή απώλεια των πακέτων, κάτι που όμως δεν οφείλεται σε αυτή την περίπτωση, στην ύπαρξη κακόβουλων κόμβων μέσα στο δίκτυο.

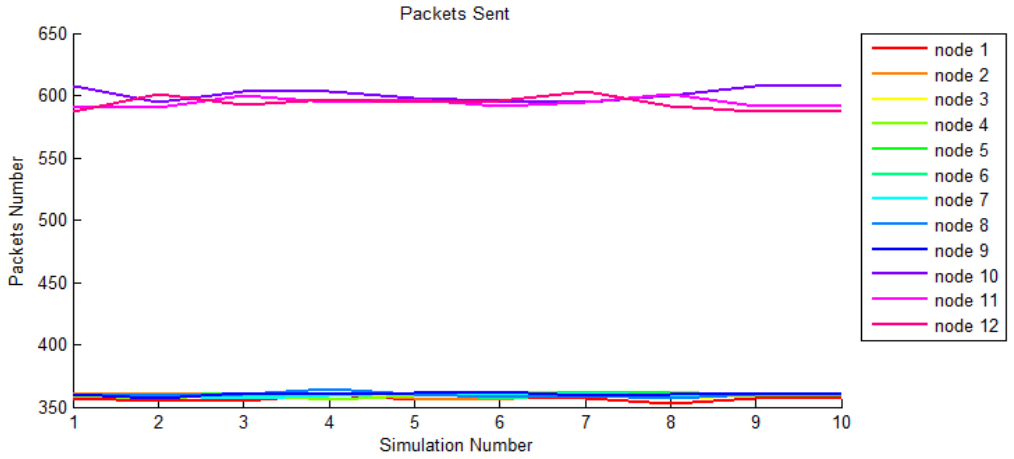


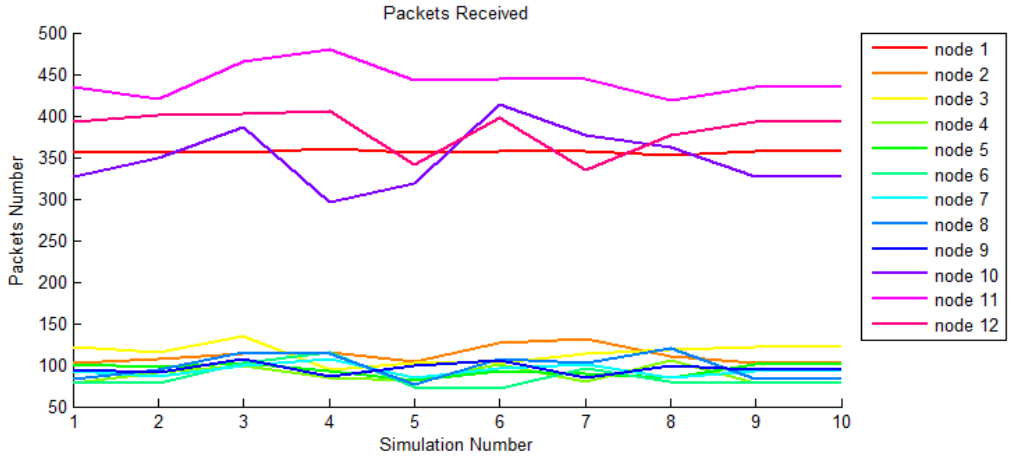
Σε αυτή την γραφική διακρίνεται διαφορά στον αριθμό των πακέτων που φτάνουν στον τελικό παραλήπτη από τους κόμβους 4,8 και 9, σε σχέση με τους υπόλοιπους κόμβους, όπου υπάρχει επίσης κάποια απώλεια πακέτων.
Όπως προαναφέρθηκε στην προηγούμενη γραφική παράσταση υπάρχουν απώλειες από κόμβους παιδιά των κακόβουλων.
Ο μέσος αριθμός πακέτων, λοιπόν που φτάνουν από τους κόμβους – παιδιά των κακόβουλων κόμβων, είναι κατά πολύ μικρότερος από τους μέσους όρους των υπολοίπων κόμβων.



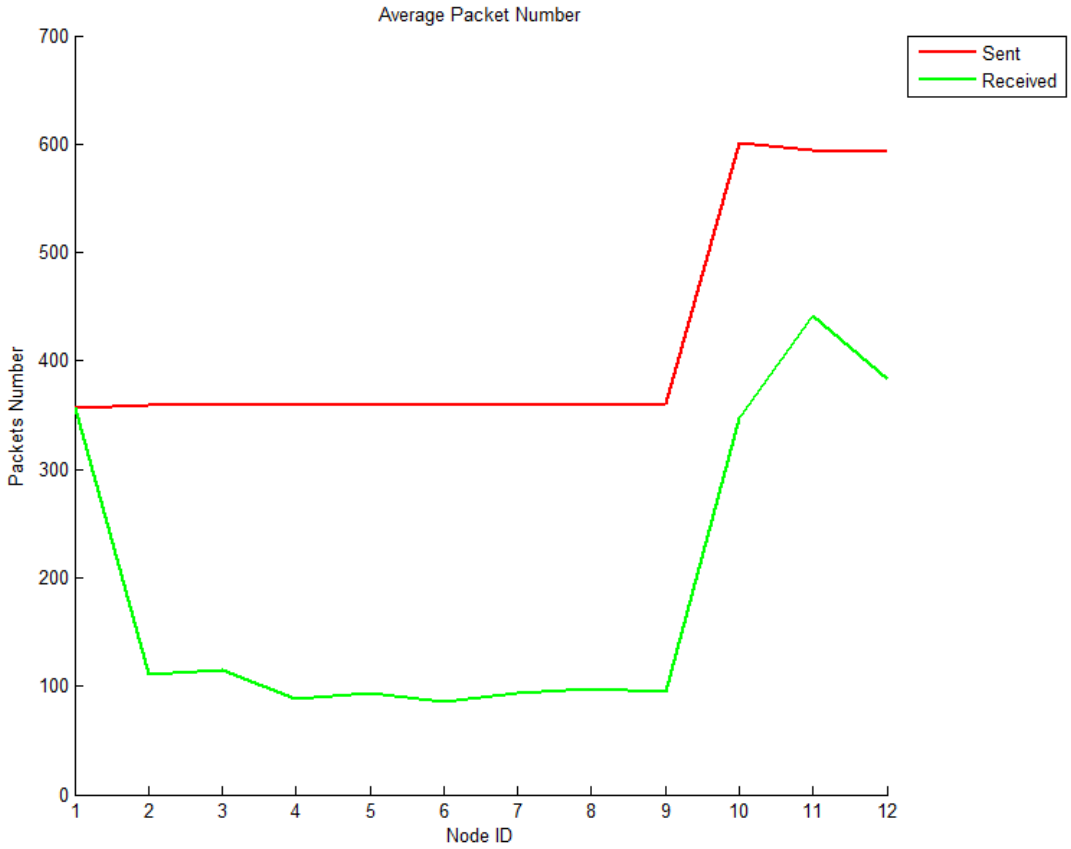
Εδώ παρουσιάζεται η τιμή του Ratio για κάθε ένα από τους κακόβουλους κόμβους, σε σχέση με τον χρόνο.

Σενάριο 2.2.2.4
9 Benign – 3 Malicious Nodes
Τοπολογία 2.2.2.4

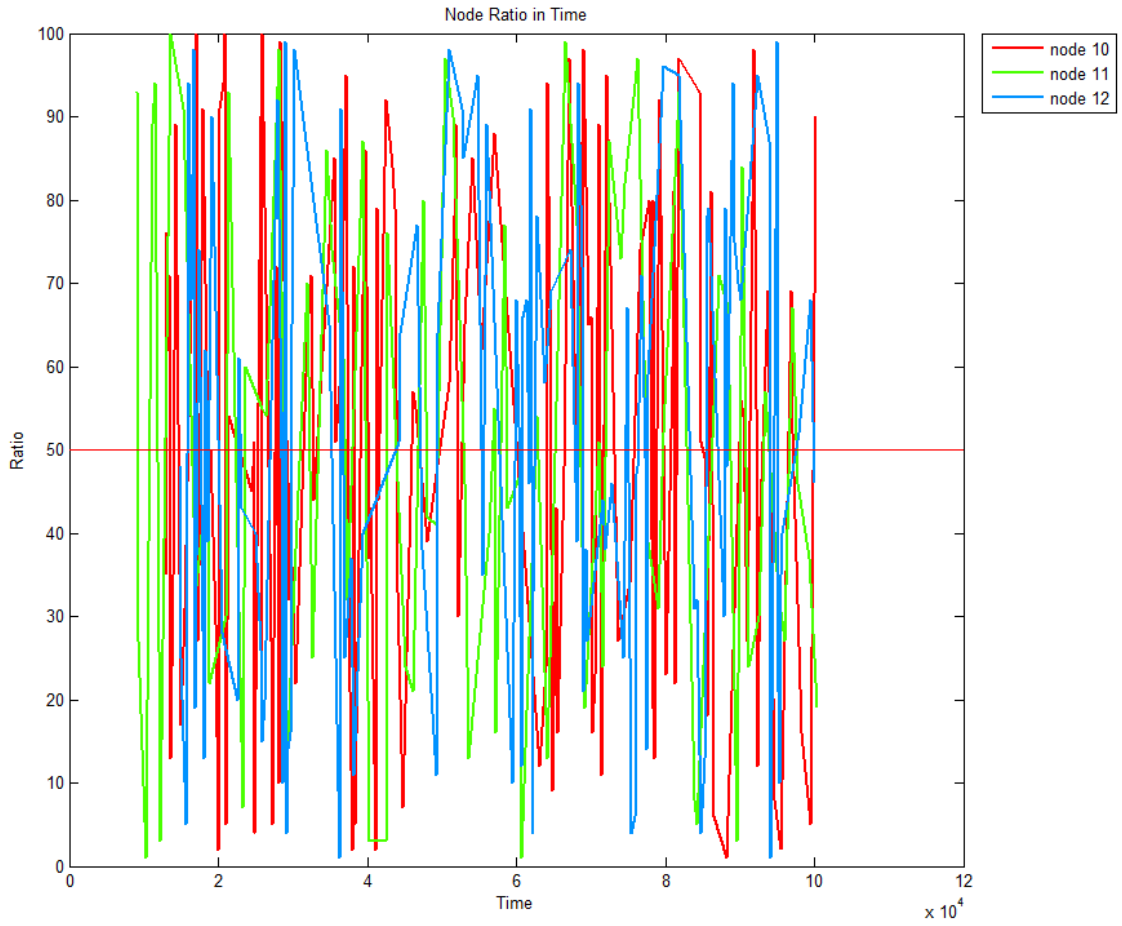




Όπως και στις προηγούμενες περιπτώσεις, το ίδιο και εδώ, ενώ φαίνεται ότι τα πακέτα προωθούνται κανονικά προς τον τελικό παραλήπτη, εντούτοις τελικά ο κόμβος 1 δεν παραλαμβάνει όλα τα πακέτα τα οποία στέλνονται από κάποιους συγκεκριμένους κόμβους.
Στην πρώτη γραφική παράσταση, φαίνεται ότι οι κόμβοι 10,11 και 12 στέλνουν ένα αρκετά μεγάλο αριθμό πακέτων, κάτι που θα μπορούσε να θεωρηθεί πως οφείλεται και στα πακέτα που φτάνουν και από άλλους κόμβους. Όσο αφορά τους υπόλοιπους κόμβους, αυτοί στέλνουν περίπου τον ίδιο αριθμό από πακέτα, μεταξύ τους. Εντούτοις, ο αριθμός των πακέτων που λαμβάνει ο sink node, από κόμβους που χρησιμοποιούν τους τρεις κακόβουλους κόμβους ως ενδιάμεσους κόμβους για να στείλουν τα πακέτα τους στον τελικό τους προορισμό, μειώνεται πάρα πολύ, σε σχέση με τον αρχικό.



Για να φανούν ακόμα πιο ξεκάθαρα οι παρατηρήσεις της προηγούμενης γραφικής παράστασης παρουσιάζεται η παρούσα.
Σε αυτό το σενάριο, η γραφική παράσταση που προκύπτει από τα αποτελέσματα κατά την προσομοίωση του ιού, δείχνει πως οι κόμβοι οι οποίοι δεν καταφέρνουν και σε αυτή την περίπτωση να προωθήσουν τα πακέτα τους στον κόμβο 1, είναι αυτοί που έχουν ως γονείς τους, τους κακόβουλους κόμβους.
Συγκρίνοντας με το αρχικό σενάριο όπου δεν υπάρχουν καθόλου κακόβουλοι κόμβοι, υπάρχει αρκετή διαφορά ως προς τον αριθμό των πακέτων που χάνονται σε αυτή την περίπτωση.



Η συγκεκριμένη γραφική παράσταση, επίσης παρουσιάζει , όπως και στις προηγούμενες δύο περιπτώσεις, την τιμή του ratio για τους τρεις κακόβουλους κόμβους, για κάθε χρονική στιγμή, από 0-100,000 ms.
Για κάθε χρονική στιγμή, φαίνεται αν η τιμή του ratio για κάθε κόμβο είναι μεγαλύτερη ή μικρότερη από 50.

5.2.3 Selective Forwarding Tree

Κόμβοι του δικτύου, οι οποίοι είναι μολυσμένοι από τον συγκεκριμένο ιό, έχουν την δυνατότητα να παρεμποδίζουν κάθε πακέτο να φτάσει στον τελικό του προορισμό, το οποίο φτάνει σε αυτούς, από οποιονδήποτε άλλο κόμβο.
Στην συγκεκριμένη τοπολογία δικτύου που χρησιμοποιήθηκε για την λήψη μετρήσεων, υπάρχουν τρία δέντρα. Κάθε ένας από τους κόμβους που βρίσκεται σε ένα τέτοιο δέντρο, το οποίο έχει ως ρίζα ένα κακόβουλο κόμβο, δεν καταφέρνει σε καμία χρονική στιγμή να προωθήσει το πακέτο του στον τελικό του παραλήπτη. Αυτό οφείλεται στο γεγονός ότι το πακέτο προκειμένου να φτάσει στον προορισμό του πρέπει πρώτα να περάσει από τον μολυσμένο κόμβο, ο οποίος και το καταστρέφει.
Αυτό ισχύει βέβαια για την περίπτωση όπου κανένας άλλος κόμβος δεν βρίσκεται μέσα στην εμβέλεια των κόμβων-παιδιών, οπότε η μετάβαση των πακέτων στον μολυσμένο κόμβο, είναι αναπόφευκτη.
Οπότε με αυτό τον ιό, είναι δυνατόν να μην προωθείται κανένα πακέτο προς τον τελικό του προορισμό, το οποίο περνά πρώτα από τον κακόβουλο κόμβο.

Σενάρια

Σε αυτή την περίπτωση του ιού, επίσης έγιναν κάποιες μετρήσεις, από τις οποίες προέκυψαν οι παρακάτω γραφικές παραστάσεις.

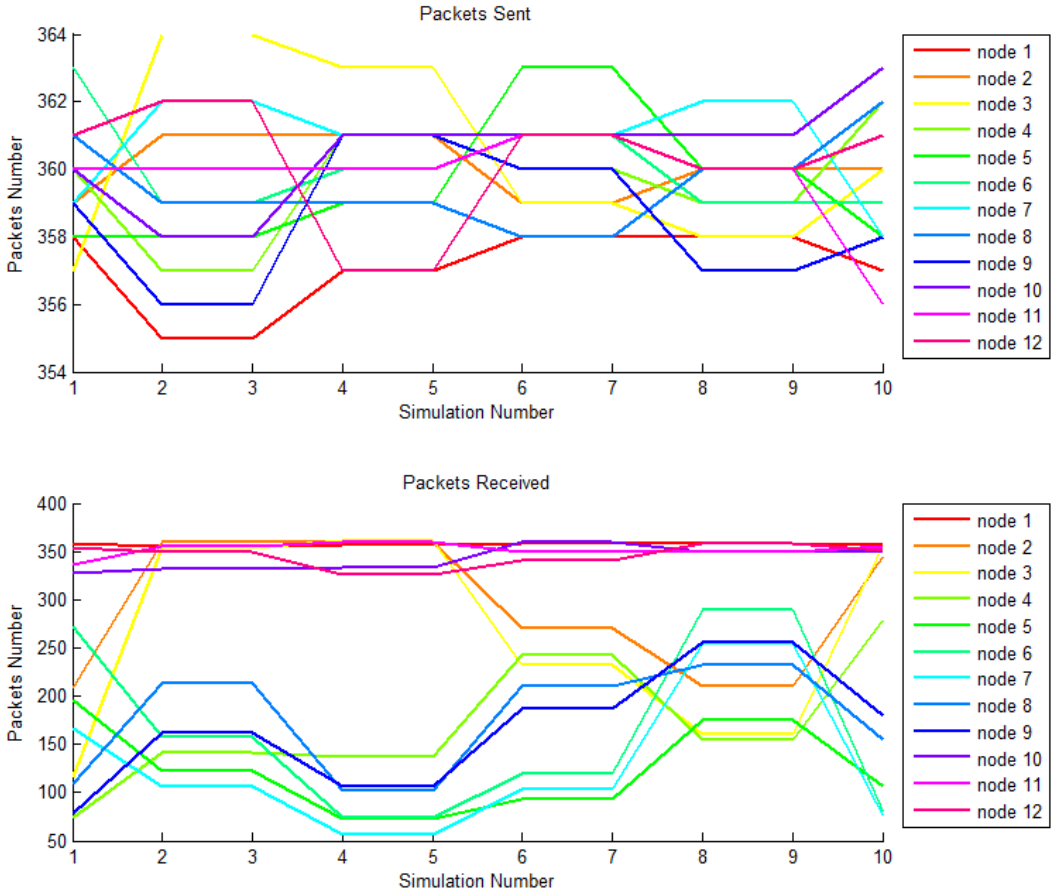
Οι γραφικές, δείχνουν τον αριθμό των πακέτων που στέλνει και λαμβάνει κάθε κόμβος μέσα στο δίκτυο, έτσι ώστε να φανεί καθαρά ο τρόπος με τον οποίο λειτουργεί ο συγκεκριμένος ιός.

Αφού ο κώδικας κάποιου από τους κόμβους, είναι μολυσμένος από τον ιό αυτό, μπορεί να μπλοκάρει κάθε πακέτο το οποίο προέρχεται από τα παιδιά του.

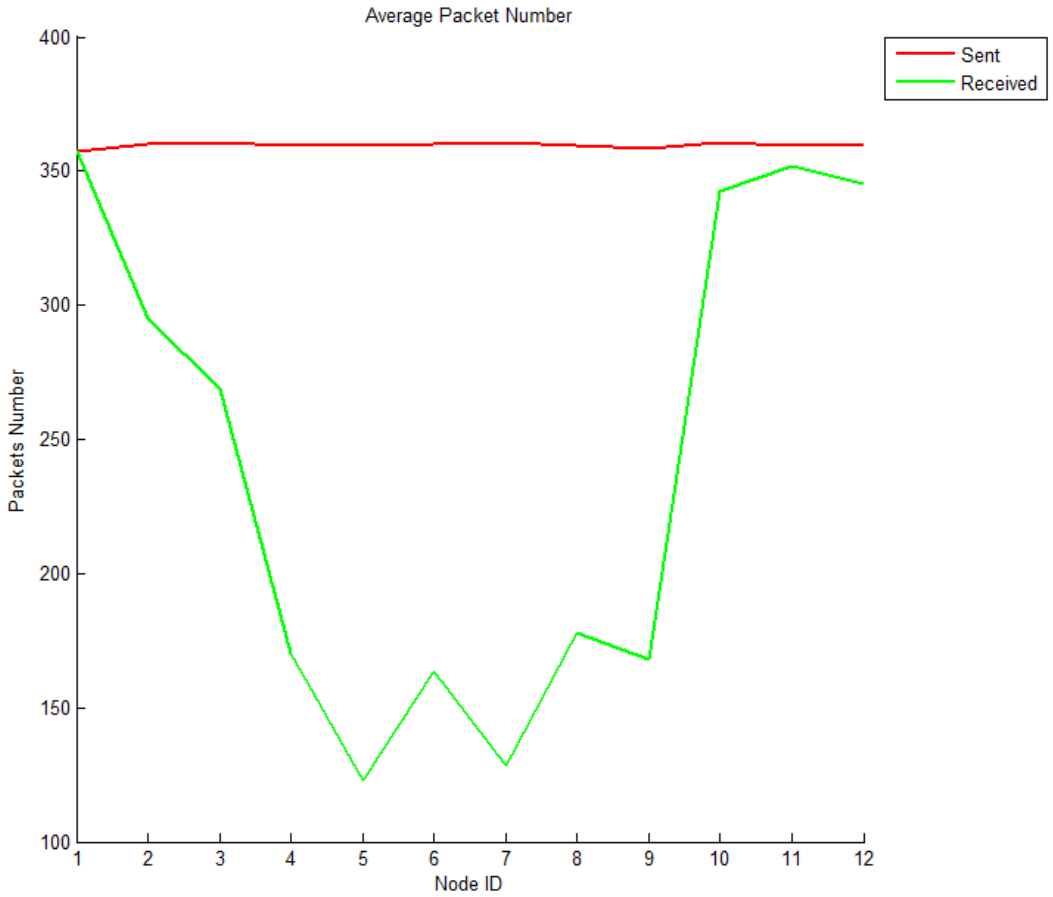
Με την δημιουργία των γραφικών που αναπαριστούν τα πακέτα που στέλνονται και λαμβάνονται, μπορεί να φανεί καθαρά ότι όντως πακέτα που στέλνονται από παιδιά κάποιου κακόβουλου κόμβου, δεν φτάνουν ποτέ στον προορισμό τους.

Στις γραφικές αυτές, φαίνεται στον άξονα y ο αριθμός των πακέτων, ενώ στον άξονα x φαίνεται ο αριθμός της προσομοίωσης. Κάθε μία από τις γραμμές της γραφικής, παρουσιάζει την συμπεριφορά του κάθε κόμβου του δικτύου.

Σενάριο 2.3.2.1
12 Benign – 0 Malicious Nodes
Τοπολογία 2.2.2.4



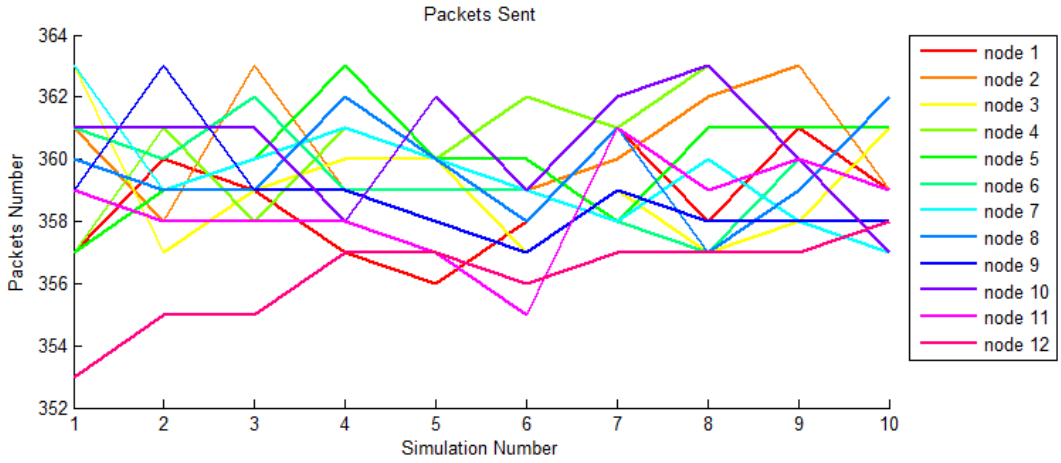
Εδώ φαίνονται τα πακέτα που κινούνται μέσα στο δίκτυο, όταν όλοι οι κόμβοι του δικτύου είναι υγιείς. Παρατηρείται πως αν και με απώλειες πακέτων, εντούτοις είναι δυνατόν να φτάνουν μερικά πακέτα στον κόμβο 1, από όλους τους κόμβους.

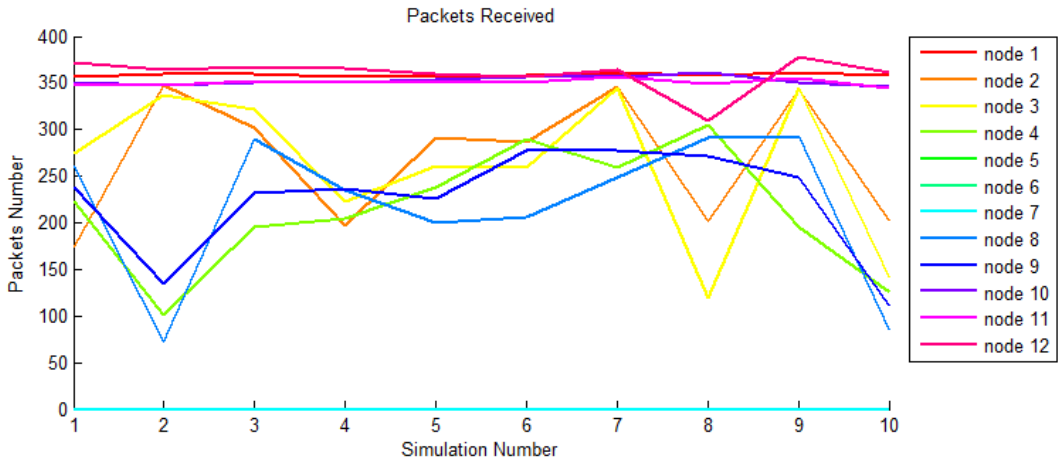


Μια καλύτερη αναπαράσταση του σεναρίου που δείχνει πιο ξεκάθαρα ποια είναι η συμπεριφορά των κόμβων μέσα στο δίκτυο όταν σε αυτό δεν υπάρχει κανένας κακόβουλος κόμβος.

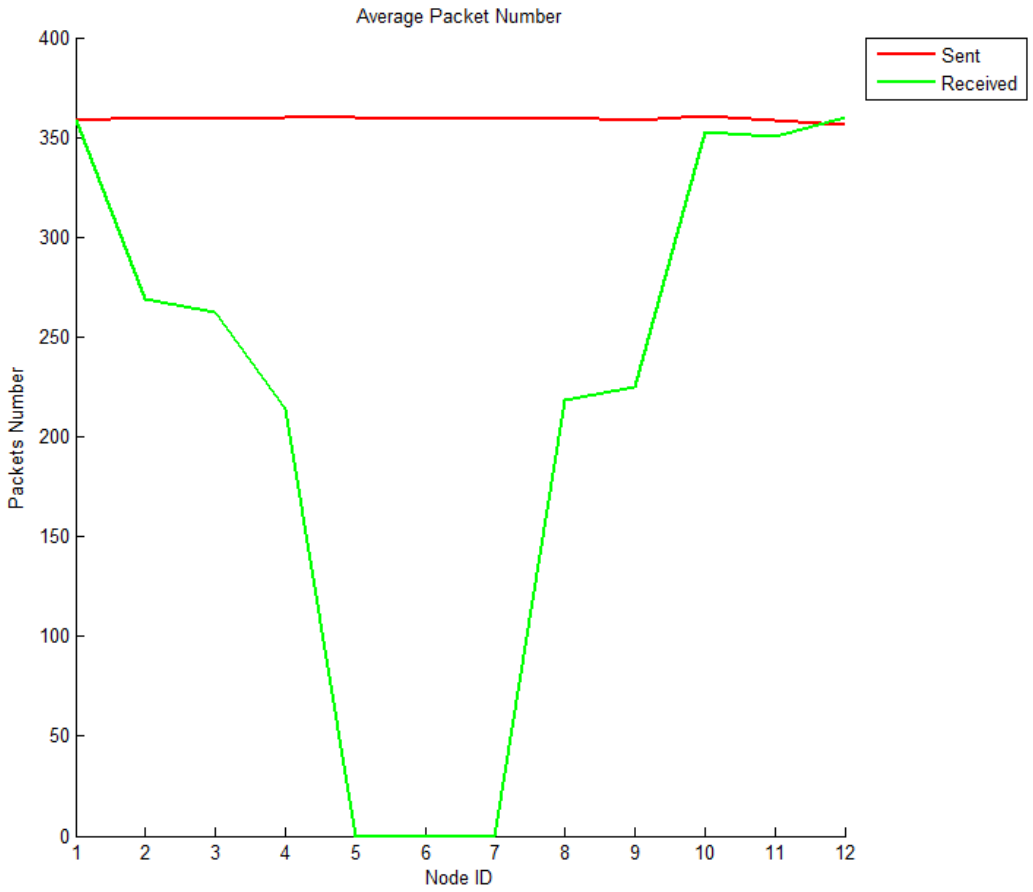
Όπως και στις προηγούμενες περιπτώσεις, παρατηρείται και σε αυτή την περίπτωση κάποια απώλεια πακέτων, ίσως από συγκρούσεις μεταξύ των πακέτων που κινούνται μέσα στο δίκτυο.
Ο μέσος όρος των πακέτων που παραλαμβάνει ο τελικός παραλήπτης από τον κάθε κόμβο και στους τρεις ιούς Selective Forwarding, είναι παρόμοιος, και κατά συνέπεια τα σχήματα των γραφικών για αυτά τα σενάρια φαίνονται πολύ παρόμοια.

Σενάριο 2.3.2.2
11 Benign – 1 Malicious Nodes
Τοπολογία 2.3.2.2



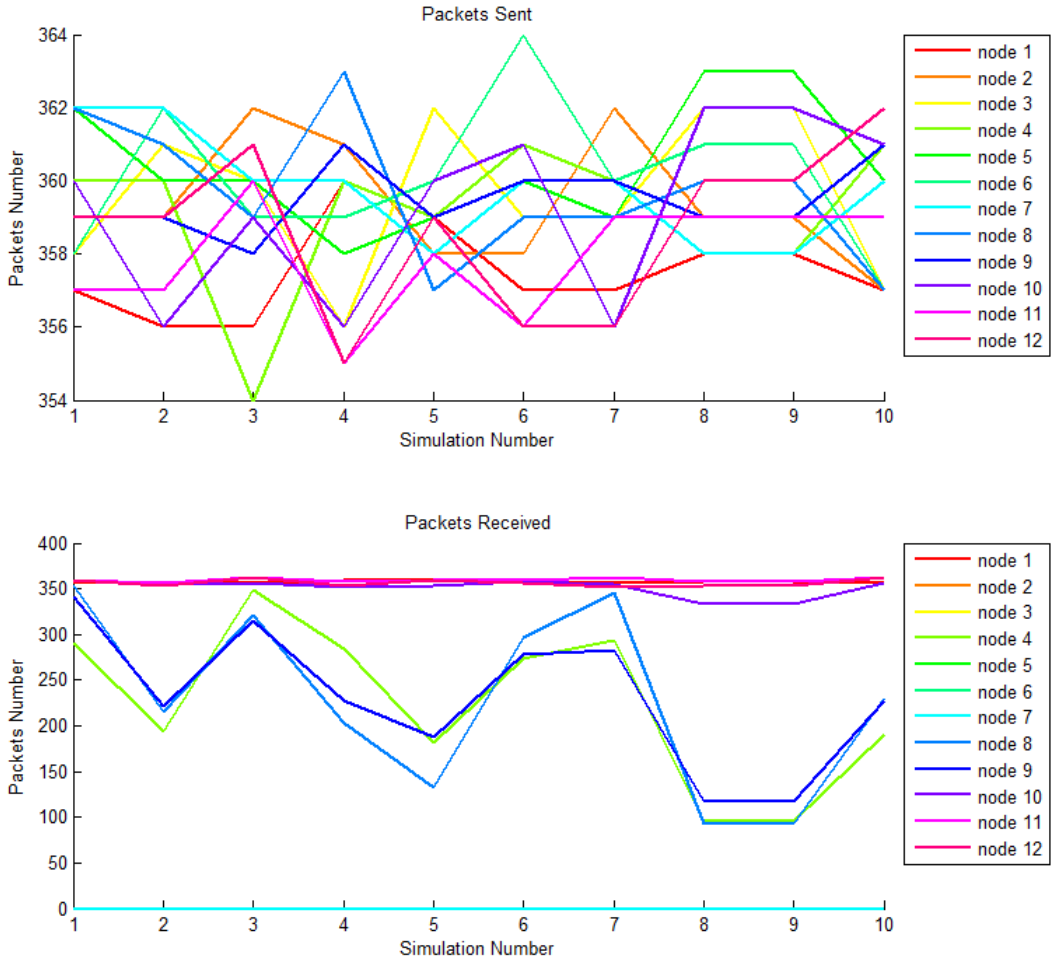


Στην πρώτη γραφική παράσταση παρουσιάζεται ο αριθμός των πακέτων που στέλνονται από κάθε κόμβο, προς τον τελικό παραλήπτη, και στην δεύτερη γραφική παράσταση, παρουσιάζεται ο αριθμός των πακέτων που λαμβάνει ο κόμβος 1 από κάθε ένα από τους υπόλοιπους κόμβους τους δικτύου.
Όπως παρατηρείται, οι κόμβοι-παιδιά του κακόβουλου κόμβου, δεν καταφέρνουν να προωθήσουν κανένα από τα πακέτα τους στον τελικό παραλήπτη, αφού αυτά καταστρέφονται από τον γονέα τους. Τα πακέτα δηλαδή, από τους κόμβους 5,6 και 7 δεν φτάνουν ποτέ στον τελικό τους προορισμό.

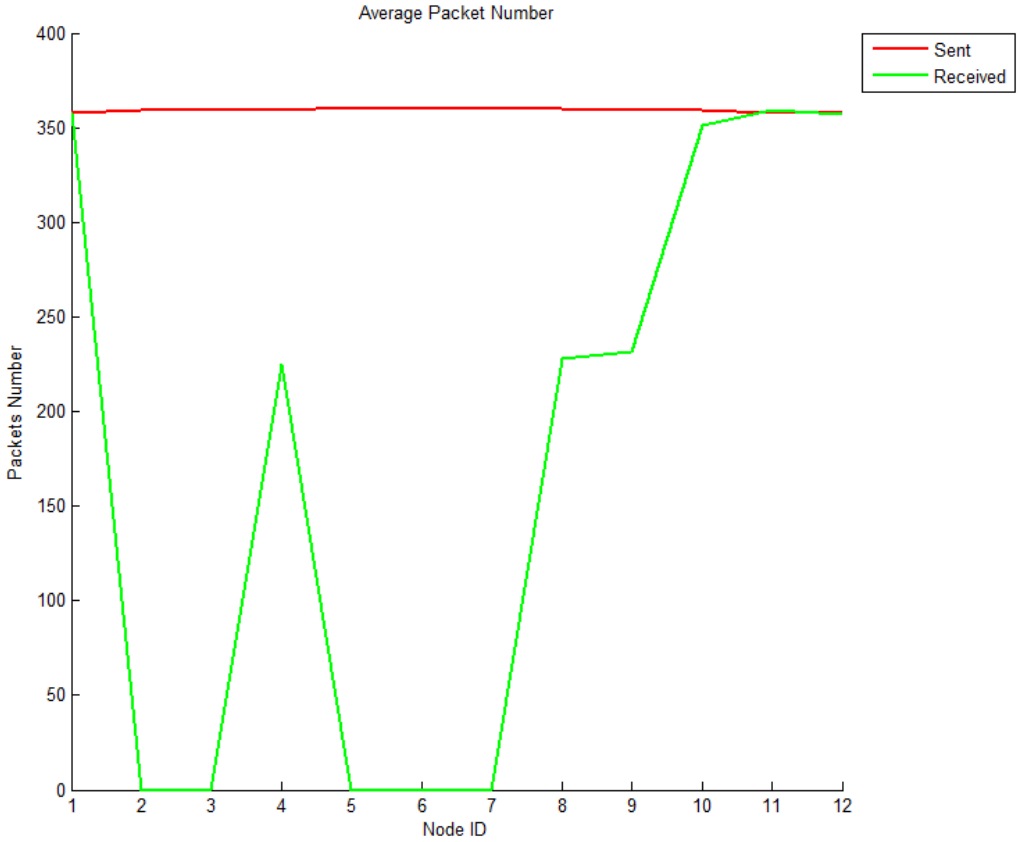


Το συγκεκριμένο διάγραμμα δίνει μια καλύτερη αναπαράσταση του τρόπου με τον οποίο συμπεριφέρονται οι κόμβοι μέσα στο δίκτυο. Φαίνεται καθαρά ότι ο μέσος όρος των πακέτων που καταφέρνουν οι κόμβοι παιδιά του μολυσμένου κόμβου να προωθήσουν στον τελικό προορισμό είναι 0.

Σενάριο 2.3.2.3
10 Benign – 2 Malicious Nodes
Τοπολογία 2.3.2.3



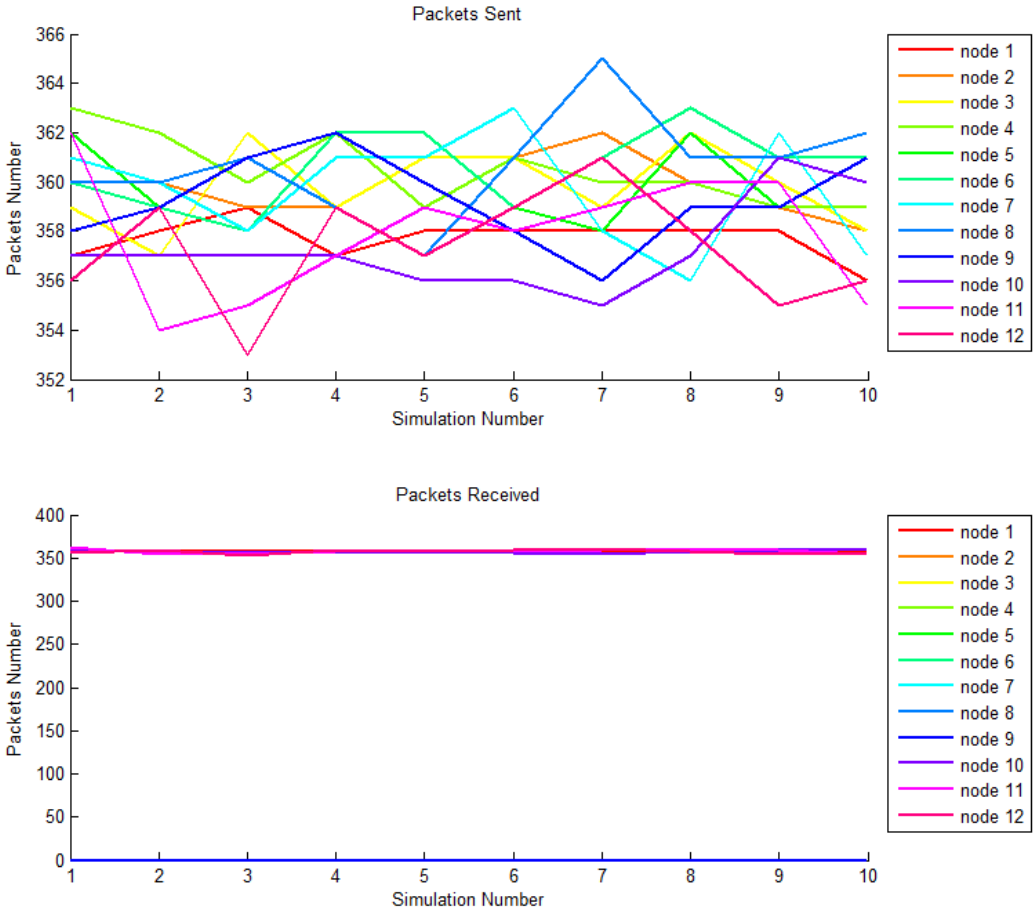
Σε αυτό το σενάριο, υπάρχουν δύο κακόβουλοι κόμβοι, οι οποίοι μπλοκάρουν εντελώς τα πακέτα που φτάνουν από τα παιδιά τους, χωρίς να τα προωθούν προς τον τελικό τους παραλήπτη.
Συγκεκριμένα, στην δεύτερη γραφική παράσταση, φαίνεται ότι ο κόμβος 1 δεν λαμβάνει καθόλου πακέτα από τους κόμβους 2,3,5,6 και 7



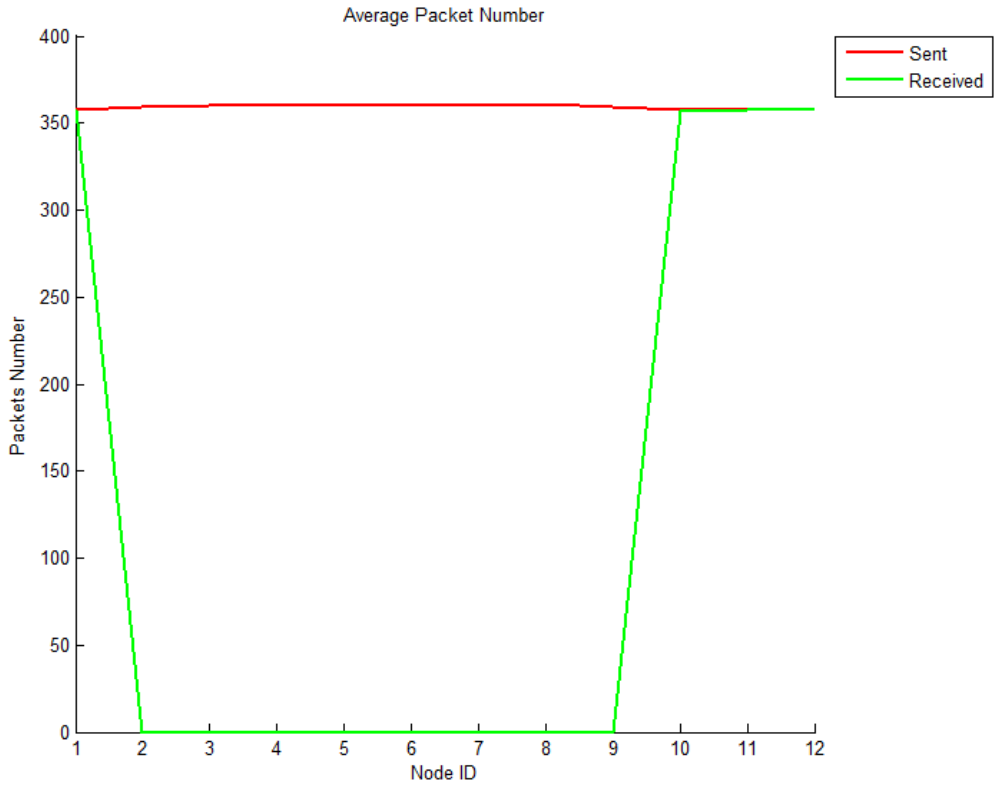
Το ίδιο με το προηγούμενο σενάριο συμβαίνει και εδώ, όπου τα πακέτα τα οποία έχουν ως αποστολείς τους κόμβους 2,3,5,6 και 7, δεν καταφέρνουν να φτάσουν ποτέ στον κόμβο 1 ο οποίος είναι ο τελικός τους προορισμός, και αυτό γιατί χρησιμοποιούν σαν ενδιάμεσους κόμβους για την δρομολόγηση των πακέτων τους, κάποιους κακόβουλους.

Σε αυτή την γραφική παρουσιάζεται η συμπεριφορά των κακόβουλων κόμβων ως προς τα παιδιά τους για όλες τις προσομοιώσεις που έγιναν.

Σενάριο 2.3.2.4
9 Benign – 3 Malicious Nodes
Τοπολογία 2.3.2.4



Αυτή η περίπτωση, είναι η χειρότερη περίπτωση σεναρίου, όπου ουσιαστικά έχουμε 3 κακόβουλους κόμβους, οι οποίοι μπλοκάρουν τα πακέτα που προέρχονται από όλους τους υπόλοιπους κόμβους του δικτύου (εκτός από τον κόμβο 1 που είναι ο παραλήπτης).
Συγκεκριμένα πακέτα φτάνουν μόνο από τους κακόβουλους κόμβους.



Η γραφική αυτή παρουσιάζει πολύ πιο καθαρά από την προηγούμενη το μέγεθος του προβλήματος που μπορεί να προκαλέσει ένας τέτοιος ιός σε ένα δίκτυο.
Είναι πολύ ξεκάθαρο ότι το συγκεκριμένο δίκτυο έχει επηρεαστεί σε μεγάλο βαθμό από κάποιον κακόβουλο ιό.
Κανένα πακέτο από κανένα κόμβο δεν φτάνει στον κόμβο 1 παρά μόνο τα πακέτα που δημιουργούνται στους κακόβουλους κόμβους.

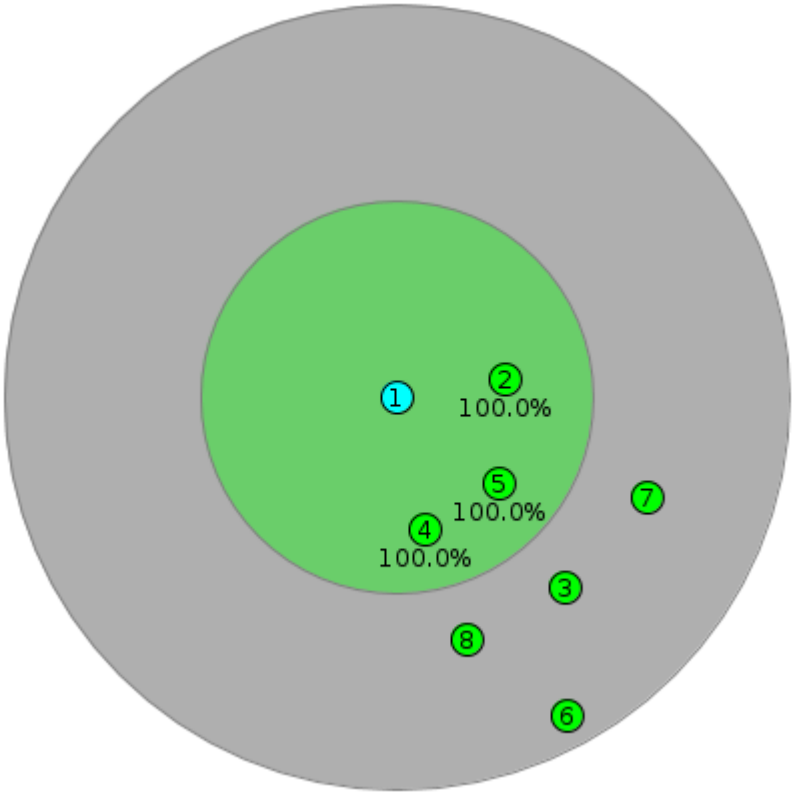
5.3 Black Hole

Οι γραφικές οι οποίες εμφανίζονται παρακάτω, παρουσιάζουν τα αποτελέσματα τα οποία προκύπτουν από ένα mesh δίκτυο, του οποίου οι κόμβοι μολύνονται από ένα ιό Black Hole.
Οι κόμβοι οι οποίοι είναι μολυσμένοι από τον συγκεκριμένο ιό, αυτό που προσπαθούν να κάνουν είναι να καταφέρουν να προσελκύσουν όλα τα πακέτα τα οποία μεταδίδει κάθε κόμβος μέσα στο δίκτυο, και που έχει σαν τελικό προορισμό, τον κόμβο 1.
Ο τρόπος με τον οποίο καταφέρνει να προσελκύσει κάθε πακέτο το οποίο κινείται μέσα στο δίκτυο, είναι διαφημίζοντας ένα χαμηλό κόστος δρομολόγησης, ίσως χαμηλότερο από τον κόμβο 1, έτσι ώστε να 'ξεγελά' τους υπόλοιπους κόμβους, παρουσιάζοντας τον εαυτό του ως τον τελικό παραλήπτη.
Συγκεκριμένα, το κόστος δρομολόγησης το οποίο παρουσιάζει ο μολυσμένος κόμβος, σχετίζεται με τον αριθμό των Hops, όπου στέλνει με μια απάντηση σε μια αίτηση που δέχεται από τους υπόλοιπους κόμβους, πως αυτός έχει το χαμηλότερο κόστος δρομολόγησης προς τον τελικό παραλήπτη, οπότε όλοι οι υπόλοιποι κόμβοι πιστεύουν πως αυτός είναι ο κόμβος είναι ο sink.
Αυτό ισχύει για την συγκεκριμένη υλοποίηση του ιού, άλλες υλοποιήσεις μπορεί να είναι διαφορετικές, αλλά να ακολουθούν την ίδια λογική.

<u>Σενάρια</u>

Οι γραφικές οι οποίες παρουσιάζονται στην συνέχεια, προέκυψαν από τρία διαφορετικά σενάρια, όπου στο πρώτο αναπαρίσταται ένα δίκτυο με 8 υγιείς κόμβους, στο δεύτερο υπάρχει ένας κακόβουλος κόμβος και στο τρίτο υπάρχουν 2 κακόβουλοι.
Συγκεκριμένα, παρουσιάζονται τα πακέτα που λαμβάνει ο κάθε κόμβος, σε κάθε προσομοίωση που γίνεται. Με αυτό τον τρόπο παρουσιάζεται ο αριθμός των πακέτων που λαμβάνει ο κάθε κόμβος μέσα στο δίκτυο, δείχνοντας έτσι ότι σε περίπτωση που παρουσιαστεί ένας κακόβουλος μέσα στο δίκτυο, τότε ο κακόβουλος κόμβος θα έχει τα περισσότερα πακέτα να καταλήγουν σε αυτόν.
Στις παρακάτω γραφικές παρουσιάζεται ο αριθμός της προσομοίωσης για κάθε σενάριο στον άξονα x, ενώ στον άξονα y παρουσιάζεται ο αριθμός των πακέτων για κάθε κόμβο στην συγκεκριμένη προσομοίωση.

Σενάριο 3.1
8 Benign – 0 Malicious Nodes

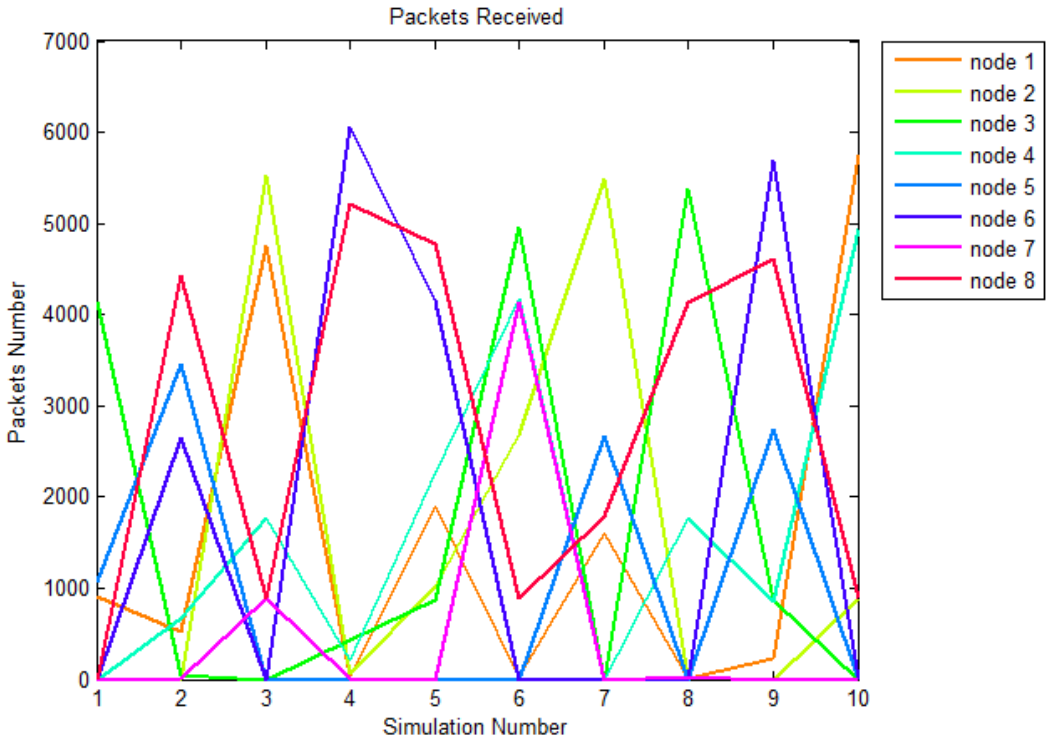


Τοπολογία 3.1

Στην πιο πάνω τοπολογία, υπάρχουν 8 καθαροί κόμβοι, οι οποίοι αποτελούν ένα mesh δίκτυο. Το δίκτυο αυτό αποτελεί το σενάριο βάση για σύγκριση των αποτελεσμάτων των επόμενων σεναρίων με τα αποτελέσματα του συγκεκριμένου, για να προκύψουν κάποια συμπεράσματα.

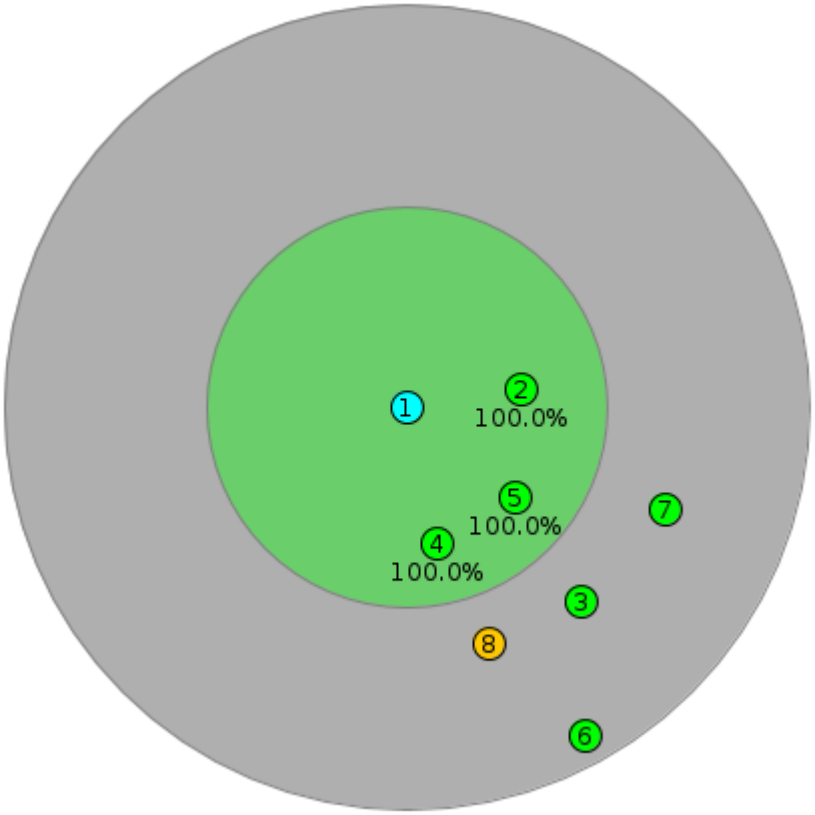
Βασική προϋπόθεση για να λειτουργήσει σωστά ο συγκεκριμένος ιός, είναι ο κακόβουλος κόμβος να βρίσκεται 2 Hops μακριά από τον τελικό παραλήπτη.

Σενάριο 3.1
8 Benign – 0 Malicious Nodes
Τοπολογία 3.1



Στην συγκεκριμένη γραφική παράσταση, φαίνεται ο αριθμός των πακέτων που λαμβάνει κάθε ένας από τους κόμβους μέσα στο δίκτυο. Παρατηρείται ότι όλοι οι κόμβοι παραλαμβάνουν παρόμοιο αριθμό πακέτων, αφού ακόμα δεν υπάρχει κάποιος κακόβουλος κόμβος ο οποίος να μπορεί να συγκεντρώνει όλα τα πακέτα που στέλνονται μέσα στο δίκτυο.
Βέβαια υπάρχουν και κάποιες εξαιρέσεις σε ορισμένα σενάρια.

Σενάριο 3.2
7 Benign – 1 Malicious Nodes



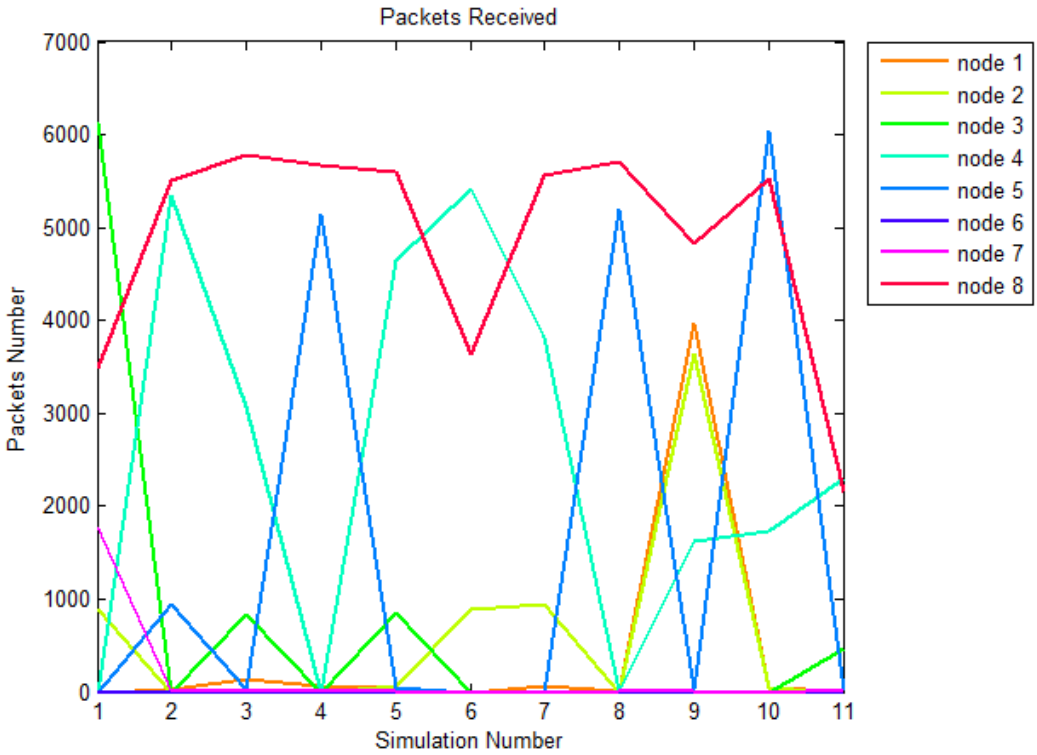
Τοπολογία 3.2

Στην τοπολογία αυτή, υπάρχει τώρα ένας κακόβουλος κόμβος , ο οποίος επηρεάζει ολόκληρο το δίκτυο, παρουσιάζοντας τον εαυτό του σαν sink. Μπορεί λοιπόν να προσελκύσει πακέτα από κόμβο ο οποίος βρίσκεται μέχρι και 3 Hops μακριά από αυτόν.

Η απόσταση αυτή καθορίζεται μέσα στον κώδικα. Μπορεί ο κακόβουλος κόμβος να επηρεάσει από 1 μέχρι και όλους τους κόμβους του δικτύου, πείθοντάς τους να του στέλνουν όλοι τα πακέτα τους.

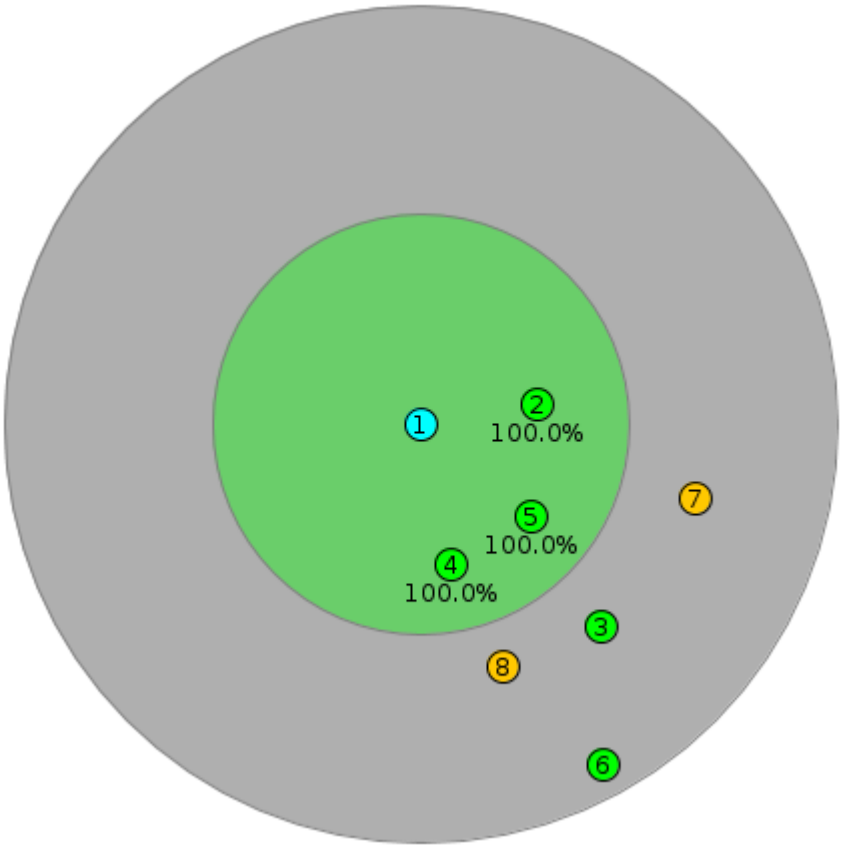
Στον κώδικα αυτό, μπορεί να πραγματοποιηθεί θέτοντας στην τιμή των hops που παρουσιάζει ο κακόβουλος κόμβος, αρνητική, οπότε με αυτό τον τρόπο, ανάλογα με το πόσο μεγάλη θέλουμε να είναι η εμβέλεια στην οποία θα έχει επίδραση ο κακόβουλος, ρυθμίζουμε και αυτή την τιμή.

Σενάριο 3.2
7 Benign – 1 Malicious Nodes
Τοπολογία 3.2



Σε αυτό το σενάριο, ο κόμβος 8, ο οποίος είναι ο κακόβουλος κόμβος, συγκεντρώνει τον μεγαλύτερο αριθμό πακέτων, σε όλες τις προσομοιώσεις σχεδόν.
Ο λόγος για τον οποίο οι κόμβοι 4 και 5, παρουσιάζεται επίσης πως λαμβάνουν ένα πολύ μεγάλο αριθμό πακέτων, οφείλεται στο ότι αυτοί λειτουργούν ως ενδιάμεσοι κόμβοι, προκειμένου να προωθήσουν τα πακέτα που φτάνουν από άλλους κόμβους, και έχουν σαν προορισμό τους τον κακόβουλο κόμβο.
Όπως φαίνεται και από τη τοπολογία του δικτύου, ο κόμβος 5 μπορεί να λάβει ένα πολύ μεγάλο αριθμό από πακέτα, λόγω της θέσης του. Όλα τα πακέτα που στέλνονται από τους υπόλοιπους κόμβους του δικτύου, έχουν σαν τελικό προορισμό τον κόμβο 1, όμως δεν καταφέρνουν ποτέ τα πακέτα να φτάσουν σε αυτό, αφού όλοι οι κόμβοι έχουν σαν επόμενο κόμβο για την προώθηση των πακέτων τους, τον κακόβουλο κόμβο. Οπότε όλα καταλήγουν σε αυτόν και κανένας άλλος δεν έχει την δυνατότητα να προωθήσει τα πακέτα σε κάποιον άλλο κόμβο προκειμένου αυτά να φτάσουν στον προορισμό τους.
Συγκρίνοντας τον αριθμό των πακέτων που μπορεί να παραλάβει ο κόμβος 1, με τα πακέτα που παραλαμβάνουν οι υπόλοιποι κόμβοι, είναι αμελητέος. Αυτό συμβαίνει γιατί όλοι οι κόμβοι λειτουργούν στην ουσία ως ενδιάμεσοι κόμβοι προκειμένου τα πακέτα να φτάσουν όλα στον κακόβουλο κόμβο.

Σενάριο 3.3
6 Benign – 2 Malicious Nodes

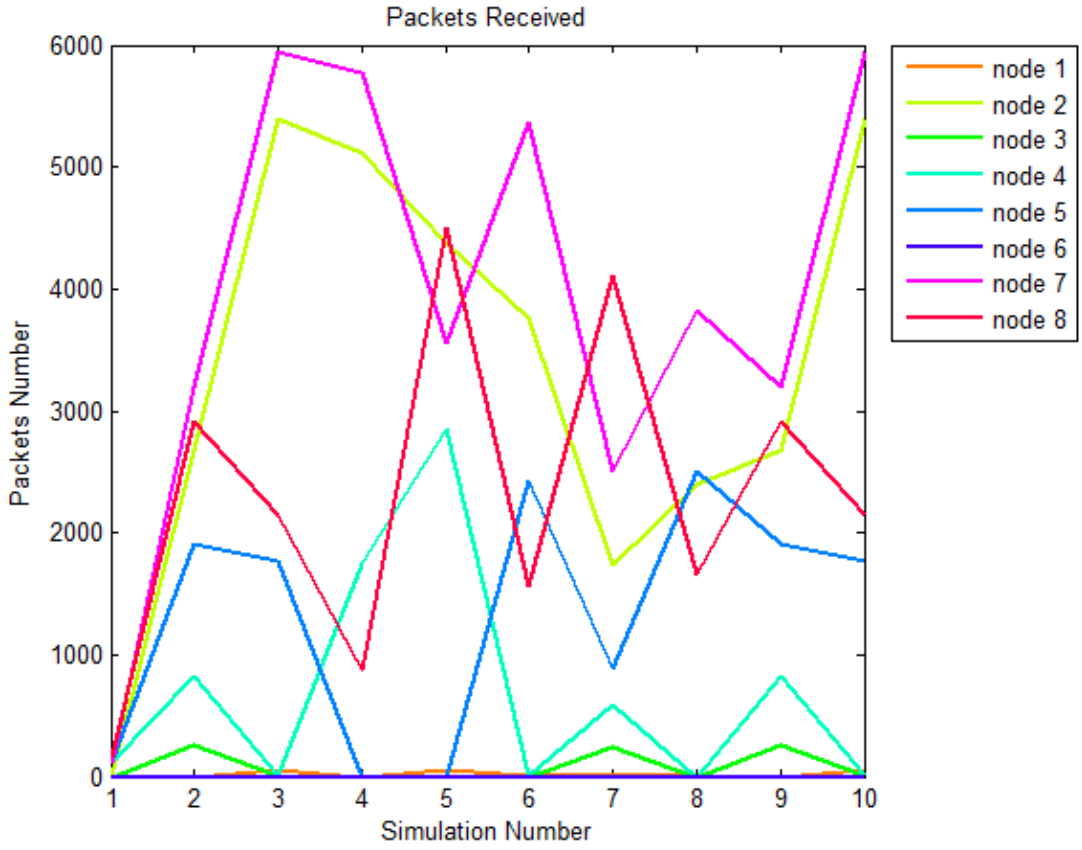


Τοπολογία 3.3

Σε αυτό το σημείο, υπάρχουν 2 κακόβουλοι κόμβοι μέσα στο δίκτυο. Με αυτό τον τρόπο, είναι δυνατόν να επηρεάζεται ένα ακόμα μεγαλύτερο μέρος του δικτύου, σε περίπτωση που ένας κακόβουλος κόμβος δεν μπορεί να καλύψει ολόκληρο το δίκτυο.

Έτσι πολλά από τα πακέτα τα οποία δεν μπορεί ο κόμβος 8 να προσελκύσει, όπως στο προηγούμενο σενάριο, καταφέρνει να τα παραλάβει ο κόμβος 7, κάνοντας ότι ακριβώς και ο κόμβος 8, παρουσιάζει δηλαδή ένα πολύ καλύτερο κόστος δρομολόγησης, ξεγελώντας τους υπόλοιπους κόμβους μέσα στο δίκτυο.

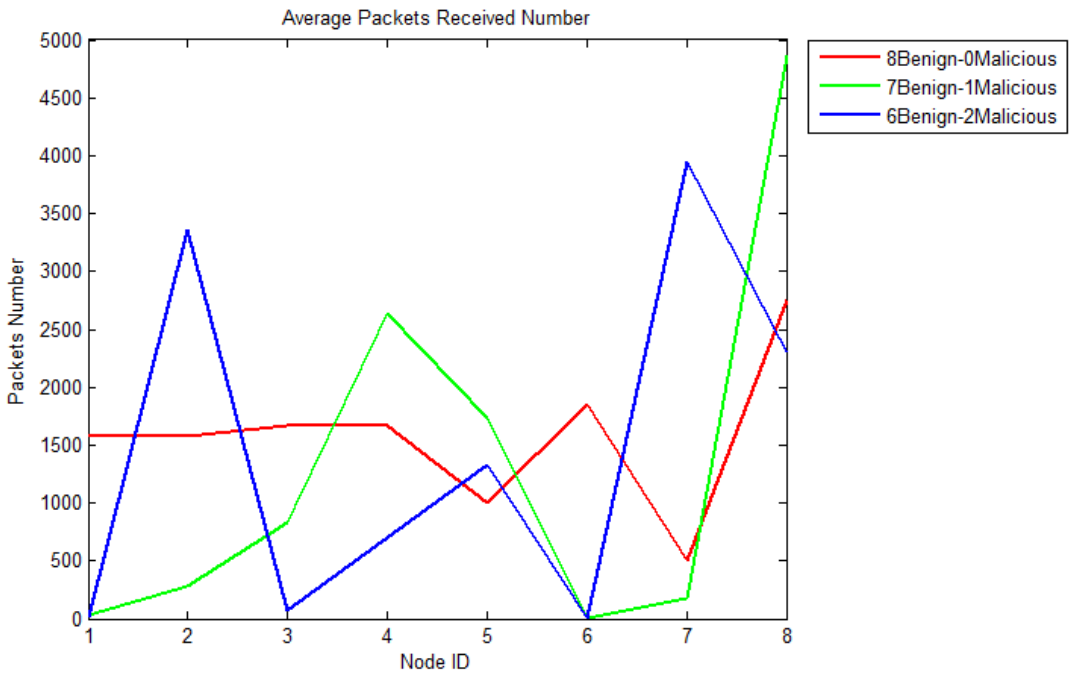
Σενάριο 3.3
6 Benign – 2 Malicious Nodes
Τοπολογία 3.3



Σε αυτή την περίπτωση, οι κακόβουλοι κόμβοι, είναι οι κόμβοι 7 και 8 , οι οποίοι όπως παρουσιάζεται και από την γραφική παράσταση λαμβάνουν ένα πολύ μεγάλο αριθμό από πακέτα.

Στους κόμβους 7,8 και 2, μαζεύονται τα περισσότερα πακέτα, αυτό συμβαίνει γιατί ο κόμβος 2 λειτουργεί ως ενδιάμεσος κόμβος, προωθώντας όλα τα πακέτα στους δύο κακόβουλους κόμβους.

Οι υπόλοιποι κόμβοι έχουν επίσης ένα πολύ μεγάλο αριθμό από πακέτα και αυτό συμβαίνει για τους ίδιους λόγους που αναφέρθηκαν πιο πάνω, στην προηγούμενη γραφική. Και πάλι ο κόμβος 1, παραλαμβάνει ένα πολύ μικρό αριθμό πακέτων, κάτι το οποίο οφείλεται στο ότι αρχικά ορισμένοι κόμβοι, στέλνουν τα πακέτα τους στον 1, αφού δεν έχουν παραλάβει ακόμα την διαφήμιση για το πολύ χαμηλότερο κόστος δρομολόγησης που φαίνεται να έχουν οι κακόβουλοι κόμβοι.



Στην πιο πάνω γραφική παράσταση, φαίνεται για κάθε ένα από τα τρία σενάρια ο μέσος όρος των πακέτων που λαμβάνει ο κάθε κόμβος. Σε αυτή την γραφική, στον άξονα x βρίσκονται οι αριθμοί που αντιστοιχούν σε κάθε κόμβο, ενώ στο κόμβο y βρίσκεται ο αριθμός των πακέτων.
Στο σενάριο όπου υπάρχουν 8 υγιείς κόμβοι, παρατηρείται μια σταθερότητα στον αριθμό των πακέτων, και για τους 8 κόμβους, με μερικές εξαιρέσεις. Ακολούθως, στο σενάριο με 7 υγιείς και 1 κακόβουλο κόμβο, παρατηρείται μια μεγάλη αύξηση στον αριθμό των πακέτων για τους κόμβους 4,5 και 8, κάτι που εξηγήθηκε πιο πάνω. Τέλος όσο αφορά το τελευταίο σενάριο, υπάρχει μια αύξηση του αριθμού των πακέτων σε περισσότερους κόμβους, και συγκεκριμένα στους 2,5,7 και 8.

Βιβλιογραφία

[1] Muhammad R Ahmed, Xu Huang, and Dharmendra Sharma, *A Taxonomy of Internal Attacks in Wireless Sensor Network*, 2012

[2] Yazeed Al-Obaisat, Robin Braun, *On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management*, University of Technology, Sydney, Australia

[3] Th. Arampatzis, J. Lygeros, Senior Member, IEEE, and S. Manesis, Member, IEEE*, A Survey of Applications of Wireless Sensors and Wireless Sensor Networks*

[4] Zorana Bankovic, *Unsupervised Intrusion Detection for Wireless Sensor Networks Based on Artificial Intelligence Techiniques*, Phd Thesis, 2011

[5] Zubair A. Baig, *Distributed Denial of Service Attack Detection in Wireless Sensor Networks*, Phd Thesis, Monash University January, 2008

[6] David Boyle and Thomas Newe*, Securing Wireless Sensor Networks: Security Architectures*, University of Limerick, Limerick, Ireland, January 2008

[7] Michael Brownfield, Yatharth Gupta and Nathaniel Davis IV, *Wireless Sensor Network Denial of Sleep Attack*, June 2005

[8] Doddapaneni Chaitanya and Ghosh Arindam , *Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation,* Middlesex University

[9] Siebe Datema, *A Case Study of Wireless Sensor Network Attacks*, Master's Thesis in Computer Science, Delft University of Technology, September 2005

[10] Bhavya Daya, *Network Security: History, Importance, and Future* University of Florida

[11] Rishav Dubey, Vikram Jain, Rohit Singh Thakur and Siddharth Dutt Choubey, *Attacks in Wireless Sensor Networks,* International Journal of Scientific & Engineering Research, March 2012

[12] Adam Dunkels., Oliver Schmidt, Thiemo Voigt., Muneeb Ali., *Protothreads: Simplifying Event-Driven Programming of Memory-Constrained Embedded Systems* Swedish Institute of Computer Science

[13] Adam Dunkels, Bjorn Gronvall, Thiemo Voigt , *Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors*, Swedish Institute of Computer Science

[14] Djallel Eddine Boubiche and Azeddine Bilami, *Cross Layer Intrusion Detection System For Wireless Sensor Network*, LaSTIC Laboratory, UHL Batna, Algeria, March 2012

[15] Tanveer Zia and Albert Zomaya, *Security Issues in Wireless Sensor Networks School of Information Technologies*, University of Sydney

[16] Wassim Znaidi, Marine Minier and Jean-Philippe Babau, *An Ontology for Attacks in Wireless Sensor Networks,* Research Report, October 2008

[17] C. Karlof and D. Wagner, *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,* University of California at Berkeley

[18] Chris Karlof and David Wagner, *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,*University of California at Berkeley

[19] Tom Karygiannis and Les Owens, *Wireless Network Security 802.11, Bluetooth and Handheld Devices,* Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, 2002

[20] Al-Sakib Khan Pathan , Hyung-Woo Lee and Choong Seon Hong, *Security in Wireless Sensor Networks: Issues and Challenges*, Kyung Hee University and Hanshin University, Korea

[21] Al-Sakib Khan Pathan, *Denial Of Service In Wireless Sensor Networks: Issues And Challenges,* Kyung Hee University, 2010

[22] Ioannis Krontiris, Tassos Dimitriou, Hamed Soroush And Mastooreh Salajegheh, *WSN Link-layer Security Frameworks*, Athens Information Technology, Greece

[23] Hemanta Kumar Kalita and Avijit Kar, *Wireless Sensor Network Security Analysis,* Jadavpur University, Kolkata, India, December 2009

[24] Dr. Manoj Kumar Jain, *Wireless Sensor Networks: Security Issues and Challenges*, 2011

[25] Shio Kumar Singh, M P Singh, and D K Singh, *Routing Protocols in Wireless Sensor Networks – A Survey*, November 2010

[26] Shio Kumar Singh, M P Singh and D K Singh, *A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks,* 2011

[27] Ruggero Lanotte1 and Massimo Merro, *Semantic Analysis of Gossip Protocols for Wireless Sensor Networks*

[28] Christopher Leidigh, *Fundamental Principles of Network Security,* 2005

[29] Javier Lopez, Rodrigo Roman, and Cristina Alcaraz, *Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks,* University of Malaga Spain, 2009

[30] Robert E. Mahan, *Security in Wireless Networks*, Level One Security Essentials Practical Assignment, 2001

[31] Eric Maiwald, Network Security A Beginner's Guide, Second Edition

[32] Joseph Migga Kizza, *A Guide to Computer Network Security*, University of Tennessee-Chattanooga, 2009

[33] Prabhudutta Mohanty, Sangram Panigrahi, Nityananda Sarma and Siddhartha Sankar Satapathy, *Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey,* Journal of Theoretical and Applied Information Technology, Tezpur University, Tezpur, India

[34] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary *Wireless Sensor Network Security: A Survey* Wayne State University

[35] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler, *SPINS: Security Protocols for Sensor Networks,* University of California, Berkeley, 2002

[36] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, *Security in Wireless Local Area Networks*, Florida Atlantic University

[37] Vishal Rathod and Mrudang Mehta, *Security in Wireless Sensor Network: A survey*, Dharmsinh Desai University

[38] David R. Raymond and Scott F. Midkiff, *Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses,* 2008

[39] K.S.Rawat and G.H.MassihaSecure, *Data Transmission Over Wireless Networks: Issues And Challenges*, University of Louisiana at Lafayette, 2003

[40] Prathiba Reddy Nalabolu, *Detecting Malicious Code In Sensor Network Applications Using Petri Nets,* Msc Thesis, Oklahoma State University, December 2007

[41] Waldir Ribeiro Pires Junior , Thiago H. de Paula Figueiredo, Hao Chi Wong and Antonio A.F. Loureiro, *Malicious Node Detection inWireless Sensor Networks,* Universidade Federal de Minas Gerais, Belo Horizonte, MG, Brazil

[42] Mohammad Saiful Islam Mamun and A.F.M. Sultanul Kabir, *Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network*, July 2010

[43] Mayank Saraogi, *Security in Wireless Sensor Networks,* University of Tennessee, Knoxville

[44] Anitha S Sastry, Shazia Sulthana and Dr. S Vagdevi, *Security Threats in Wireless Sensor Networks in Each Layer*, Global Academy of Technology, Bangalore, November 2012

[45] Kalpana Sharma and M K Ghose, *Wireless Sensor Networks: An Overview on its Security Threats*, SMIT, Sikkim, India, 2010

[46] Ritu Sharma, Yogesh Chaba and Yudhvir Singh, *Analysis of Security Protocols in Wireless Sensor Network*, University of Science & Technology, Hisar (Haryana) – India, 2010

[47] William Stallings, *Cryptography and Network Security Principles and Practise*, 5th Edition, 2011

[48] John A. Stankovic, *Wireless Sensor Networks*, University of Virginia, 2006

[49] Andreas A. Strikos , *A full approach for Intrusion Detection in Wireless Sensor Networks*, School of Information and Communication Technology, March 2007

[50] Sushma, Deepak Nandal and Vikas Nandal, *Security Threats in Wireless Sensor Networks*, May 2011

[51] Rohit Tiwari and Monika Kohli, *Security Aspects for Wireless Sensor Network*, Institute of Engg. & Tech., Vadodara, India, October 2012

[52] Llanos Tobarra, Diego Cazorlaand and Fernando Cuartero, *Security in Wireless Sensor Networks: A Formal Approach*

[53] Bonepalli Uppalaiah, Nadipally Vamsi Krishna, Renigunta Rajendher, *Layer Based Intrusion Detection System for Network Security* (LBIDS) November-2011

[54] QinghuaWang and Ilangko Balasingham, *Wireless Sensor Networks - An Introduction*

[55] QinghuaWang and Ilangko Balasingham, *Wireless Sensor Networks - An Introduction. in Book "Wireless Sensor Networks: Application-Centric Design*", Intech Publisher, edited by Geoff V Merrett and Yen Kheng Tan, December 2010

[56] Ning Xu, *A Survey of Sensor Network Applications*, University of Southern California

[57] Dr. James H. Yu & Mr. Tom K. Le, Internet and Network Security, 2001

[58] 2013.*Contiki: The Open Source Operating System for the Internet of Things*. [ONLINE] Available at: http://www.contiki-os.org/.

[59] Demand Management and Wireless Sensor Networks in the Smart Grid | InTechOpen. 2013. Demand Management and Wireless Sensor Networks in the Smart Grid | InTechOpen. [ONLINE] Available at: http://www.intechopen.com/books/energy-management-systems/demand-management-and-wireless-sensor-networks-in-the-smart-grid.

[60] *A Beginner's Guide to Network Security*, Cisco Systems, 2001