Ατομική Διπλωματική Εργασία

ΑΠΟΚΑΤΑΣΤΑΣΗ ΚΟΜΒΟΥ ΚΑΙ ΔΙΚΤΥΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Ιωάννης Ευγενίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αποκατάσταση Κόμβου και Δικτύου στο Διαδίκτυο των Πραγμάτων

Ιωάννης Ευγενίου

Επιβλέπων Καθηγητής
Βάσσος Βασιλείου

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

Μάιος 2021

Ευχαριστίες

Ολοκληρώνοντας την διπλωματική μου εργασία θα ήθελα να ευχαριστήσω τους ανθρώπους που με στήριξαν και καθοδήγησαν στην επιτυχή πραγματοποίηση της. Το θέμα της παρούσας διπλωματικής εργασίας ήταν άγνωστο για εμένα, όμως με τις συστηματικές συμβουλές που παρέλαβα από αυτούς τους ανθρώπους κατάφερα να αναπτύξω μία ολοκληρωμένη δουλεία.

Αρχικά, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας Δρ. Βασιλείου Βάσσο, ο οποίος μου έδωσε την ευκαιρία να ασχοληθώ με αυτό το ενδιαφέρον και σημαντικό θέμα. Επιπρόσθετα, θέλω να τον ευχαριστήσω για την σπουδαία καθοδήγηση που μου παρείχε καθ' όλη την διάρκεια της διαδικασίας.

Ακόμη, θα ήθελα να ευχαριστήσω και την Δρ. Ιωάννου Χριστιάνα η οποία βρισκόταν δίπλα μου κατά την υλοποίηση της προτεινόμενης πρότασης. Οποιεσδήποτε απορίες εμφανίζονταν μου παρείχε σημαντικές πληροφορίες για την επίλυση τους. Ιδιαίτερες ευχαριστίες για την υποστήριξη της στην προγραμματιστική πτυχή της διπλωματικής μου εργασίας.

Περίληψη

Το Διαδίκτυο των Πραγμάτων είναι μία πρόσφατη σχετικά έννοια η οποία προήλθε από την ανάγκη των ανθρώπων να διευκολύνουν και να ενισχύσουν τις διαδικασίες της καθημερινότητας τους. Όμως στο Διαδίκτυο των Πραγμάτων δύναται να εμφανιστούν πολλαπλά προβλήματα στον τομέα της ασφάλειας λόγω της φύσεως του. Πολλοί εισβολείς έχουν την δυνατότητα να εκμεταλλευτούν τυχόν ευπάθειες και προβλήματα για να εκτελέσουν μία γκάμα από επιθέσεις.

Στην παρούσα διπλωματική εργασία προτείνεται μία λύση του επιπέδου αντίδρασης για αποκατάσταση κόμβου και δικτύου στο Διαδίκτυο των Πραγμάτων. Γενικότερα, προτείνεται ένας μηχανισμός αντίδρασης ο οποίος ενεργοποιείται με τον επιτυχή εντοπισμό κάποιας επίθεσης σε ένα κακόβουλο κόμβο που εμποδίζει την ομαλή προώθηση πακέτων πληροφορίας προς την κεντρική πύλη του δικτύου.

Ο πρώτος μηχανισμός είναι αυτός της επαναδρομολόγησης ο οποίος ενημερώνει τους γείτονες του κακόβουλου κόμβου με τη χρήση ενός πακέτου συνδέσμου ασφαλείας για την παρούσα κατάστασή του. Ο δεύτερος μηχανισμός είναι ο μηχανισμός της επανεκκίνησης, ο οποίος ενεργοποιείται ακριβώς μετά από τον μηχανισμό της επαναδρομολόγησης.

Στην παρούσα διπλωματική εργασία καταγράφονται τέσσερεις μετρήσεις απόδοσης για αξιολόγηση της αποτελεσματικότητας της προτεινόμενης λύσης. Γενικότερα, όλες οι μετρήσεις αφορούν τα πακέτα πληροφορίας που προωθούνται μέσα στο δίκτυο αλλά και τους χρόνους αποκατάστασης του κακόβουλου κόμβου.

Περιεχόμενα

Κεφάλαιο 1 ..... **7**
1.1 Διαδίκτυο των Πραγμάτων 7
1.2 Προβλήματα στο Διαδίκτυο των Πραγμάτων 8
1.3 Επιθέσεις στο Διαδίκτυο των Πραγμάτων 8
1.4 Ασφάλεια στο Διαδίκτυο των Πραγμάτων 9
1.5 Συνεισφορά Διπλωματικής Εργασίας 10
Κεφάλαιο 2 ..... **12**
2.1 Επισκόπηση 12
2.2 Σύστημα ανίχνευσης εισβολής 12
2.3 Υπάρχουσα πρόταση 13
2.4 Άλλες προτάσεις 15
Κεφάλαιο 3 ..... **16**
3.1 Επισκόπηση 16
3.2 Sinkhole 16
3.3 Blackhole 17
3.4 Selective Forward 18
3.4.1 Forwarding Ratio 18
3.4.2 Block Node 18
Κεφάλαιο 4 ..... **19**
4.1 Επισκόπηση 19
4.2 Πρωτόκολλο δρομολόγησης Weighted Shortest Path 20
4.3 Πρωτόκολλο κόμβου RDC ContikiMAC 21
4.4 Πρωτόκολλο κόμβου RDC Null 22
4.5 Πακέτο συνδέσμου ασφαλείας 22
4.6 Επαναδρομολόγηση 25
4.7 Επανεκκίνηση 26
4.8 Χρήση συστήματος ανιχνεύσεως εισβολής mIDS 28
4.9 Επιθέσεις μετά από καθυστέρηση 29
4.10 Μετρήσεις απόδοσης 31
Κεφάλαιο 5 ..... **32**
5.1 Επισκόπηση 32
5.2 Τοπολογία 32
5.3 Περιβάλλον COOJA και Contiki OS 33
5.4 Σενάρια αξιολόγησης 34

5.4.1 Σενάριο Benign 35
5.4.2 Σενάρια No Recovery 35
5.4.2.1 Σενάριο No Recovery Mid 36
5.4.2.2 Σενάριο No Recovery Top 36
5.4.2.3 Σενάριο No Recovery RDC Mid 37
5.4.2.4 Σενάριο No Recovery RDC Top 37
5.4.2.5 Σενάριο No Recovery delayed Mid 38
5.4.2.6 Σενάριο No Recovery delayed Top 38
5.4.2.7 Σενάριο No Recovery delayed RDC Mid 39
5.4.2.8 Σενάριο No Recovery delayed RDC Top 39
5.4.3 Σενάρια Rerouting 40
5.4.3.1 Σενάριο Rerouting Mid 40
5.4.3.2 Σενάριο Rerouting Top 41
5.4.3.3 Σενάριο Rerouting RDC Mid 41
5.4.3.4 Σενάριο Rerouting RDC Top 42
5.4.3.5 Σενάριο Rerouting delayed Mid 43
5.4.3.6 Σενάριο Rerouting delayed Top 43
5.4.3.7 Σενάριο Rerouting delayed RDC Mid 44
5.4.3.8 Σενάριο Rerouting delayed RDC Top 45
5.4.4 Σενάρια Rerouting and Reboot 45
5.4.4.1 Σενάριο Rerouting and Reboot Mid 46
5.4.4.2 Σενάριο Rerouting and Reboot Top 46
5.4.4.3 Σενάριο Rerouting and Reboot RDC Mid 47
5.4.4.4 Σενάριο Rerouting and Reboot RDC Top 48
5.4.4.5 Σενάριο Rerouting and Reboot delayed Mid 48
5.4.4.6 Σενάριο Rerouting and Reboot delayed Top 49
5.4.4.7 Σενάριο Rerouting and Reboot delayed RDC Mid 50
5.4.4.8 Σενάριο Rerouting and Reboot delayed RDC Top 50
Κεφάλαιο 6 52
6.1 Επισκόπηση 52
6.2 Μελλοντική Δουλειά 52
6.3 Τελικά Συμπεράσματα 54
Βιβλιογραφία 55
Παράρτημα Α 58
Παράρτημα Β 60
Παράρτημα Γ 73

Κεφάλαιο 1

Εισαγωγή

1.1 Διαδίκτυο των Πραγμάτων
1.2 Προβλήματα στο Διαδίκτυο των Πραγμάτων
1.3 Επιθέσεις στο Διαδίκτυο των Πραγμάτων
1.4 Ασφάλεια στο Διαδίκτυο των Πραγμάτων
1.5 Συνεισφορά Διπλωματικής Εργασίας

1.1 Διαδίκτυο των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων είναι μία πρόσφατη σχετικά έννοια η οποία προήλθε από την ανάγκη των ανθρώπων να διευκολύνουν και να ενισχύσουν τις διαδικασίες της καθημερινότητας τους. Αποτελεί ένα διαφοροποιημένο δίκτυο το οποίο βασίζεται σε πολλές τεχνολογίες και τρόπους επικοινωνίας.

Γενικότερα, το Διαδίκτυο των Πραγμάτων αποτελείται από συσκευές που είναι συνδεδεμένες στο διαδίκτυο και επικοινωνούν μεταξύ τους. Συνδυάζοντας αυτές τις συσκευές με αυτόνομα συστήματα, καθίσταται δυνατή η συλλογή και ανάλυση της πληροφορίας για παραγωγή διαφόρων δράσεων, με στόχο να βοηθήσει τον ενδιαφερόμενο να ολοκληρώσει συγκεκριμένη εργασία ή να μάθει μέσω κάποιας διαδικασίας. Με άλλα λόγια, το Διαδίκτυο των Πραγμάτων έχει ως στόχο να βελτιώσει την καθημερινότητα των ανθρώπων μέσω έξυπνων συσκευών όπως αισθητήρων, έξυπνων τηλεοράσεων, έξυπνων τηλεφώνων, κ.α.

Οι έξυπνες αυτές συσκευές μπορούν και να μην είναι απευθείας συνδεδεμένες στο διαδίκτυο, με αποτέλεσμα να μην υπάρχει επικοινωνία μεταξύ τους εξ αποστάσεως. Αντιθέτως, μπορούν να είναι συνδεδεμένες σε ένα τοπικό δίκτυο, όπου για να υπάρξει επικοινωνία μεταξύ τους θα πρέπει να εγκατασταθεί η κατάλληλη καλωδίωση, γνωστή και ως δομημένη καλωδίωση. Με αυτό τον τρόπο, όλες οι έξυπνες συσκευές συνδέονται σε ένα κεντρικό σημείο όπου με τη χρήση μιας κατάλληλης εφαρμογής δίνεται η δυνατότητα σε όποιον την διαθέτει να επικοινωνήσει μαζί τους.

1.2 Προβλήματα στο Διαδίκτυο των Πραγμάτων

Στο Διαδίκτυο των Πραγμάτων δύναται να εμφανιστούν πολλαπλά προβλήματα στον τομέα της ασφάλειας λόγω της φύσεως του [3].

Αρχικά, λόγω έλλειψης καθολικών προτύπων ασφαλείας, οι συσκευές που ανήκουν στο Διαδίκτυο των Πραγμάτων θα εξακολουθήσουν να κατασκευάζονται με μειωμένη ασφάλεια. Αυτό συμβαίνει διότι οι κατασκευαστές δεν έχουν πάντα την έννοια της ασφάλειας ως πρώτιστο μέλημα στη διαδικασία σχεδιασμού των συσκευών τους. Συγκεκριμένα, οι συσκευές αυτές μπορεί να έχουν αδύναμους κωδικούς πρόσβασης, προβλήματα στο υλικό, πεπαλαιωμένα λειτουργικά συστήματα και λογισμικό, ή και ακόμα μή ασφαλή αποθήκευση και μεταφορά δεδομένων.

Επιπρόσθετα, υπάρχει έλλειψη γνώσης από τους χρήστες των συγκεκριμένων συσκευών, επειδή η τεχνολογία του Διαδικτύου των Πραγμάτων είναι καινούργια για αυτούς. Αξίζει να σημειωθεί πως η μειωμένη γνώση του χρήστη για τις λειτουργίες που διαθέτουν οι έξυπνες αυτές συσκευές αποτελεί ένα από τους μεγαλύτερους κινδύνους στον τομέα της ασφάλειας. Αυτό έχει σαν αποτέλεσμα το γεγονός ότι ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στη συσκευή αυτού του χρήστη, και με αυτό τον τρόπο να εισέλθει παράνομα στο Διαδίκτυο των Πραγμάτων.

Ακόμη, έχει γνωστοποιηθεί το γεγονός ότι υπάρχουν προβλήματα ασφαλείας στην διαχείριση ενημερώσεων των συσκευών του Διαδικτύου των Πραγμάτων. Για παράδειγμα, εάν ανακαλυφθεί κάποια ευπάθεια στο λογισμικό κάποιας έξυπνης συσκευής δεν θα εγκατασταθούν αυτόματα οι απαραίτητες ενημερώσεις όπως συμβαίνει στους προσωπικούς μας υπολογιστές, με αποτέλεσμα να παραμείνει η ευπάθεια χωρίς σύντομη αντιμετώπιση. Επίσης, κατά την διάρκεια μιας ενημέρωσης η συσκευή θα στείλει το αντίγραφο της στο “cloud” και εάν η σύνδεση δεν είναι κρυπτογραφημένη ή τα αρχεία ενημέρωσης δεν προστατεύονται, ένας εισβολέας μπορεί να κλέψει ευαίσθητες πληροφορίες.

1.3 Επιθέσεις στο Διαδίκτυο των Πραγμάτων

Πολλοί εισβολείς έχουν την δυνατότητα να εκμεταλλευτούν τις ευπάθειες και τα προβλήματα που περιεγράφηκαν στο Παράρτημα 1.2 και να εκτελέσουν μία γκάμα από επιθέσεις [3]. Αναλόγως της τοποθεσίας του εκτεθειμένου κόμβου, η κεντρική πύλη μπορεί να παραλαμβάνει μέχρι και τα μισά δεδομένα [13].

Για παράδειγμα ένας εισβολέας μπορεί να εκτελέσει μια επίθεση “botnet” στις συσκευές του Διαδικτύου των Πραγμάτων, όπου δημιουργεί ένα στρατό από κακόβουλες συσκευές τις οποίες καθοδηγεί για να στείλουν χιλιάδες αιτήματα ανά δευτερόλεπτο σε κάποιο στόχο. Ο στόχος αυτός στην συνέχεια καθίσταται μη διαθέσιμος για τους χρήστες του δικτύου.

Ακόμη, κάποιος εισβολέας μπορεί να εκτελέσει επίθεση “eavesdrop” όπου κάνει κατασκοπεία ή και υποκλοπή ευαίσθητων δεδομένων, τα οποία μπορεί να χρησιμοποιήσει ενάντια του κατόχου της έξυπνης συσκευής. Επίσης, λόγω του ότι οι περισσότερες συσκευές του Διαδικτύου των Πραγμάτων απορροφούν πληροφορίες από το περιβάλλον, ένας εισβολέας μπορεί να πάρει πρόσβαση σε μια τέτοια συσκευή και να αλλοιώσει τα δεδομένα που συλλέγει, εκτελώντας μία επίθεση που επηρεάζει την ακεραιότητα των δεδομένων.

Τέλος, κάποιος εισβολέας μπορεί να σπάσει την περίμετρο ενός δικτύου με την τοποθέτηση κάποιας κακόβουλης συσκευής σε αυτό. Με την τοποθέτηση της, η συσκευή αυτή θα αντικαταστήσει την πρωτότυπη ή θα ενσωματωθεί ως μέλος μιας ομάδας για την συλλογή ή την τροποποίηση ευαίσθητων πληροφοριών. Συνεπώς, κρίνεται επιτακτική η ανάγκη για την ανάπτυξη μιας μεθοδολογίας που θα αυξάνει την άμυνα του δικτύου απέναντι σε τέτοιες επιθέσεις.

1.4 Ασφάλεια στο Διαδίκτυο των Πραγμάτων

Η ασφάλεια στο Διαδίκτυο των Πραγμάτων αποτελεί βασικό πυλώνα διασφάλισης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πόρων. Λόγω του ότι μπορεί να εκτελεστεί μία γκάμα από επιθέσεις, εξακολουθεί να υπάρχει ανάγκη για ενσωμάτωση μεθοδολογιών που μπορούν να αντιμετωπίσουν τις επιθέσεις αυτές. Υπάρχουν κυρίως τρία επίπεδα αντιμετώπισης επιθέσεων σε όλα τα πληροφοριακά συστήματα [1] [2].

Το πρώτο επίπεδο είναι το επίπεδο της αποτροπής, το οποίο μπορεί να χαρακτηριστεί ως το πιο εύκολο ως προς την πλευρά του χρήστη διότι αυτός ο τύπος ασφάλειας δεν απαιτεί τη γνώση και την τεχνολογία της κυβερνοασφάλειας που είναι απαραίτητες για τον εντοπισμό μιας εισβολής σε ένα δίκτυο. Συγκεκριμένα, πραγματοποιείται χρήση τειχών προστασίας τα οποία εφαρμόζουν ενημερώσεις κώδικα για αναγνωρισμένες ευπάθειες και έτσι μειώνεται δραματικά η πιθανότητα επιτυχούς επίθεσης. Επίσης, το συγκεκριμένο επίπεδο είναι πολύ αποτελεσματικό επειδή εάν κάποιος εισβολέας αποτραπεί από το να αποκτήσει πρόσβαση στο δίκτυο, τότε έχει περιορισμένη ευκαιρία να προκαλέσει ζημιά ή να κλέψει ευαίσθητα δεδομένα.

Το δεύτερο επίπεδο είναι αυτό της ανίχνευσης, το οποίο λαμβάνει μέτρα για τον περιορισμό των επιπτώσεων και των ζημιών που μπορεί να προκληθούν από κάποια αναπόφευκτη παραβίαση. Συγκεκριμένα, ψάχνει για σημάδια που δείχνουν ότι έχει σημειωθεί κάποιου είδους επίθεση και έτσι μπορούν να ξεκινήσουν οι διαδικασίες αντίδρασης και αποκατάστασης συμβάντων πολύ πιο γρήγορα. Ακόμη, μέσω αυτού του επιπέδου εάν πραγματοποιηθεί γρήγορη ανταπόκριση, μπορεί να εξοικονομηθεί ένα σημαντικό ποσό από χρήματα. Αξίζει να σημειωθεί πως η τοποθεσία των συστημάτων ανίχνευσης στο Διαδίκτυο των Πραγμάτων εξαρτάται από τον περιορισμό των έξυπνων συσκευών σε ενέργεια και μνήμη, καθώς και του περιβάλλοντος εγκατάστασης τους [13] [14].

Το τρίτο και τελευταίο επίπεδο είναι το επίπεδο της αντίδρασης το οποίο αναλύει τις παραβιάσεις του παρελθόντος και του παρόντος αντί να προβλέψει μελλοντικούς κινδύνους. Όταν κάποιο δίκτυο υποπέσει θύμα μιας συγκεκριμένης απειλής, οι ιδιοκτήτες του δικτύου καθορίζουν την σημαντικότητα της απειλής, αξιολογούν το ύψος της ζημιάς και εγκαθιστούν μέτρα για την αποφυγή επανάληψης ενός τέτοιου συμβάντος. Αυτό το επίπεδο ασφάλειας δύναται να θεωρηθεί ως το πιο οικονομικό διότι δεν καθίσταται αναγκαία η εγκατάσταση μηχανισμών για αντιμετώπιση κάθε είδους πιθανής απειλής.

1.5 Συνεισφορά Διπλωματικής Εργασίας

Στην παρούσα διπλωματική εργασία προτείνεται μία λύση του επιπέδου αντίδρασης για αποκατάσταση κόμβου και δικτύου στο Διαδίκτυο των Πραγμάτων.

Γενικότερα, προτείνεται ένας μηχανισμός αντίδρασης ο οποίος ενεργοποιείται με τον επιτυχή εντοπισμό κάποιας επίθεσης σε ένα κακόβουλο κόμβο που εμποδίζει την ομαλή προώθηση πακέτων πληροφορίας προς την κεντρική πύλη του δικτύου. Η μέθοδος που αναπτύχθηκε και υλοποιήθηκε, εγκαταστάθηκε σε κόμβους με περιορισμένη ενεργειακή και υπολογιστική ισχύ με την βοήθεια του προσομοιωτή Cooja ο οποίος παρουσιάζεται στο Κεφάλαιο 5.

Συγκεκριμένα, ο μηχανισμός της αντίδρασης μπορεί να χωριστεί σε δύο κύριους ξεχωριστούς μηχανισμούς. Ο πρώτος μηχανισμός είναι αυτός της επαναδρομολόγησης ο οποίος ενημερώνει τους γείτονες του κακόβουλου κόμβου με τη χρήση ενός πακέτου συνδέσμου ασφαλείας για την κατάστασή του. Με την επιτυχή λήψη του συγκεκριμένου πακέτου από τους γειτονικούς κόμβους επιτυγχάνεται η επιλογή ενός εναλλακτικού μονοπατιού για την δρομολόγηση των πακέτων προς την κεντρική πύλη το οποίο είναι ασφαλές.

Ο δεύτερος μηχανισμός είναι ο μηχανισμός της επανεκκίνησης, ο οποίος ενεργοποιείται ακριβώς μετά από τον μηχανισμό της επαναδρομολόγησης. Ο συγκεκριμένος μηχανισμός εκτελείται τοπικά και επαναφέρει τον κακόβουλο κόμβο στην αρχική και αξιόπιστη κατάσταση του. Αυτό έχει ως αποτέλεσμα η κεντρική πύλη να λαμβάνει πλέον πακέτα πληροφορίας και από αυτόν τον κόμβο ο οποίος έχει επανακτήσει την αξιοπιστία του.

Συνοπτικά, ο μηχανισμός της επαναδρομολόγησης μειώνει τον αριθμό των πακέτων που απορροφώνται από τον κακόβουλο κόμβο με αποτέλεσμα να περιορίζεται η έκταση της εισβολής μέσα στο δίκτυο. Αφετέρου, ο μηχανισμός της επανεκκίνησης αυξάνει τον αριθμό τον πακέτων που λαμβάνονται από την κεντρική πύλη, λόγω του ότι ο κακόβουλος κόμβος επαναφέρεται στην ομαλή επιθυμητή λειτουργία του.

Κεφάλαιο 2

Σχετική Δουλειά

2.1 Επισκόπηση
2.2 Σύστημα ανίχνευσης εισβολής
2.3 Υπάρχουσα πρόταση
2.4 Άλλες προτάσεις

2.1 Επισκόπηση

Σε αυτό το κεφάλαιο περιγράφεται το σύστημα ανίχνευσης που χρησιμοποιήθηκε για την επιτυχή υλοποίηση της παρούσας πρότασης. Επιπρόσθετα, παρουσιάζεται η ήδη υπάρχουσα πρόταση στην οποία στηρίχθηκε η παρούσα, καθώς και άλλες ενδιαφέρον προτεινόμενες προτάσεις.

2.2 Σύστημα ανίχνευσης εισβολής

Ένα σύστημα ανίχνευσης εισβολής αποτελείται από μια εφαρμογή λογισμικού ή συσκευή υλικού η οποία παρακολουθεί την κίνηση που υπάρχει σε ένα δίκτυο για αναζήτηση κακόβουλης συμπεριφοράς και γνωστών απειλών. Αμέσως μετά τον εντοπισμό της εισβολής στέλνονται οι ανάλογες ειδοποιήσεις στο δίκτυο.

Κακόβουλη συμπεριφορά ορίζεται ως η συμπεριφορά δικτύου που αναπτύσσεται από κόμβους που έχουν ως στόχο να διακόψουν ή και να θέσουν σε κίνδυνο την ομαλή λειτουργία ενός δικτύου [16].

Γενικότερα ο σκοπός του συστήματος ανίχνευσης εισβολής είναι να ενημερώσει ότι δύναται να πραγματοποιηθεί εισβολή στο δίκτυο. Οι πληροφορίες προειδοποίησης που παράγει περιλαμβάνουν τη διεύθυνση προέλευσης της εισβολής, τη διεύθυνση στόχου και τον τύπο υποψίας επίθεσης. Συγκεκριμένα, κάθε σύστημα ανίχνευσης εισβολής είναι προγραμματισμένο να αναλύει την κυκλοφορία και να εντοπίζει μοτίβα σε εκείνη την κίνηση που μπορεί να υποδηλώνει επιθέσεις διαφόρων ειδών.

Στην παρούσα διπλωματική εργασία πραγματοποιήθηκε χρήση του συστήματος ανίχνευσης εισβολής mIDS [15], το οποίο ανιχνεύει ανωμαλίες σε ένα δίκτυο με βάση το Binary Logistic Regression [4]. Η στατιστική αυτή τεχνική χρησιμοποιείται για πρόβλεψη της σχέσης μεταξύ μιας ανεξάρτητης και μιας εξαρτημένης μεταβλητής, όπου η εξαρτημένη μεταβλητή είναι δυαδική. Όλες οι ανεξάρτητες μεταβλητές δοκιμάζονται σε ένα μπλοκ για να εκτιμηθεί η προγνωστική τους ικανότητα και ελέγχονται για τις επιδράσεις τους σε άλλες μεταβλητές του μοντέλου.

Ακόμη, βασίζεται στο πρωτόκολλο RMT [5] το οποίο στηρίζεται σε μια ιεραρχική δομή στην οποία οι δέκτες ομαδοποιούνται σε τοπικούς τομείς και σε κάθε τομέα υπάρχει ένας ειδικός δέκτης. Ο συγκεκριμένος δέκτης είναι υπεύθυνος για την τακτική αποστολή επιβεβαιώσεων στον αποστολέα, για την επεξεργασία της αναγνώρισης από τους δέκτες στον τομέα του και για την αναμετάδοση χαμένων πακέτων στους αντίστοιχους δέκτες.

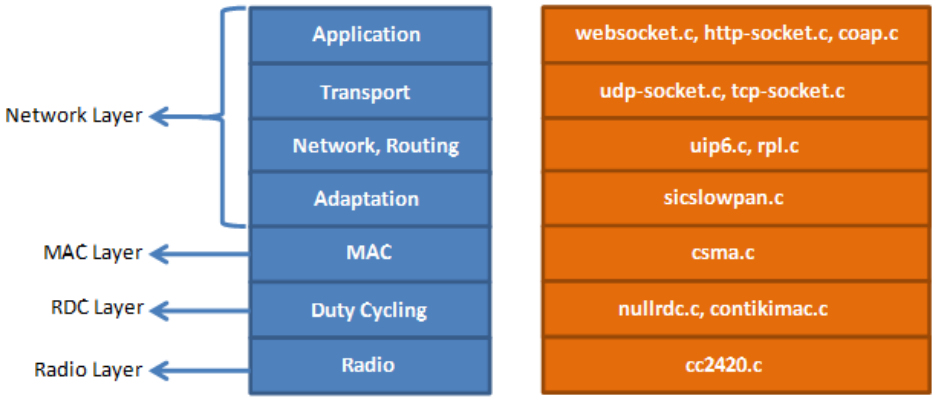
Συγκεκριμένα το σύστημα ανίχνευσης εισβολής mIDS χρησιμοποιεί καλοήθη και κακόβουλα δεδομένα που μετακινούνται μέσα στο δίκτυο για να αντλήσει τις μετρήσεις ανίχνευσης και να εντοπίσει κάποια επίθεση. Το σύστημα αυτό εκπαιδεύτηκε σε κρίσιμες επιθέσεις που μπορεί να εμφανιστούν στο Διαδίκτυο των Πραγμάτων, οι οποίες είναι οι Sinkhole, Selective Forward και Blackhole και θα αναλυθούν στο Κεφάλαιο 3. Τέλος, αξίζει να σημειωθεί πως το συγκεκριμένο σύστημα εκπαιδεύτηκε στο πρωτόκολλο κόμβου RDC ContikiMAC το οποίο θα αναλυθεί στο Κεφάλαιο 4.

Συνοψίζοντας, το σύστημα mIDS μόλις εντοπίσει κάποια κακόβουλη συμπεριφορά μέσα στο δίκτυο ενεργοποιεί τον μηχανισμό αντίδρασης που αυτός με την σειρά του αποκαθιστά τον κακόβουλο κόμβο και συνεπώς το δίκτυο.

2.3 Υπάρχουσα πρόταση

Όταν στο επίπεδο ανίχνευσης εντοπισθεί μια μη ομαλή συμπεριφορά στο δίκτυο, το επίπεδο αντίδρασης ενεργοποιείται για να επαναφέρει το δίκτυο στην αρχική του ομαλή λειτουργία. Η συγκεκριμένη μεθοδολογία μελετάται αρκετά χρόνια λόγω του ότι θεωρείται κρίσιμη στην αντιμετώπιση κακόβουλων ενεργειών στο δίκτυο .

Συνεπώς, η παρούσα διπλωματική εργασία στηρίχθηκε σε προηγούμενη μελέτη [17]. Σκοπός του συγκεκριμένου παραρτήματος είναι να παρουσιάσει εν ολίγοις την ήδη υπάρχουσα πρόταση, καθώς και πως επεκτάθηκε στην παρούσα διπλωματική εργασία.



Εικόνα 2.1: Στοίβα Contiki OS

Αρχικά, στην προηγούμενη διπλωματική εργασία αναπτύχθηκε και χρησιμοποιήθηκε το πρωτόκολλο δρομολόγησης Weighted Shortest Path για δρομολόγηση των πακέτων. Παράλληλα, αναπτύχθηκε και το πακέτο συνδέσμου ασφαλείας το οποίο προωθείτο μέσα στο δίκτυο για προκαθορισμένο χρονικό διάστημα. Επιπρόσθετα, μελετήθηκαν οι μηχανισμοί επαναδρομολόγησης και επανεκκίνησης, οι οποίοι ενεργοποιούνταν σε συγκεκριμένο χρονικό διάστημα μίας προσομοίωσης.

Στην παρούσα διπλωματική εργασία οι συγκεκριμένοι μηχανισμοί ενεργοποιούνται όταν ανακαλυφθεί μία κακόβουλη συμπεριφορά στο δίκτυο από κάποιο κόμβο μέσω του συστήματος ανίχνευσης εισβολής mIDS. Αυτό πραγματοποιείται μέσω της χρήσης και ενσωμάτωσης του συγκεκριμένου συστήματος στην πρόταση. Ακόμη, τροποποιήθηκαν τα χρονικά διαστήματα στα οποία προωθείται το πακέτο συνδέσμου ασφαλείας ούτως ώστε να είναι πιο αποδοτική η προτεινόμενη λύση.

Επίσης, στην προηγούμενη διπλωματική εργασία υλοποιήθηκαν και εκτελέστηκαν σχετικά πειράματα μόνο με χρήση σεναρίων όπου τρέχει το πρωτόκολλο κόμβου RDC ContikiMAC. Στην παρούσα διπλωματική εργασία επεκτάθηκε η συγκεκριμένη δουλειά, καθώς πραγματοποιήθηκε χρήση και του πρωτοκόλλου κόμβου RDC Null (Εικόνα 2.1).

Σημαντικό είναι ότι, στην παρούσα διπλωματική εργασία ενισχύθηκαν και οι μετρήσεις απόδοσης, καθώς λήφθηκε υπόψη και το ποσοστό επιτυχούς αποκατάστασης. Παράλληλα, εκτελέστηκαν και πειράματα όπου ο κακόβουλος κόμβος διεξήγαγε επίθεση Selective Forward Block Node για περαιτέρω αξιολόγηση της προτεινόμενης λύσης. Τέλος, στην παρούσα διπλωματική εργασία αναπτύχθηκαν και σενάρια στα οποία ο κακόβουλος κόμβος εμφανίζεται μέσα στο δίκτυο μετά από καθυστέρηση για αξιολόγηση των επιπτώσεων που δύναται να εμφανιστούν σε αυτό.

2.4 Άλλες προτάσεις

Η αντιμετώπιση επιθέσεων στο Διαδίκτυο των Πραγμάτων είναι ένα πολύ ζεστό ζήτημα στις μέρες μας. Είναι γνωστό πως εάν υπάρξει εκμετάλλευση των συσκευών που ανήκουν σε αυτό, η ακεραιότητα και η εμπιστευτικότητα της πληροφορίας δύναται να επηρεαστεί.

Λόγω του ότι αυξάνονται καθημερινά οι συσκευές που ανήκουν στο Διαδίκτυο των Πραγμάτων, πολλοί ερευνητές κλήθηκαν να αναπτύξουν και να μελετήσουν προτάσεις οι οποίες μπορούν να αντιμετωπίσουν επιθέσεις που μπορεί να εμφανιστούν σε αυτές. Συνεπώς, διάφοροι ερευνητές ανέπτυξαν πρωτόκολλα [18] – [26] τα οποία αποσκοπούν στην δημιουργία εναλλακτικών μονοπατιών. Αυτά τα πρωτόκολλα προσπαθούν να αντιμετωπίσουν επιθέσεις που δύναται να εμφανιστούν στην δρομολόγηση των πακέτων πληροφορίας.

Στα πρωτόκολλα στα οποία πραγματοποιείται προληπτική μέθοδος, προκαθορίζεται από πριν το μονοπάτι το οποίο θα ακολουθηθεί. Συγκεκριμένα, με τον εντοπισμό κάποιας κακόβουλης συμπεριφοράς στο δίκτυο, οι κόμβοι αναμεταδίδουν πακέτα πληροφορίας προς όλες τις διαδρομές του δικτύου με αποτέλεσμα να υπάρχει αχρείαστη συμφόρηση στο δίκτυο.

Στα πρωτόκολλα στα οποία πραγματοποιείται αντιδραστική μέθοδος, τα νέα μονοπάτια δημιουργούνται δυναμικά με την ανίχνευση της κακόβουλης συμπεριφοράς στο δίκτυο. Με αυτό τον τρόπο, το πρωτόκολλο δρομολόγησης χρησιμοποιεί τα νέα αυτά μονοπάτια για την δρομολόγηση των πακέτων πληροφορίας μέσα στο δίκτυο. Όμως, οι συγκεκριμένες μέθοδοι αποτελούν είτε καινούργια πρωτόκολλα δρομολόγησης που δεν υπήρχαν, είτε επεκτάσεις υφισταμένων.

Κεφάλαιο 3

Επιθέσεις στο Διαδίκτυο των Πραγμάτων

3.1 Επισκόπηση
3.2 Sinkhole
3.3 Blackhole
3.4 Selective Forward
3.4.1 Forwarding Ratio
3.4.2 Block Node

3.1 Επισκόπηση

Οι επιθέσεις που εμφανίζονται στο Διαδίκτυο των Πραγμάτων, μπορεί να προέρχονται από τα κανάλια που συνδέουν τα στοιχεία του μεταξύ τους. Αρκετά πρωτόκολλα που χρησιμοποιούνται σε συσκευές του Διαδικτύου των Πραγμάτων τυγχάνει να έχουν ζητήματα ασφάλειας που μπορεί να επηρεάσουν ολόκληρο το δίκτυο. Επίσης, οι συσκευές αυτές είναι ευαίσθητες σε επιθέσεις δικτύου που επηρεάζουν την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών που μεταδίδονται από τη μία προς την άλλη. Σε αυτό το κεφάλαιο, παρουσιάζεται μία γκάμα από επιθέσεις που χρησιμοποιήθηκαν για την αξιολόγηση της προτεινόμενης λύσης και συχνά εμφανίζονται στο Διαδίκτυο των Πραγμάτων.

3.2 Sinkhole

Το συγκεκριμένο είδος επίθεσης μπορεί να χαρακτηριστεί ως ένα από τα πιο σοβαρά και αποτελεσματικά είδη επίθεσης. Οι επιθέσεις Sinkhole [6] πραγματοποιούνται είτε χάνοντας έναν κόμβο είτε εισάγοντας ένα κατασκευασμένο κόμβο μέσα στο δίκτυο.

Ένας εισβολέας έχει την δυνατότητα να παραβιάσει την δρομολόγηση των πακέτων πληροφορίας, να μεταδώσει ψευδείς πληροφορίες ή ακόμη και ψευδείς αναφορές επίθεσης για να διαταράξει το δίκτυο [28]. Μια τέτοια επίθεση μπορεί ακόμη να προκαλέσει εξάντληση ενέργειας στους κόμβους [27].

Συγκεκριμένα, ο κακόβουλος κόμβος προσποιείται ότι είναι η κεντρική πύλη με χρήση ή αλλοίωση πακέτων που στέλνονται από αυτή. Με αυτό τον τρόπο, ο κακόβουλος κόμβος προσπαθεί να καθοδηγήσει τα πακέτα με πληροφορίες που στέλνονται από άλλους κόμβους προς τον εαυτό του. Λόγω του ότι ο κακόβουλος κόμβος παρουσιάζεται ως ο πιο ελκυστικός κόμβος διαφημίζοντας πως είναι η κεντρική πύλη στους γείτονές του, δημιουργείται μία τρύπα μέσα στο δίκτυο. Συνεπώς, παίρνοντας όλα τα πακέτα από τους γείτονές του ο κακόβουλος κόμβος έχει την δυνατότητα να τους εξαντλήσει αλλά και να απορρίψει τα συγκεκριμένα πακέτα που λαμβάνει.

Ακόμη, αξίζει να σημειωθεί πως ανάλογα με την απόσταση που έχει ο κακόβουλος κόμβος από την κεντρική πύλη, αλλάζει η αποτελεσματικότητα της επίθεσης [13]. Για παράδειγμα, εάν σε κάποια συγκεκριμένη τοπολογία δικτύου ο κακόβουλος κόμβος τοποθετηθεί πολύ κοντά στην κεντρική πύλη θα προσελκύσει πολύ περισσότερα δεδομένα από το να βρίσκεται μακριά της. Όμως, αποδείχθηκε πως ακόμη και εάν ο κακόβουλος κόμβος βρίσκεται μακριά από την κεντρική πύλη, πάλι έχει την δυνατότητα να απορρίψει πακέτα πληροφορίας τα οποία έπρεπε να ληφθούν από την κεντρική πύλη.

3.3 Blackhole

Στις επιθέσεις Blackhole [7], ο κακόβουλος κόμβος χρησιμοποιεί το πρωτόκολλο δρομολόγησης για να διαφημίσει στους γείτονές του πως έχει μικρό ή και μηδαμινό κόστος δρομολόγησης από την κεντρική πύλη. Στη παρούσα διπλωματική εργασία όταν ο κακόβουλος κόμβος διεξάγει επίθεση τύπου Blackhole, διαφημίζει ότι είναι άμεσος γείτονας με την κεντρική πύλη.

Συνεπώς, διαφημίζοντας πως βρίσκεται στη συντομότερη διαδρομή προς την κεντρική πύλη, αυτός ο κακόβουλος κόμβος παρουσιάζει ως διαθέσιμα νέα δρομολόγια ανεξάρτητα από τον έλεγχο του πίνακα δρομολόγησης. Έτσι, ο κακόβουλος κόμβος έχει πάντα την δυνατότητα να απαντά σε ένα αίτημα διαδρομής για να παραλάβει τα πακέτα από τους γείτονες του και να τα παρακολουθήσει, να τα αλλοιώσει ή και να τα απορρίψει.

Σημαντικό είναι πως σε πρωτόκολλα του Διαδικτύου των Πραγμάτων τα οποία βασίζονται στην τεχνική της πλημμύρας η απάντηση του κακόβουλου κόμβου θα ληφθεί συντομότερα από τον αιτούμενο κόμβο παρά του μη κακόβουλου κόμβου. Με αυτό τον τρόπο ο κακόβουλος κόμβος θα δημιουργήσει ένα ψεύτικο μονοπάτι και μέσω αυτού του μονοπατιού θα αποφασίσει τι θα κάνει με τα πακέτα που λαμβάνει.

Τέλος, αυτή η επίθεση συνδυάζεται συχνά με επιθέσεις τύπου Selective Forward που αναλύονται στο Παράρτημα 3.4, ούτως ώστε να υπάρχει μεγαλύτερη επιρροή στο δίκτυο και να επηρεαστούν περισσότερα πακέτα [13].

3.4 Selective Forward

Σε αυτό τον τύπο επίθεσης δικτύου, ο κακόβουλος κόμβος απορρίπτει το αίτημα για μεταφορά πακέτων πληροφορίας και διασφαλίζει πως δεν θα μεταφερθούν περαιτέρω μέσα στο δίκτυο [29]. Συνεπώς, ο κακόβουλος κόμβος προσπαθεί να καταστρέψει την λειτουργικότητα του δικτύου μέσω της απόρριψης πακέτων επιλεκτικά ή τυχαία. Αυτό είναι εφικτό διότι οι ενδιάμεσοι κόμβοι του δικτύου προωθούν πακέτα πληροφορίας προς την κεντρική πύλη.

Γενικά, υπάρχουν δύο τρόποι με τους οποίους ο εισβολέας μπορεί να επιτεθεί στο δίκτυο. Ο πρώτος τρόπος ο οποίος είναι δύσκολο να εντοπιστεί πραγματοποιείται μέσω της κλοπής πληροφοριών ή κάποιου κλειδιού από τους κόμβους του δικτύου. Ο δεύτερος τρόπος πραγματοποιείται μέσω της παρεμπόδισης της διαδρομής δρομολόγησης μεταξύ των νόμιμων κόμβων του δικτύου.

3.4.1 Forwarding Ratio

Η επίθεση αυτή αποτελεί παραλλαγή της επίθεσης Selective Forward, όπου πραγματοποιείται απόρριψη πακέτων πληροφορίας με μια προκαθορισμένη πιθανότητα r. Συνεπώς, όταν ο κακόβουλος κόμβος παραλάβει κάποιο πακέτο από κάποιο γείτονα θα το προωθήσει μετέπειτα μέσα στο δίκτυο με πιθανότητα (1 – r) ή θα το απορρίψει με πιθανότητα r. Για τις πειραματικές μετρήσεις της παρούσας διπλωματικής εργασίας για αξιολόγηση της προτεινόμενης λύσης, χρησιμοποιήθηκε η τιμή r = 0.5.

3.4.2 Block Node

Η επίθεση αυτή αποτελεί παραλλαγή της επίθεσης Selective Forward και στην συγκεκριμένη επίθεση ο κακόβουλος κόμβος στοχεύει κάποιο συγκεκριμένο γείτονα για τον οποίο επιλέγει να μην προωθήσει πακέτα πληροφορίας του μέσα στο δίκτυο όταν τα παραλάβει. Συνήθως, η επιλογή στοχευμένου γείτονα πραγματοποιείται τυχαία, όμως ο κακόβουλος κόμβος έχει την δυνατότητα να αλλάξει θύματα περιοδικά και δυναμικά. Για τις πειραματικές μετρήσεις της παρούσας διπλωματικής εργασίας για αξιολόγηση της προτεινόμενης λύσης, ο κακόβουλος κόμβος αλλάζει θύμα μετά τον αποκλεισμό 10 πακέτων πληροφορίας.

Κεφάλαιο 4

Μεθοδολογία

4.1 Επισκόπηση
4.2 Πρωτόκολλο δρομολόγησης Weighted Shortest Path
4.3 Πρωτόκολλο κόμβου RDC ContikiMAC
4.4 Πρωτόκολλο κόμβου RDC Null
4.5 Πακέτο συνδέσμου ασφαλείας
4.6 Επαναδρομολόγηση
4.7 Επανεκκίνηση
4.8 Χρήση συστήματος ανιχνεύσεως εισβολής mIDS
4.9 Επιθέσεις μετά από καθυστέρηση
4.10 Μετρήσεις απόδοσης

4.1 Επισκόπηση

Στην παρούσα διπλωματική εργασία πραγματοποιείται χρήση δύο τεχνικών αποκατάστασης κόμβου και δικτύου στο Διαδίκτυο των Πραγμάτων. Η πρώτη τεχνική είναι αυτή της επαναδρομολόγησης όπου οι γείτονες του κακόβουλου κόμβου προσπαθούν να βρουν ένα καινούργιο μονοπάτι το οποίο είναι ασφαλές για να δρομολογήσουν τα πακέτα πληροφορίας τους. Η δεύτερη τεχνική είναι η τεχνική της επανεκκίνησης η οποία ενεργοποιείται ακριβώς μετά από τον μηχανισμό της επαναδρομολόγησης και επαναφέρει τον κακόβουλο κόμβο στην αρχική και μη κακόβουλη κατάσταση του. Η “σκανδάλη” ενεργοποίησης των δύο μηχανισμών τοποθετήθηκε στο σύστημα ανίχνευσης εισβολής mIDS, το οποίο με την σειρά του κάνει χρήση του πακέτου συνδέσμου ασφάλειας. Επιπρόσθετα, το πρωτόκολλο δρομολόγησης που χρησιμοποιήθηκε είναι το Weighted Shortest Path και το πρωτόκολλο κόμβου που χρησιμοποιήθηκε είναι οι δύο παραλλαγές RDC. Ακόμη, αναπτυχθήκαν σενάρια όπου ο κακόβουλος κόμβος εμφανίζεται μέσα στο δίκτυο μετά από κάποιο χρονικό διάστημα αντί εξαρχής για περαιτέρω εκτίμηση της προτεινόμενης λύσης. Τέλος, παρουσιάζονται οι μετρήσεις απόδοσης που χρησιμοποιήθηκαν για την αξιολόγηση της πρότασης.

4.2 Πρωτόκολλο δρομολόγησης Weighted Shortest Path

Στην παρούσα διπλωματική εργασία έγινε χρήση του πρωτόκολλου δρομολόγησης Weighted Shortest Path για αξιολόγηση της προτεινόμενης λύσης.

Έχουν προταθεί πολλαπλά πρωτόκολλα δρομολόγησης για το Διαδίκτυο των Πραγμάτων, όμως η επιλογή του συγκεκριμένου πρωτόκολλου δρομολόγησης βασίστηκε στο γεγονός ότι είναι απλό. Επιλέγοντας το, δεν εμφανίζεται οποιουδήποτε είδους επιβάρυνση στην αποστολή πακέτων πληροφορίας μέσα στο δίκτυο.

Συνεπώς, με αυτό τον τρόπο υπήρξε αντικειμενική αξιολόγηση των μηχανισμών αποκατάστασης που προτείνονται. Αξίζει να σημειωθεί ότι το συγκεκριμένο πρωτόκολλο δρομολόγησης βασίζεται στην έννοια του συντομότερου μονοπατιού και δεν παρουσιάζει ιδιαιτερότητες και περιορισμούς που συχνά εμφανίζονται σε άλλα πρωτόκολλα.

Ο απώτερος σκοπός του κάθε κόμβου που βρίσκεται μέσα στο δίκτυο είναι να προωθήσει τα πακέτα πληροφορίας του ιδίου ή κάποιου γειτονικού του κόμβου προς την κεντρική πύλη με όσο το δυνατό μικρότερο κόστος. Συγκεκριμένα, το κόστος πρέπει να είναι όσο μικρότερο γίνεται λόγω του ότι οι κόμβοι που βρίσκονται μέσα στο δίκτυο στηρίζονται σε ενέργεια μπαταρίας και έτσι δεν διαθέτουν μεγάλη ενεργειακή απόδοση. Με την εγκατάσταση αυτού του πρωτόκολλου δρομολόγησης στο δίκτυο, ο κάθε κόμβος προσπαθεί να προωθήσει τα πακέτα πληροφορίας στους γειτονικούς του κόμβους με βάση την απόσταση που έχουν από την κεντρική πύλη και την ισχύ του σήματος μετάδοσης.

Κατά την διάρκεια του σχηματισμού της τοπολογίας του δικτύου το οποίο έχει διάρκεια δύο λεπτά, ο κάθε κόμβος δημιουργεί ένα πίνακα γειτνίασης με βάση τις ανακοινώσεις που λαμβάνει από τους γειτονικούς του κόμβους. Οι συγκεκριμένες ανακοινώσεις που αναμεταδίδονται περιοδικά μέσα στο δίκτυο περιέχουν πληροφορίες για την θέση του κάθε κόμβου μέσα στο δίκτυο.

Ο πίνακας γειτνίασης κάθε κόμβου ενημερώνεται με τις θέσεις των γειτονικών του κόμβων μέσα στο δίκτυο ούτως ώστε να γνωρίζει τον τρόπο με τον οποίο θα δρομολογήσει τα πακέτα προς την κεντρική πύλη όσο πιο αποδοτικά γίνεται. Οποιαδήποτε καταχώρηση πραγματοποιηθεί στον πίνακα γειτνίασης χαρακτηρίζεται από την μοναδική ταυτότητα του κόμβου η οποία ονομάζεται Rime Address, από την απόσταση του κόμβου από την κεντρική πύλη και την τιμή ένδειξης ισχύος του σήματος μετάδοσης που ονομάζεται RSSI.

Στην παρούσα διπλωματική εργασία πραγματοποιήθηκε και χρήση μίας τιμής ασφαλείας η οποία καταχωρείται και αυτή στον πίνακα γειτνίασης ενός κόμβου. Η συγκεκριμένη τιμή μπορεί να ισούται με 1 που υποδεικνύει πως ο γειτονικός κόμβος είναι αξιόπιστος και έτσι μπορούν να προωθηθούν πακέτα πληροφορίας σε αυτόν. Επίσης, η τιμή μπορεί να ισούται με 0 που υποδεικνύει πως ο γειτονικός κόμβος είναι κακόβουλος και δεν θα πρέπει να δρομολογηθούν πακέτα πληροφορίας προς αυτόν.

Η τιμή ασφαλείας αλλάζει από 0 σε 1 ή και αντίθετα, μέσω του πακέτου συνδέσμου ασφαλείας το οποίο προωθείται κατά την διάρκεια του μηχανισμού επαναδρομολόγησης που θα αναλυθεί στο Παράρτημα 4.5.

4.3 Πρωτόκολλο κόμβου RDC ContikiMAC

Οι συσκευές που ανήκουν στο Διαδίκτυο των Πραγμάτων είναι συχνά χαμηλής ισχύος και λειτουργούν με μπαταρία. Συνεπώς, οι συσκευές αυτές πρέπει να έχουν για όσο μεγαλύτερο χρονικό διάστημα γίνεται, ανενεργή την αντένα τους, ούτως ώστε να μην υπάρχει σπατάλη ενέργειας. Παράλληλα, οι συσκευές πρέπει να ξυπνούν αρκετά συχνά για να είναι σε θέση να λαμβάνουν πακέτα πληροφορίας από τους γείτονες τους.

Το πρωτόκολλο κόμβου RDC ContikiMAC [11] [12] χρησιμοποιεί έναν ενεργειακά αποδοτικό μηχανισμό αφύπνισης με ένα σύνολο χρονικών περιορισμών για να επιτρέπει στους κόμβους να έχουν ανενεργή την αντένα τους. Συγκεκριμένα, με αυτό το πρωτόκολλο οι κόμβοι μπορούν να συμμετέχουν σε επικοινωνία μέσα στο δίκτυο και παράλληλα να έχουν ανενεργή την αντένα τους περίπου το 99% του χρόνου.

Αυτό το πρωτόκολλο έχει σχεδιαστεί για να είναι απλό στην κατανόηση και εφαρμογή του χρησιμοποιώντας μόνο ασύγχρονο και σιωπηρό συγχρονισμό. Ακόμη, δεν απαιτεί μηνύματα σηματοδότησης ή επιπρόσθετες κεφαλίδες. Το σχήμα συγχρονισμού που χρησιμοποιεί επιτρέπει στον κόμβο να εξοικονομήσει ενέργεια και να προωθεί πακέτα πληροφορίας αποδοτικά.

Ένα παράδειγμα τρόπου λειτουργίας αυτού του πρωτοκόλλου είναι το εξής:
Έστω ότι υπάρχει ένας κόμβος Α και ένας άλλος κόμβος Β όπου ο κόμβος Α προσπαθεί να προωθήσει κάποιο πακέτο πληροφορίας στον κόμβο Β. Εάν η αντένα του κόμβου Β είναι ανενεργή εκείνο το χρονικό διάστημα που προωθείται το πακέτο, ο κόμβος Α συνεχίζει να προωθεί το ίδιο πακέτο μέχρι ο κόμβος Β να ενεργοποιήσει την αντένα του.

4.4 Πρωτόκολλο κόμβου RDC Null

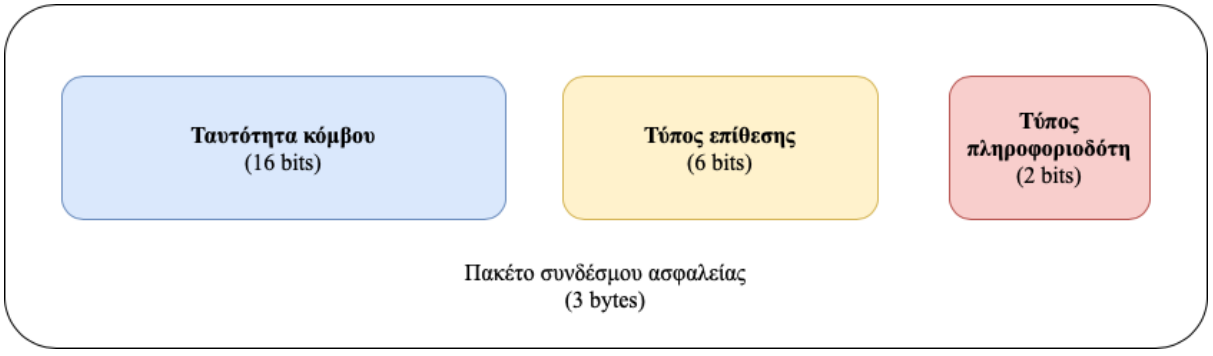
Το πρωτόκολλο κόμβου RDC Null [12] χρησιμοποιεί τις συναρτήσεις Framer για την δημιουργία και την ανάλυση κεφαλίδων. Οι συναρτήσεις αυτές χειρίζονται όλες τις πληροφορίες της κεφαλίδας με αφηρημένο τρόπο, κάνοντας χρήση μίας δομής που ονομάζεται Packetbuf.

Επιπρόσθετα, δεν εξοικονομεί ενέργεια και λειτουργεί ως στρώμα διέλευσης που μεταδίδει μόνο ένα πακέτο. Με την μετάδοση κάποιου πακέτου στο δίκτυο, το πρωτόκολλο RDC Null επιστρέφει τα αποτελέσματα αυτής της μετάδοσης, δηλαδή εάν ήταν επιτυχής ή συγκρούστηκε. Επειδή σε ένα δίκτυο δύναται να υπάρχουν πολλοί κόμβοι που αναμεταδίδουν συχνά πακέτα, το πρωτόκολλο αυτό χρησιμοποιείται για αντιμετώπιση της συμφόρησης.

Για παράδειγμα, έστω ότι υπάρχει ένας κόμβος Α και ένας άλλος κόμβος Β. Ο κόμβος Α προσπαθεί να προωθήσει κάποιο πακέτο πληροφορίας στον κόμβο Β. Εάν η αντένα του κόμβου Β είναι ανενεργή εκείνο το χρονικό διάστημα που προωθείται το πακέτο πληροφορίας και γίνετε χρήση του πρωτόκολλου RDC Null, τότε ο κόμβος Β δεν θα παραλάβει ποτέ το πακέτο.

Συμπερασματικά, στην παρούσα διπλωματική εργασία πραγματοποιήθηκαν πειράματα κάνοντας χρήση και αυτού του πρωτοκόλλου κόμβου για να εντοπισθεί εάν μπορούν να προωθηθούν περισσότερα πακέτα προς την κεντρική πύλη. Αυτή η απόφαση πάρθηκε μετά από εντοπισμό ότι το πρωτόκολλο κόμβου RDC ContikiMAC προκαλεί συμφόρηση στο δίκτυο και δεν προωθείται ένας ικανοποιητικός αριθμός πακέτων προς την κεντρική πύλη.

4.5 Πακέτο συνδέσμου ασφαλείας



Εικόνα 4.1: Αρχιτεκτονική Πακέτου Ασφαλείας

Τύπος Επίθεσης	*Συνδυασμός Bits*
Sinkhole	**00 0001**
Blackhole	**00 1000**
Selective Forward	**00 0100**
Selective Forward Forwarding Ratio	**00 0101**
Selective Forward Block Node	**00 0110**
Selective Forward Forwarding Ratio & Blackhole	**00 1101**
Selective Forward Block Node & Blackhole	**00 1110**
Benign	**00 0000**
Unknown	**11 1111**

Πίνακας 4.1: Αναγνωριστικά Επίθεσης

Το πακέτο συνδέσμου ασφαλείας αποτελεί ένα μήνυμα που στέλνεται από τους κόμβους του δικτύου και δύναται να χαρακτηριστεί ως ο πυλώνας αυτής της προτεινόμενης λύσης. Γενικότερα, το συγκεκριμένο πακέτο μεταφέρεται περιοδικά μέσα στο δίκτυο ούτως ώστε να ενημερώνει κάθε κόμβο για την κατάσταση των γειτονικών του κόμβων.

Συγκεκριμένα, το πακέτο συνδέσμου ασφαλείας έχει μέγεθος 3 bytes και χωρίζεται σε τρία βασικά μέρη. Το πρώτο μέρος το οποίο έχει μέγεθος 16 bits αποτελεί την μοναδική ταυτότητα του γειτονικού κόμβου που το στέλνει και ονομάζεται Rime Address. Το δεύτερο μέρος του πακέτου συνδέσμου ασφαλείας έχει μέγεθος 6 bits όπου αναγράφεται ο τύπος επίθεσης που διεξάγεται στον γειτονικό κόμβο. Τέλος, το τρίτο και τελευταίο μέρος του πακέτου το οποίο έχει μέγεθος 2 bits αποτελεί τον τύπο του πληροφοριοδότη.

Ο τύπος πληροφοριοδότη, αναπαριστά τον τρόπο με τον οποίο ανιχνεύθηκε μια κακόβουλη συμπεριφορά σε κάποιο κόμβο. Ο συνδυασμός bits 00 υποδηλώνει πως η ανίχνευση της επίθεσης πραγματοποιήθηκε από κάποιο ειδικό σύστημα που εκτελείται τοπικά στον κόμβο. Ο συνδυασμός bits 01 υποδηλώνει πως η ανίχνευση πραγματοποιήθηκε από κάποιο κόμβο ασφαλείας που λειτουργεί σαν συσκευή παρακολούθησης συμπεριφοράς του δικτύου, ενώ η ακολουθία 10 δείχνει πως η ανίχνευση πραγματοποιήθηκε από κάποιο καθολικό κόμβο του δικτύου, όπως την κεντρική πύλη. Στην παρούσα διπλωματική εργασία γίνεται χρήση του συστήματος ανίχνευσης εισβολής mIDS το οποίο εκτελείται τοπικά σε κάθε κόμβο και άρα πάντα η ακολουθία τύπου πληροφοριοδότη θα ισούται με 00. Συνεπώς, εάν διεξάγεται κάποια επίθεση σε κάποιο κόμβο, το σύστημα ανίχνευσης εισβολής mIDS είναι υπεύθυνο για να την εντοπίσει και να αναγνωρίσει τον τύπο της επίθεσης.

Για αυτό τον λόγο, τα 4 από τα 6 bits του τύπου επίθεσης στο πακέτο συνδέσμου ασφαλείας χρησιμοποιούνται για αναπαράσταση των πιο γνωστών επιθέσεων που εμφανίζονται στο Διαδίκτυο των Πραγμάτων. Άρα, εάν εμφανιστεί μία επίθεση τύπου Sinkhole σε κάποιο κόμβο, ο τύπος επίθεσης στο πακέτο συνδέσμου ασφαλείας θα αποθηκεύσει τον συνδυασμό bits 00 0001, εάν εμφανιστεί μία τύπου Blackhole θα αποθηκεύσει τον συνδυασμό 00 1000 και εάν εμφανιστεί μία τύπου Selective Forward θα αποθηκεύσει τον συνδυασμό 00 0100.

Όπως αναφέρθηκε και στο Κεφάλαιο 3, η επίθεση τύπου Selective Forward δύναται να διαχωριστεί σε δύο παραλλαγές. Συνεπώς, εάν εμφανιστεί η παραλλαγή επίθεσης τύπου Forwarding Ratio, στον τύπο επίθεσης θα αποθηκευτεί ο συνδυασμός bits 00 0101 και εάν εμφανιστεί η παραλλαγή τύπου Block Node θα αποθηκευτεί ο συνδυασμός 00 0110.

Ακόμη, λόγω του ότι οι συνδυασμοί επιθέσεων Selective Forward Forwarding Ratio με Blackhole και Selective Forward Block Node με Blackhole εμφανίζονται συχνά στο Διαδίκτυο των Πραγμάτων, αναπτύχθηκε αναπαράσταση bits και για αυτούς. Ο πρώτος συνδυασμός επιθέσεων χαρακτηρίζεται από την ακολουθία bits 00 1101 ενώ ο δεύτερος από την ακολουθία 00 1110.

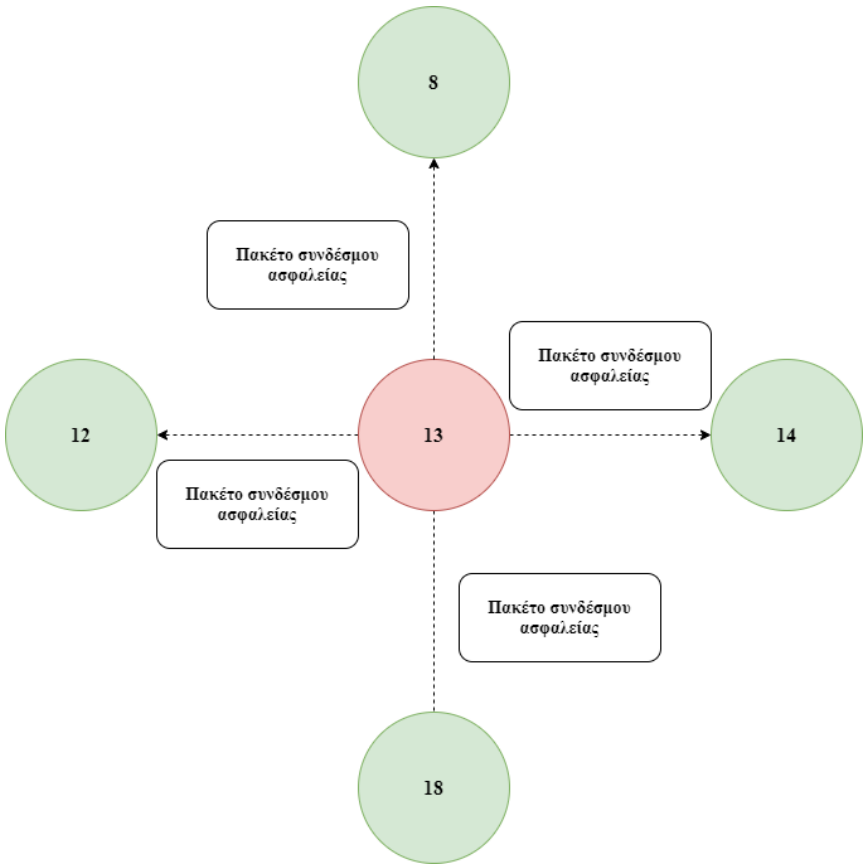
Επιπρόσθετα, όπως αναγράφτηκε προηγουμένως το πακέτο συνδέσμου ασφαλείας χρησιμοποιείται και από τους μη κακόβουλους κόμβους για να ενημερώσουν τους γειτονικούς τους κόμβους πως είναι αξιόπιστοι και έχουν την δυνατότητα να προωθήσουν πακέτα προς την κεντρική πύλη. Για αυτό τον λόγο ο συνδυασμός bits 00 0000 του τύπου επίθεσης στο πακέτο συνδέσμου ασφαλείας χαρακτηρίζει έναν αξιόπιστο κόμβο.

Είναι κατανοητό πως τα πρώτα 2 bits από τα 6 του τύπου επίθεσης παρέμειναν αχρησιμοποίητα στο παρόν στάδιο. Τα συγκεκριμένα bits μπορούν να χρησιμοποιηθούν στο μέλλον για διάφορες άλλες παραλλαγές επιθέσεων που δύναται να εμφανιστούν στο Διαδίκτυο των Πραγμάτων.

Το συγκεκριμένο πακέτο χρησιμοποιείται κυρίως σε δύο σενάρια όπου ενημερώνει τον κάθε κόμβο για την κατάσταση τον γειτόνων του, δηλαδή εάν είναι αξιόπιστοι ή κακόβουλοι. Το πρώτο σενάριο χρήσης αυτού του πακέτου όπου οι γειτονικοί κόμβοι είναι αξιόπιστοι εξαρχής, είναι κατά την διάρκεια δημιουργίας της τοπολογίας του δικτύου όπου οι κόμβοι αναμεταδίδουν το πακέτο μέσα στο δίκτυο. Στην συγκεκριμένη περίπτωση ο τύπος επίθεσης του πακέτου έχει την τιμή 00 0000 που υποδηλώνει έναν αξιόπιστο κόμβο. Στην παρούσα διπλωματική εργασία αυτό το πακέτο αναμεταδίδεται κάθε 1 λεπτό μέσα στο δίκτυο.

Το δεύτερο σενάριο χρήσης του πακέτου συνδέσμου ασφαλείας είναι όταν ένας κακόβουλος κόμβος εντοπισθεί από το σύστημα ανίχνευσης εισβολής mIDS και ενεργοποιείται ο μηχανισμός επαναδρομολόγησης για ενημέρωση των γειτόνων του κακόβουλου κόμβου. Ο τύπος επίθεσης σε αυτή την περίπτωση χαρακτηρίζεται με την ακολουθία bits που αντιστοιχούν στην επίθεση που ανιχνεύτηκε από το σύστημα. Για την παρούσα διπλωματική εργασία ο χρόνος αναμετάδοσης είναι ίσος με 1 πακέτο ανά δευτερόλεπτο για συνολικά 10 δευτερόλεπτα από τον εντοπισμό της επίθεσης και στην συνέχεια 1 πακέτο ανά λεπτό.

4.6 Επαναδρομολόγηση



Εικόνα 4.2: Μηχανισμός Επαναδρομολόγησης

Ο πρώτος μηχανισμός αποκατάστασης κόμβου και δικτύου στο Διαδίκτυο των Πραγμάτων της προτεινόμενης λύσης είναι αυτός της επαναδρομολόγησης.

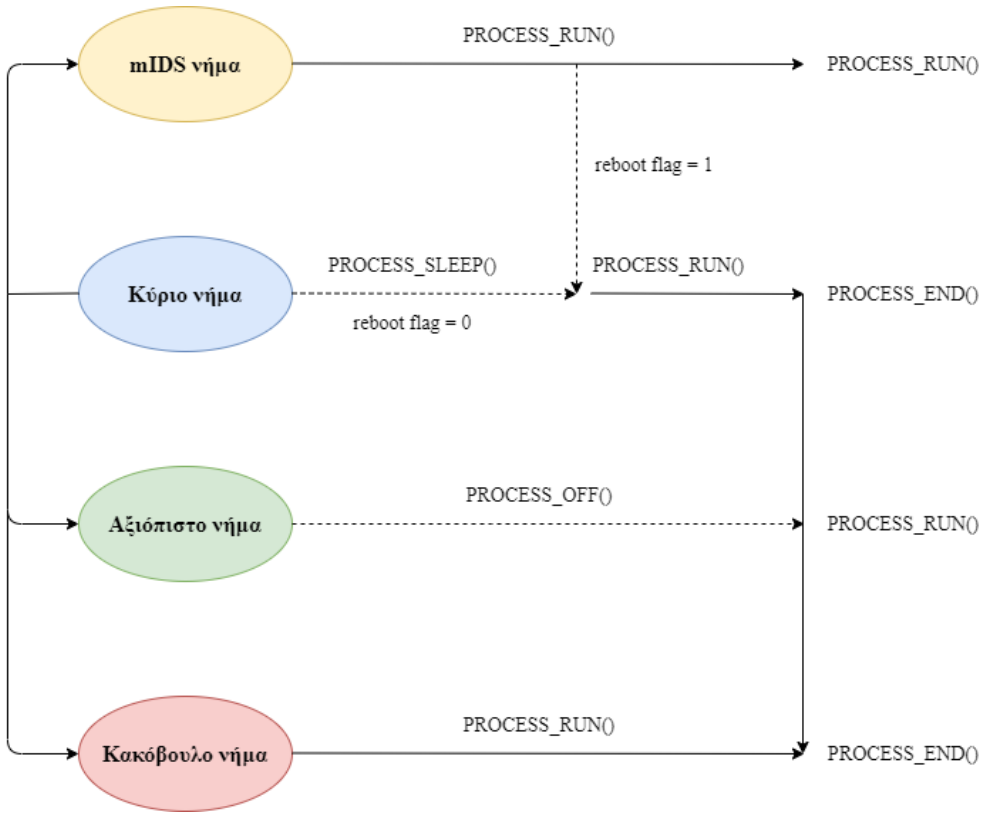
Ο συγκεκριμένος μηχανισμός ενεργοποιείται από το σύστημα ανίχνευσης εισβολής mIDS, το οποίο εκτελείται τοπικά σε κάθε κόμβο. Χρησιμοποιώντας την τεχνική Binary Logistic Regression, με τον επιτυχές εντοπισμό του κακόβουλου κόμβου, σηματοδοτείται η εκκίνηση της επαναδρομολόγησης.

Στην συνέχεια, ο μηχανισμός αναμεταδίδει πακέτα συνδέσμου ασφαλείας μέσα στο δίκτυο. Τα αναμεταδιδόμενα αυτά πακέτα μεταφέρονται μέσα στο δίκτυο κάθε 1 δευτερόλεπτο για 10 δευτερόλεπτα από την στιγμή που ενεργοποιήθηκε ο μηχανισμός. Μετέπειτα, ο μηχανισμός της επαναδρομολόγησης αναλαμβάνει να αναμεταδίδει 1 πακέτο ανά λεπτό ούτως ώστε να ενημερώνονται και τυχόν νέοι γείτονες του κακόβουλου κόμβου στο δίκτυο.

Συνεπώς, ο μηχανισμός αυτός αποσκοπεί στην ενημέρωση των γειτονικών κόμβων ενός κακόβουλου κόμβου πως είναι αναξιόπιστος. Μέσω της ενημέρωσης, οι γειτονικοί κόμβοι θέτουν την τιμή του bit ασφαλείας του κακόβουλου κόμβου στον πίνακα γειτνίασης ίση με 0. Στην συνέχεια, οι γειτονικοί κόμβοι προσπαθούν να επιλέξουν ένα εναλλακτικό μονοπάτι το οποίο είναι ασφαλές, για την δρομολόγηση των πακέτων τους προς την κεντρική πύλη, λαμβάνοντας υπόψη τα bit ασφαλείας του πίνακα γειτνίασης.

Συμπερασματικά, η τεχνική της επαναδρομολόγησης βοηθά στην επιτυχή λήψη πακέτων πληροφορίας από την κεντρική πύλη. Χωρίς την τεχνική αυτή, οι αξιόπιστοι κόμβοι θα συνέχιζαν να στέλνουν πακέτα προς τον γειτονικό τους κακόβουλο κόμβο, με αποτέλεσμα τα πακέτα αυτά να μην έφταναν ποτέ στον ορθό προορισμό τους.

4.7 Επανεκκίνηση



Εικόνα 4.3: Μηχανισμός Επανεκκίνησης

Ο δεύτερος μηχανισμός αποκατάστασης κόμβου και δικτύου στο Διαδίκτυο των Πραγμάτων της προτεινόμενης λύσης είναι αυτός της επανεκκίνησης. Γενικότερα, με τον επιτυχή εντοπισμό ενός κακόβουλου κόμβου από το σύστημα ανίχνευσης εισβολής mIDS, ο μηχανισμός της επανεκκίνησης ενεργοποιείται μετά από την σηματοδότηση του μηχανισμού της επαναδρομολόγησης από το σύστημα.

Στην συγκεκριμένη περίπτωση, ενεργοποιείται αναμετάδοση πακέτου συνδέσμου ασφαλείας μόνο για 10 δευτερόλεπτα, όπου στέλνεται 1 πακέτο ανά δευτερόλεπτο μέσα στο δίκτυο. Αυτό συμβαίνει για να αποφευχθεί η απώλεια πακέτων πληροφορίας από το δίκτυο μέχρις ότου να ενεργοποιηθεί ο μηχανισμός της επανεκκίνησης.

Συγκεκριμένα, υπάρχει μία κύρια εφαρμογή κόμβου η οποία είναι υπεύθυνη για την διαχείριση τριών διαδικασιών. Η πρώτη διαδικασία που αναλαμβάνει η κύρια εφαρμογή είναι η εκκίνηση του συστήματος ανίχνευσης εισβολής mIDS και η δεύτερη η εκκίνηση της κακόβουλης συμπεριφοράς του κόμβου. Αφού ενεργοποιήσει και τις δύο διαδικασίες, τότε η κύρια εφαρμογή κόμβου περιμένει, αναμένοντας το τέλος της επαναδρομολόγησης με χρήση μίας σημαίας η οποία είναι υπεύθυνη για αυτό.

Μόλις εντοπισθεί η κακόβουλη συμπεριφορά από το σύστημα ανίχνευσης εισβολής mIDS, το σύστημα ενεργοποιεί τον μηχανισμό της επαναδρομολόγησης. Με την επιτυχή ολοκλήρωση του μηχανισμού αυτού, ενεργοποιείται ο μηχανισμός της επανεκκίνησης όπου η κύρια εφαρμογή του κόμβου σταματά την κακόβουλη συμπεριφορά του. Ταυτόχρονα, ενεργοποιεί το εφεδρικό αντίγραφο της εφαρμογής που βρίσκεται φορτωμένο στην κύρια του μνήμη ούτως ώστε ο κόμβος να επιστρέψει σε μια αξιόπιστη συμπεριφορά. Με την επιτυχή επιστροφή του κόμβου στην αξιόπιστη του συμπεριφορά, η κύρια του εφαρμογή ενεργοποιεί την τρίτη διαδικασία. Η διαδικασία αυτή χρησιμοποιεί το πακέτο συνδέσμου ασφαλείας για να ενημερώσει τους γειτονικούς κόμβους πως ο πρώην κακόβουλος κόμβος είναι και πάλι αξιόπιστος.

Με αυτό τον τρόπο, οι γειτονικοί κόμβοι θέτουν την τιμή του bit ασφαλείας στον πίνακα γειτνίασης τους από 0 σε 1 και έτσι προωθούν πακέτα προς την κεντρική πύλη και μέσω του πλέον αξιόπιστου κόμβου. Αξίζει να σημειωθεί πως για να καθοριστεί γρήγορα η θέση του νέου αξιόπιστου κόμβου μέσα στο δίκτυο, όταν οι γειτονικοί κόμβοι ενημερώνονται για αλλαγή του bit ασφαλείας, ανακοινώνουν αμέσως τις προδιαγραφές της δρομολόγησης. Η ανακοίνωση αυτή αφορά την απόσταση που απέχουν οι κόμβοι από την κεντρική πύλη και την τιμή ισχύς της μετάδοσης του σήματος.

Συνοπτικά, ο μηχανισμός της επανεκκίνησης βοηθά στην λήψη περισσότερων πακέτων πληροφορίας από την κεντρική πύλη. Αυτό συμβαίνει λόγω του ότι με την επαναφορά του κακόβουλου κόμβου σε αξιόπιστη κατάσταση, προωθεί και αυτός με την σειρά του πακέτα προς την κεντρική πύλη. Χωρίς αυτή την τεχνική, ο κακόβουλος κόμβος θα παρέμενε αδρανής μέσα στο δίκτυο εάν δεν λάμβανε πακέτα μέσω του μηχανισμού επαναδρομολόγησης. Συνεπώς, προτείνεται να πραγματοποιείται χρήση και των δύο μηχανισμών ταυτόχρονα.

4.8 Χρήση συστήματος ανιχνεύσεως εισβολής mIDS

Όπως έχει ήδη λεχθεί, η παρούσα διπλωματική εργασία χρησιμοποιεί το σύστημα ανίχνευσης εισβολής mIDS το οποίο είναι υπεύθυνο για τον εντοπισμό κακόβουλης συμπεριφοράς ενός κόμβου καθώς και για την ενεργοποίηση των δύο μηχανισμών ανάκτησης κόμβου και δικτύου στο Διαδίκτυο των Πραγμάτων. Γενικότερα, η κύρια εφαρμογή κάθε κακόβουλου κόμβου είναι υπεύθυνή για την εκκίνηση της συγκεκριμένης διαδικασίας που αφορά το σύστημα mIDS.

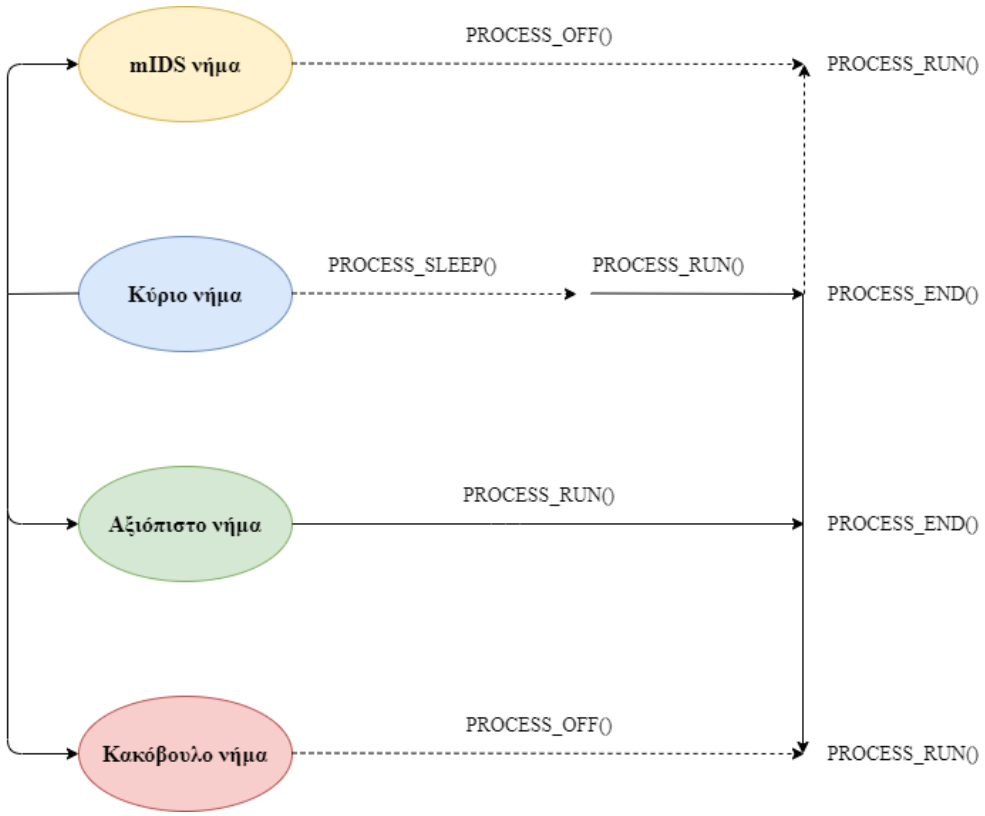
Συγκεκριμένα, ο κάθε κακόβουλος κόμβος θέτει κάποια τιμή σε μία σημαία αποκατάστασης παράλληλα με την εκκίνηση του συστήματος ανίχνευσης εισβολής mIDS. Η σημαία αυτή παίρνει την τιμή reroute = 1 εάν είναι επιθυμητό να ενεργοποιηθεί μόνο ο μηχανισμός της επαναδρομολόγησης από το σύστημα mIDS με τον επιτυχή εντοπισμό ενός κακόβουλου κόμβου μέσα στο δίκτυο. Παράλληλα, εάν είναι επιθυμητό να ενεργοποιηθεί ο μηχανισμός επανεκκίνησης μετά από την επαναδρομολόγηση, η συγκεκριμένη σημαία παίρνει την τιμή reboot = 1. Αντιθέτως, εάν η συγκεκριμένη σημαία δεν πάρει κάποια από τις τιμές που προαναφέρθηκαν, τότε δεν ενεργοποιείται κανένας μηχανισμός αποκατάστασης κόμβου και δικτύου.

Η κύρια εφαρμογή του συστήματος mIDS χρησιμοποιεί μοντέλο ανίχνευσης επιθέσεων που βασίζεται στο Binary Logistic Regression [4] για εντοπισμό επιθέσεων που συχνά εμφανίζονται στο Διαδίκτυο των Πραγμάτων και αναλύθηκαν στο Κεφάλαιο 3. Αξίζει να σημειωθεί πως το συγκεκριμένο σύστημα εκπαιδεύτηκε μόνο σε περιβάλλον που τρέχει το πρωτόκολλο κόμβου RDC ContikiMAC παρόλο που έγινε και χρήση του πρωτόκολλου RDC Null για περαιτέρω εκτίμηση της προτεινόμενης λύσης. Η χρήση του πρωτόκολλου RDC Null όμως βοήθησε στην αξιολόγηση του συστήματος mIDS, καθώς επιτράπηκε η αξιολόγηση της αποτελεσματικότητας εντοπισμού επιθέσεων σε πρωτόκολλο κόμβου όπου δεν υπήρξε εκπαίδευση.

Όταν διεξάγεται κάποια επίθεση, το σύστημα mIDS ανιχνεύει το είδος της επίθεσης. Στην συνέχεια, η κύρια εφαρμογή του συστήματος θέτει μία σημαία συναγερμού με την τιμή που αντιστοιχεί στην επίθεση που εντοπίσθηκε. Συγκεκριμένα, η τιμή για Sinkhole είναι alert = 1, η τιμή για Selective Forward Forwarding Ratio είναι alert = 2, η τιμή για Selective Forward Block Node είναι alert = 3, η τιμή για Selective Forward Forwarding Ratio με Blackhole είναι alert = 5 και η τιμή για Selective Forward Block Node με Blackhole είναι alert = 6. Οι τιμές alert = 4 και alert = 7 αφορούν γενικές παραλλαγές της επίθεσης Selective Forward.

Θέτοντας την σημαία alert με την αντίστοιχη τιμή της επίθεσης που διεξάγεται, η κύρια εφαρμογή του συστήματος mIDS προχωρά στην ενεργοποίηση κάποιου μηχανισμού αποκατάστασης. Ο μηχανισμός που θα ενεργοποιηθεί εξαρτάται από την τιμή που έθεσε η κύρια εφαρμογή του κακόβουλου κόμβου στην σημαία αποκατάστασης. Με την επιτυχή ολοκλήρωση ενεργοποίησης ενός μηχανισμού, η κύρια εφαρμογή του συστήματος mIDS επαναφέρει τη σημαία συναγερμού στην τιμή 0. Αυτό συμβαίνει ούτως ώστε το σύστημα mIDS να έχει την δυνατότητα να ανιχνεύσει ξανά κάποια επίθεση που μπορεί να εμφανιστεί. Συμπερασματικά, το σύστημα mIDS ενορχηστρώνει τους μηχανισμούς αποκατάστασης και εξασφαλίζει την λειτουργικότητα της παρούσας λύσης.

4.9 Επιθέσεις μετά από καθυστέρηση



Εικόνα 4.4: Μηχανισμός Σεναρίων Καθυστέρησης

Η προτεινόμενη λύση αξιολογήθηκε σε σενάρια όπου ο κακόβουλος κόμβος εμφανιζόταν εξαρχής μέσα στο δίκτυο και χρησιμοποιούταν τα πρωτόκολλα κόμβου RDC ContikiMAC και RDC Null.

Για περεταίρω εκτίμηση της αποτελεσματικότητας της προτεινόμενης λύσης αναπτύχθηκαν και σενάρια όπου ο κακόβουλος κόμβος εμφανιζόταν μετά από καθυστέρηση μέσα στο δίκτυο όπου και σε αυτά πραγματοποιήθηκε χρήση των δύο αντίστοιχων πρωτοκόλλων. Γενικότερα, σε αυτά τα σενάρια η επίθεση που διεξάγεται στον κακόβουλο κόμβο εμφανίζεται μετά από 1 λεπτό από την στιγμή που δημιουργείται η τοπολογία του δικτύου, δηλαδή στο 3ο λεπτό.

Συγκεκριμένα, η κύρια εφαρμογή του κακόβουλου κόμβου αναλαμβάνει να ενεργοποιήσει τρεις διαδικασίες. Η πρώτη διαδικασία που ενεργοποιείται είναι η διαδικασία που εκτελείται για έναν αξιόπιστο κόμβο που προωθεί πακέτα προς την κεντρική πύλη. Αυτή η διαδικασία εκτελείται για 1 λεπτό μετά από την δημιουργία της τοπολογίας του δικτύου, δηλαδή από το 2ο μέχρι το 3ο λεπτό και έχει την ίδια συμπεριφορά με τις διαδικασίες που εκτελούνται στους αξιόπιστους κόμβους του δικτύου.

Με την ολοκλήρωση της συγκεκριμένης διαδικασίας στο 3ο λεπτό, σηματοδοτείται ο τερματισμός της αξιόπιστης διαδικασίας όπου αναλαμβάνεται από την κύρια εφαρμογή του κακόβουλου κόμβου. Στην συνέχεια, η κύρια εφαρμογή ενεργοποιεί την διαδικασία του συστήματος ανίχνευσης εισβολής mIDS και παράλληλα την διαδικασία κακόβουλης συμπεριφοράς.

Με την επιτυχή ενεργοποίηση των διαδικασιών αυτών η κύρια εφαρμογή τερματίζεται εάν δεν υπάρχει τιμή στην σημαία αποκατάστασης ίση με reboot = 1. Αντιθέτως εάν υπάρχει, τότε η κύρια εφαρμογή του κακόβουλου κόμβου παγώνει, αναμένοντας την σηματοδότηση για επανεκκίνηση. Με τον επιτυχή εντοπισμό της επίθεσης που διεξάγεται στον κακόβουλο κόμβο από το σύστημα mIDS όπως αναγράφεται στο Παράρτημα 4.7, τότε ενεργοποιείται ο μηχανισμός της επανεκκίνησης όπως περιγράφεται στο Παράρτημα 4.6 ή μόνο ο μηχανισμός της επαναδρομολόγησης όπως περιγράφεται στο Παράρτημα 4.5.

Συμπερασματικά, το συγκεκριμένο είδος σεναρίων αναπτύχθηκε για μελέτη πιθανών συμπεριφορών που δύναται να εμφανιστούν στην προτεινόμενη λύση και που δεν εμφανίζονταν στα σενάρια όπου ο κακόβουλος κόμβος υπήρχε εξαρχής μέσα στο δίκτυο. Οι συμπεριφορές αυτές μπορεί να έχουν επιρροή στους μηχανισμούς.

4.10 Μετρήσεις απόδοσης

Στην παρούσα διπλωματική εργασία καταγράφονται τέσσερεις μετρήσεις απόδοσης για αξιολόγηση της αποτελεσματικότητας της προτεινόμενης λύσης. Γενικότερα, όλες οι μετρήσεις αφορούν τα πακέτα πληροφορίας που προωθούνται μέσα στο δίκτυο αλλά και τους χρόνους αποκατάστασης του κακόβουλου κόμβου.

Η πρώτη μέτρηση απόδοσης αντιστοιχεί στα πακέτα που λαμβάνονται από την κεντρική πύλη καταγράφοντας τον μέσο όρο από όλα τα σενάρια. Η μέτρηση αυτή υπολογίζεται μέσω της καταγραφής του αριθμού των μηνυμάτων που εκτυπώνονται από την κεντρική πύλη και είναι τα "packets_received_by_sink" κατά την διάρκεια εκτέλεσης των πειραμάτων.

Η δεύτερη μέτρηση απόδοσης αφορά τα πακέτα τα οποία προωθήθηκαν σε κάποιο κακόβουλο κόμβο και στην συνέχεια απορρίφθηκαν. Και σε αυτή την μέτρηση απόδοσης καταγράφεται ο μέσος όρος των πακέτων από όλα τα σενάρια. Το μήνυμα που εκτυπώνεται κατά την διάρκεια της εκτέλεσης των πειραμάτων από κάποιο κακόβουλο κόμβο που βοηθά στον υπολογισμό της συγκεκριμένης μέτρησης για την επίθεση Selective Forward Block Node είναι το μήνυμα "You have been blocked" για την επίθεση Selective Forward Forwarding Ratio είναι το μήνυμα "did not find a neighbor to foward to" και για την επίθεση Sinkhole είναι το μήνυμα "SinkHole received". Για τους συνδυασμούς επιθέσεων Selective Forward Forwarding Ratio με Blackhole και Selective Forward Block Node με Blackhole εκτυπώνονται τα μηνύματα "did not find a neighbor to foward to" και "You have been blocked" αντίστοιχα.

Η τρίτη μέτρηση απόδοσης αντιστοιχεί στον χρόνο που χρειάστηκε για να ολοκληρωθεί ο μηχανισμός της επαναδρομολόγησης αλλά και της επανεκκίνησης αντίστοιχα. Ο συγκεκριμένος χρόνος μετριέται σε δευτερόλεπτα και καταγράφεται ο μέσος όρος του από όλα τα σενάρια. Τα μηνύματα που εκτυπώνονται στα πειράματα από κάποιο κακόβουλο κόμβο για αξιολόγηση του μηχανισμού επαναδρομολόγησης είναι τα "Broadcasting Alert for Malicious" και "trusted bit 0" ενώ για αξιολόγηση της επανεκκίνησης χρησιμοποιήθηκαν τα μηνύματα "Broadcasting Alert for Malicious" και "Broadcasting Alert Benign".

Η τέταρτη και τελευταία μέτρηση απόδοσης αντιστοιχεί στο ποσοστό επιτυχούς αποκατάστασης. Δηλαδή, από όλα τα σενάρια που εκτελέστηκαν σε πόσα σενάρια εντοπίσθηκε η επίθεση αλλά και ήταν επιτυχής ο μηχανισμός επαναδρομολόγησης ή επανεκκίνησης.

Κεφάλαιο 5

Πειραματικό Περιβάλλον

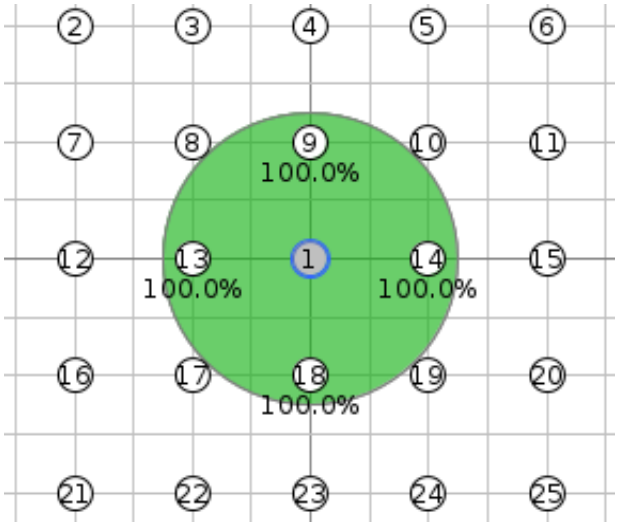
5.1 Επισκόπηση
5.2 Τοπολογία
5.3 Περιβάλλον COOJA και Contiki OS
5.4 Σενάρια αξιολόγησης
5.4.1 Σενάρια Benign
5.4.2 Σενάρια No Recovery
5.4.2.1 - 5.4.2.8 Παραλλαγές σεναρίου No Recovery
5.4.3 Σενάρια Rerouting
5.4.3.1 - 5.4.3.8 Παραλλαγές σεναρίου Rerouting
5.4.4 Σενάρια Rerouting and Reboot
5.4.4.1 - 5.4.4.8 Παραλλαγές σεναρίου Rerouting and Reboot

5.1 Επισκόπηση

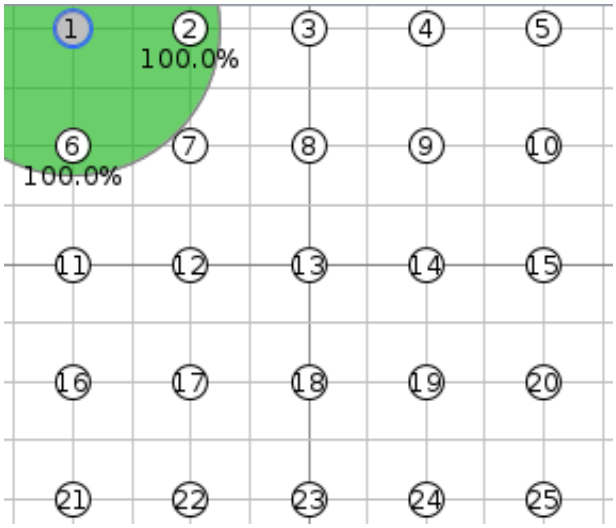
Σε αυτό το κεφάλαιο αναλύονται οι δύο τοπολογίες οι οποίες χρησιμοποιήθηκαν για την αξιολόγηση της πρότασης. Επιπρόσθετα, περιγράφεται το περιβάλλον COOJA μαζί με τα τέσσερα διαφορετικά σενάρια τα οποία εκτελέστηκαν σε αυτό. Τέλος, παρουσιάζονται οι μετρήσεις απόδοσης από κάθε σενάριο με βάση τα πειράματα που πραγματοποιήθηκαν.

5.2 Τοπολογία

Τα σενάρια αξιολόγησης στηρίζονται σε δύο βασικές τοπολογίες για την πραγματοποίηση των πειραμάτων και την παραγωγή των μετρήσεων απόδοσης. Συγκεκριμένα, και στις δύο τοπολογίες υπάρχουν 25 κόμβοι όπου πάντοτε ο ένας από αυτούς αποτελεί την κεντρική πύλη. Η πρώτη τοπολογία είναι αυτή όπου η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου και υπάρχει η δυνατότητα να προωθούνται πακέτα από τέσσερεις γείτονες της. Η δεύτερη τοπολογία είναι αυτή όπου η κεντρική πύλη βρίσκεται στην άκρη του δικτύου και μπορούν να προωθηθούν πακέτα από δύο γείτονες προς αυτήν.



Εικόνα 5.1: Κεντρική Πύλη στο Κέντρο



Εικόνα 5.2: Κεντρική Πύλη στο Άκρο

Η κεντρική πύλη χαρακτηρίζεται από έναν μοναδικό αριθμό, ο οποίος είναι το 1. Επίσης, ένας από τους υπόλοιπους 24 κόμβους αποτελεί τον κακόβουλο κόμβο ο οποίος έχει την δυνατότητα να διεξάγει επίθεση Sinkhole, Blackhole, Selective Forward ή και συνδυασμό μεταξύ Selective Forward με Blackhole. Ο κακόβουλος αυτός κόμβος χρησιμοποιείται για παρεμπόδιση της ομαλής λειτουργίας του δικτύου ούτως ώστε να αξιολογηθεί η προτεινόμενη λύση. Οι υπόλοιποι 23 κόμβοι αποτελούν αξιόλογους κόμβους οι οποίοι προωθούν πακέτα πληροφορίας προς την κεντρική πύλη.

Ο κάθε κόμβος του δικτύου μπορεί να προωθήσει και να παραλάβει πακέτα από τους κόμβους γείτονές του οι οποίοι έχουν την δυνατότητα να βρίσκονται δεξιά, αριστερά πάνω ή κάτω από αυτόν. Αυτό συνεπάγει ότι ο κάθε κόμβος του δικτύου μπορεί να έχει το μέγιστο τέσσερεις γείτονες.

5.3 Περιβάλλον COOJA και Contiki OS

Το Contiki [8] [9] είναι ένα δωρεάν και ανοιχτού κώδικα λειτουργικό σύστημα για προγραμματισμό Διαδικτύου των Πραγμάτων με χρήση της γλώσσας προγραμματισμού C. Ακόμη, μπορεί να χρησιμοποιηθεί για επικοινωνία μεταξύ τσιπ χαμηλής ισχύος σε ασύρματα δίκτυα με υψηλό βαθμό απόδοσης και ασφάλειας.

Αξίζει να σημειωθεί πως το Contiki έχει την δυνατότητα να λειτουργήσει σε δίκτυα που υποστηρίζουν IPv4 και IPv6 αντίστοιχα. Αυτό πραγματοποιείται μέσω της ενσωμάτωσης ελαφρών πρωτοκόλλων τα οποία βοηθούν τα τσιπ χαμηλής ισχύος και ραδιοσυχνοτήτων να μπορούν να συνδεθούν χωρίς προβλήματα απόδοσης.

Ο προγραμματισμός στο λειτουργικό Contiki πραγματοποιείται μέσω του προσομοιωτή δικτύου Cooja [8] [10], στον οποίο διατίθενται οι βασικές βιβλιοθήκες των τσιπ και αισθητήρων σε γλώσσα προγραμματισμού C. Για προγραμματισμό, έλεγχο και παρακολούθηση των συσκευών που ανήκουν στο Διαδίκτυο των Πραγμάτων μπορούν να αναπτυχθούν και να μεταγλωττιστούν σχετικά προγράμματα ούτως ώστε να παραχθούν τα επιθυμητά αποτελέσματα.

Τέλος ο προσομοιωτής Cooja έχει γίνει ένα ευρέως χρησιμοποιούμενο εργαλείο στον τομέα των ασύρματων δικτύων αισθητήρων διότι παρέχει την δυνατότητα προσομοίωσης του φυσικού μέσου. Όλοι οι κόμβοι που χρησιμοποιήθηκαν στα πειράματα είναι Tmote-Sky με εύρος λήψης ακτίνας 25 μέτρων.

5.4 Σενάρια αξιολόγησης

Για αξιολόγηση της προτεινόμενης λύσης χρησιμοποιήθηκαν τέσσερα βασικά σενάρια, όπου το καθένα από αυτά αναφέρεται σε διαφορετικές συμπεριφορές του δικτύου.

Το πρώτο σενάριο αξιολόγησης είναι αυτό του Benign όπου όλοι οι κόμβοι του δικτύου είναι αξιόλογοι, δηλαδή δεν υπάρχει κανένας κακόβουλος κόμβος μέσα στο δίκτυο. Ο κάθε κόμβος προωθεί πακέτα πληροφορίας προς την κεντρική πύλη και με την παραλαβή του κάθε πακέτου γίνεται καταγραφή του. Ο σκοπός αυτού του σεναρίου είναι να παρουσιάσει τον μέσο όρο πακέτων που μπορεί να παραλάβει η κεντρική πύλη εάν δεν υπάρχει κακόβουλη συμπεριφορά.

Το δεύτερο σενάριο αξιολόγησης είναι το No Recovery όπου ο ένας από τους κόμβους του δικτύου είναι κακόβουλος. Στο συγκεκριμένο σενάριο, με τον εντοπισμό του κακόβουλου κόμβου από το σύστημα ανίχνευσης εισβολής δεν πραγματοποιείται κάποια αποκατάσταση στο δίκτυο. Ο σκοπός αυτού του σεναρίου είναι να παρουσιάσει πόσα πακέτα δεν θα παραλάβει η κεντρική πύλη εάν δεν αντιμετωπισθεί ο κακόβουλος κόμβος.

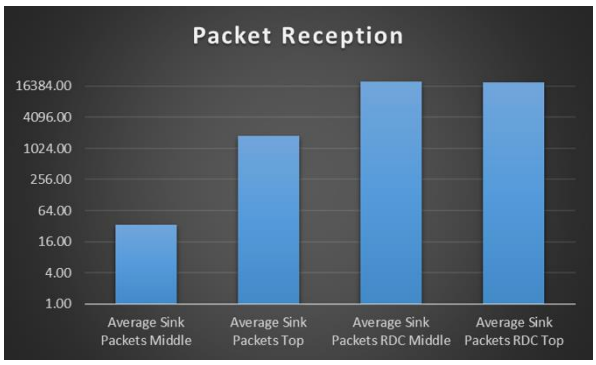
Το τρίτο σενάριο αποτελεί το Rerouting στο οποίο ο ένας από τους κόμβους του δικτύου είναι κακόβουλος. Εάν εντοπισθεί η κακόβουλη συμπεριφορά του από το σύστημα mIDS, τότε ενεργοποιείται ο μηχανισμός της επαναδρομολόγησης. Σκοπός του συγκεκριμένου σεναρίου είναι να αξιολογήσει τον μηχανισμό αυτό. Μέσα από αυτά τα πειράματα μπορεί να εντοπισθεί εάν είναι αποτελεσματικό να χρησιμοποιηθεί μόνο ο μηχανισμός επαναδρομολόγησης.

Το τέταρτο σενάριο αξιολόγησης είναι αυτό του Rerouting and Reboot όπου ο ένας από τους κόμβους του δικτύου είναι κακόβουλος. Σε αυτό το σενάριο η αποκατάσταση που πραγματοποιείται στο δίκτυο με τον επιτυχή εντοπισμό του κακόβουλου κόμβου είναι η επαναδρομολόγηση και η επανεκκίνηση. Με αυτό το σενάριο αξιολογούνται και οι δύο μηχανισμοί αποκατάστασης. Μέσα από αυτά τα πειράματα μπορεί να εντοπισθεί εάν είναι αποτελεσματικό να χρησιμοποιηθούν και οι δύο μηχανισμοί μαζί.

5.4.1 Σενάριο Benign

Για αυτό το σενάριο δημιουργήθηκαν 4 παραλλαγές και κάθε παραλλαγή εκτελέστηκε 10 φορές. Σε κάθε παραλλαγή αλλάζει η τοποθεσία της κεντρικής πύλης (άκρο ή κέντρο του δικτύου) και το πρωτόκολλο κόμβου που χρησιμοποιείται (RDC ContikiMAC ή RDC Null).

Πιο κάτω, δίνεται μια γραφική παράσταση που απεικονίζει τον μέσο όρο πακέτων που παρέλαβε η κεντρική πύλη και ένας πίνακας ο οποίος δείχνει λεπτομερώς τα αποτελέσματα. Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.



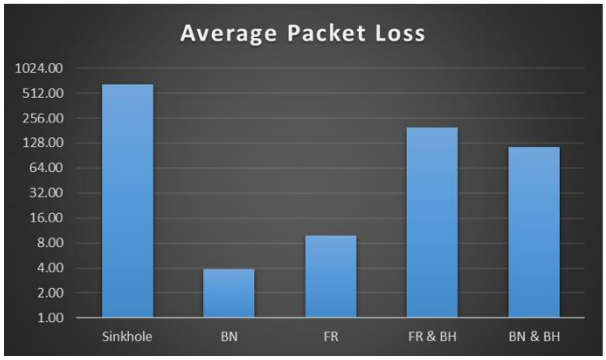
Average Sink Packets Middle	33.77
Average Sink Packets Top	1804.89
Average Sink Packets RDC Middle	19998.60
Average Sink Packets RDC Top	19158.40

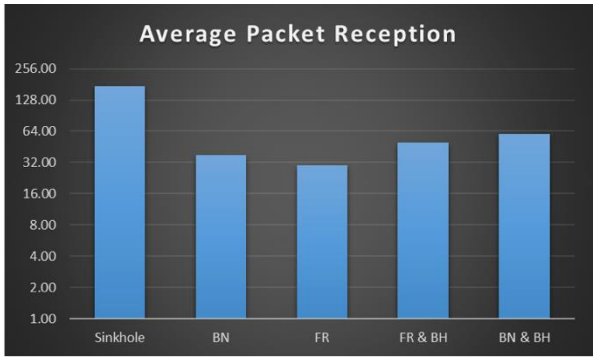
5.4.2 Σενάρια No Recovery

Για αξιολόγηση του σεναρίου No Recovery, αναπτυχθήκαν 8 παραλλαγές σεναρίων, όπου σε κάθε παραλλαγή αλλάζει είτε το πρωτόκολλο κόμβου, είτε χρησιμοποιούνται επιθέσεις μετά από καθυστέρηση. Για κάθε παραλλαγή σεναρίου υλοποιήθηκαν 24 παραλλαγές πειραμάτων όπου σε κάθε παραλλαγή η επίθεση διεξάγεται σε διαφορετικό κόμβο. Επιπρόσθετα, σε κάθε παραλλαγή πραγματοποιούνται 5 εκτελέσεις πειραμάτων, μια για κάθε επίθεση. Για κάθε σενάριο, παρουσιάζεται μια γραφική παράσταση που απεικονίζει τον μέσο όρο πακέτων πληροφορίας που παρέλαβε η κεντρική πύλη αλλά και μια που απεικονίζει τον μέσο όρο πακέτων που χάθηκαν. Επίσης, δίνεται ένας πίνακας ο οποίος δείχνει λεπτομερώς τα αποτελέσματα.

5.4.2.1 Σενάριο No Recovery Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

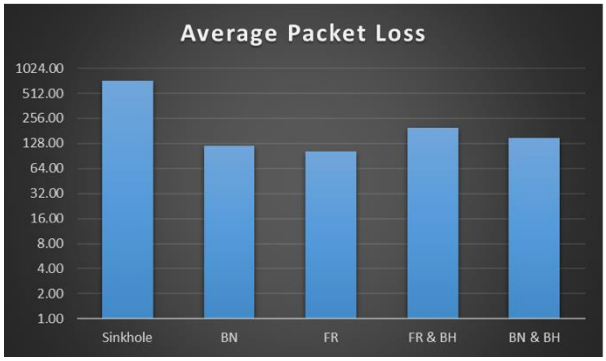


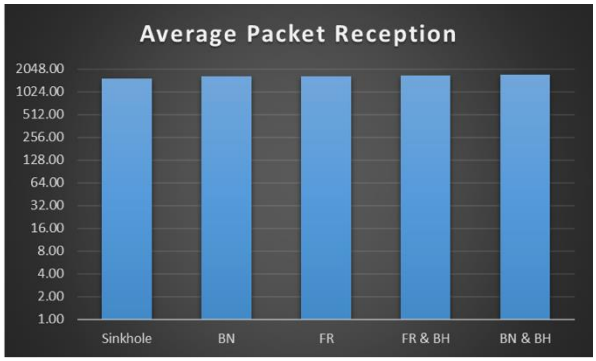


Sinkhole	**Average Packets Lost Mid**	654.87
	Average Sink Packets Mid	172.83
BN	**Average Packets Lost Mid**	3.91
	Average Sink Packets Mid	37.95
FR	**Average Packets Lost Mid**	9.91
	Average Sink Packets Mid	29.91
FR & BH	**Average Packets Lost Mid**	195.37
	Average Sink Packets Mid	49.91
BN & BH	**Average Packets Lost Mid**	113.45
	Average Sink Packets Mid	60.08

5.4.2.2 Σενάριο No Recovery Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

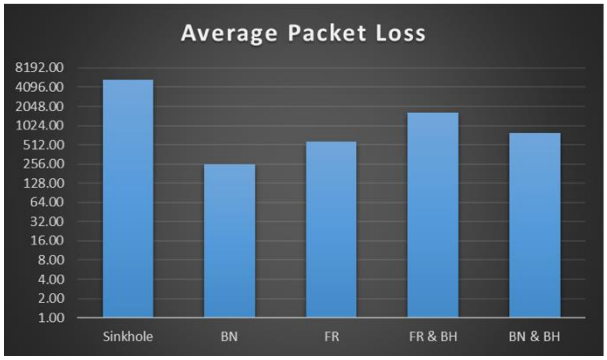


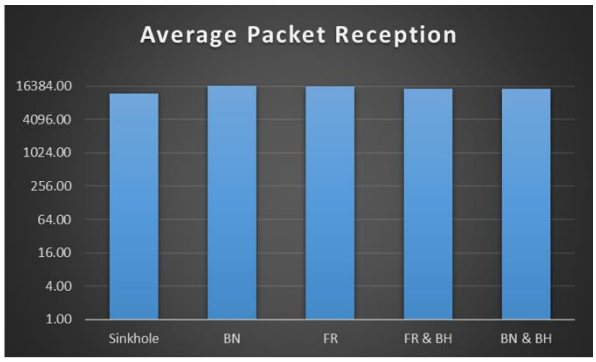


Sinkhole	**Average Packets Lost Top**	721.62
	Average Sink Packets Top	1516.00
BN	**Average Packets Lost Top**	119.04
	Average Sink Packets Top	1642.75
FR	**Average Packets Lost Top**	101.66
	Average Sink Packets Top	1649.25
FR & BH	**Average Packets Lost Top**	197.20
	Average Sink Packets Top	1656.08
BN & BH	**Average Packets Lost Top**	147.20
	Average Sink Packets Top	1715.33

5.4.2.3 Σενάριο No Recovery RDC Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

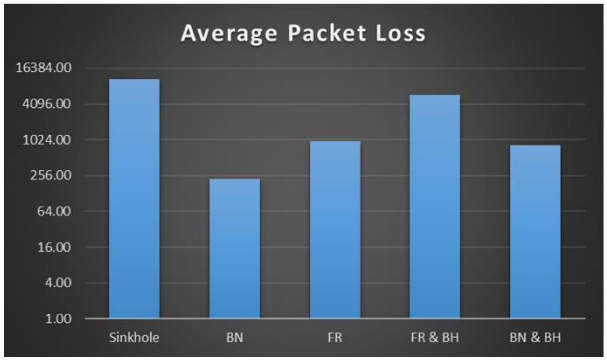


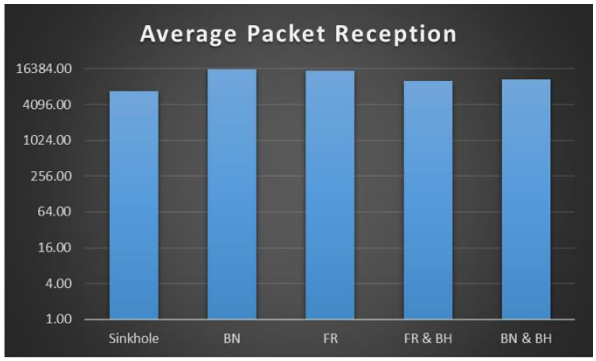


Sinkhole	**Average Packets Lost RDC Mid**	5291.46
	Average Sink Packets RDC Mid	12249.60
BN	**Average Packets Lost RDC Mid**	257.04
	Average Sink Packets RDC Mid	16709.10
FR	**Average Packets Lost RDC Mid**	579.41
	Average Sink Packets RDC Mid	16214.80
FR & BH	**Average Packets Lost RDC Mid**	1628.29
	Average Sink Packets RDC Mid	14946.30
BN & BH	**Average Packets Lost RDC Mid**	786.45
	Average Sink Packets RDC Mid	14917.50

5.4.2.4 Σενάριο No Recovery RDC Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

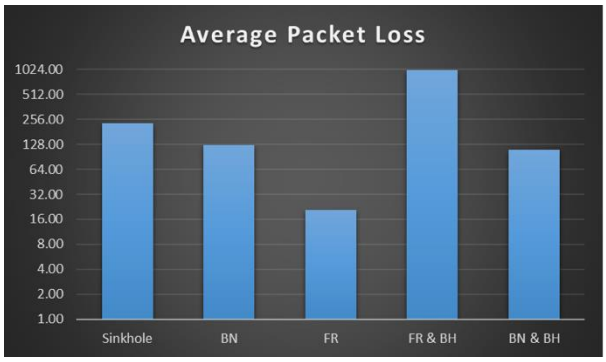


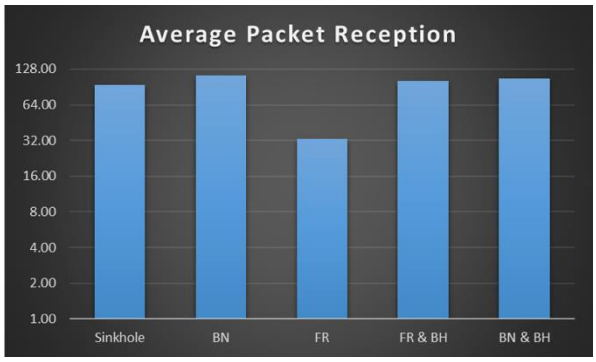


Sinkhole	**Average Packets Lost RDC Top**	10659.40
	Average Sink Packets RDC Top	6806.62
BN	**Average Packets Lost RDC Top**	226.04
	Average Sink Packets RDC Top	16228.80
FR	**Average Packets Lost RDC Top**	953.95
	Average Sink Packets RDC Top	15195.40
FR & BH	**Average Packets Lost RDC Top**	5881.67
	Average Sink Packets RDC Top	10124.20
BN & BH	**Average Packets Lost RDC Top**	841.54
	Average Sink Packets RDC Top	10709.30

5.4.2.5 Σενάριο No Recovery delayed Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

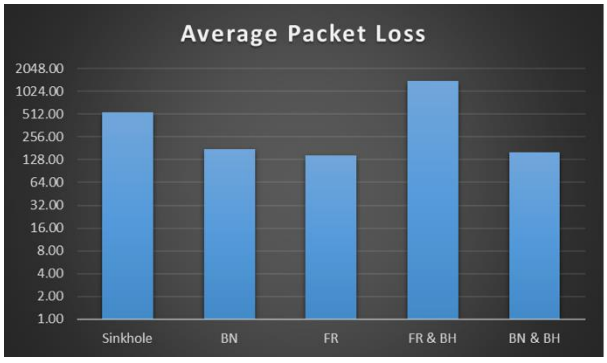


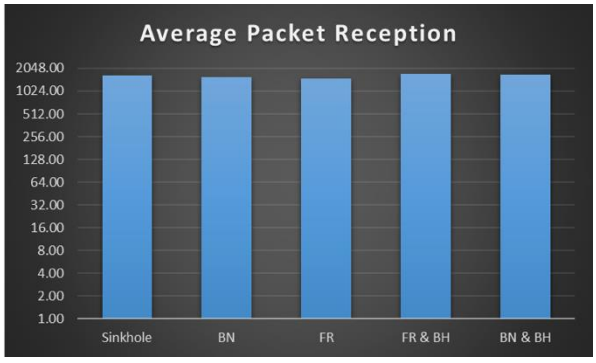


Sinkhole	**Average Packets Lost delayed Mid**	230.95
	Average Sink Packets delayed Mid	94.75
BN	**Average Packets Lost delayed Mid**	126.12
	Average Sink Packets delayed Mid	112.75
FR	**Average Packets Lost delayed Mid**	20.87
	Average Sink Packets delayed Mid	33.20
FR & BH	**Average Packets Lost delayed Mid**	1006.92
	Average Sink Packets delayed Mid	101.79
BN & BH	**Average Packets Lost delayed Mid**	109.62
	Average Sink Packets delayed Mid	107.04

5.4.2.6 Σενάριο No Recovery delayed Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

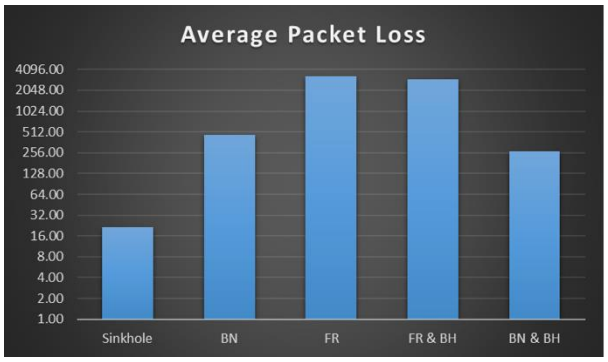


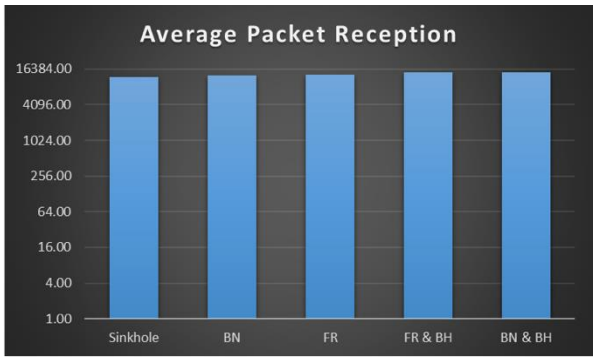


Sinkhole	**Average Packets Lost delayed Top**	545.16
	Average Sink Packets delayed Top	1632.04
BN	**Average Packets Lost delayed Top**	174.83
	Average Sink Packets delayed Top	1578.67
FR	**Average Packets Lost delayed Top**	144.20
	Average Sink Packets delayed Top	1500.38
FR & BH	**Average Packets Lost delayed Top**	1420.96
	Average Sink Packets delayed Top	1710.83
BN & BH	**Average Packets Lost delayed Top**	159.20
	Average Sink Packets delayed Top	1705.21

5.4.2.7 Σενάριο No Recovery delayed RDC Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

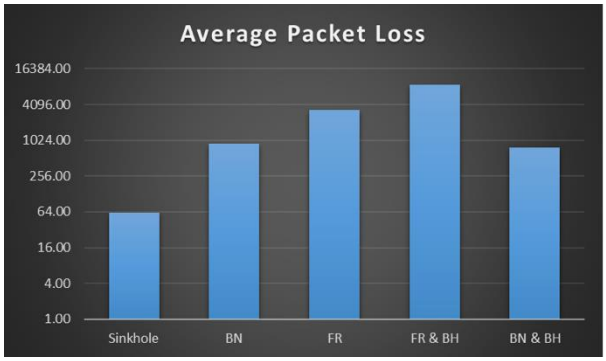


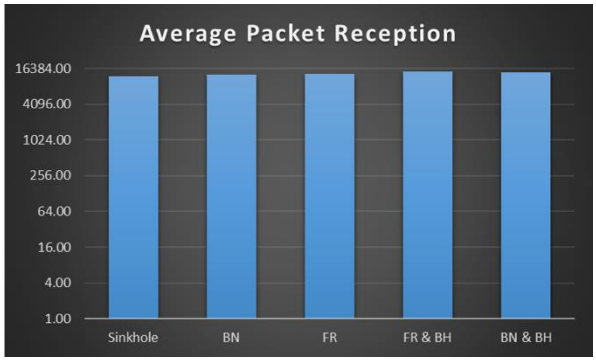


Sinkhole	**Average Packets Lost delayed RDC Mid**	21.41
	Average Sink Packets delayed RDC Mid	12209.20
BN	**Average Packets Lost delayed RDC Mid**	458.66
	Average Sink Packets delayed RDC Mid	12737.30
FR	**Average Packets Lost delayed RDC Mid**	3283.71
	Average Sink Packets delayed RDC Mid	13181.30
FR & BH	**Average Packets Lost delayed RDC Mid**	2919.38
	Average Sink Packets delayed RDC Mid	14533.80
BN & BH	**Average Packets Lost delayed RDC Mid**	271.00
	Average Sink Packets delayed RDC Mid	14249.30

5.4.2.8 Σενάριο No Recovery delayed RDC Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.





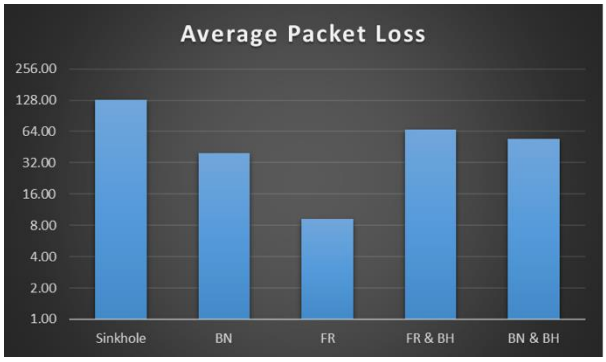
Sinkhole	**Average Packets Lost delayed RDC Top**	62.00
	Average Sink Packets delayed RDC Top	6087.83
BN	**Average Packets Lost delayed RDC Top**	905.62
	Average Sink Packets delayed RDC Top	6937.88
FR	**Average Packets Lost delayed RDC Top**	3283.71
	Average Sink Packets delayed RDC Top	13181.30
FR & BH	**Average Packets Lost delayed RDC Top**	8779.33
	Average Sink Packets delayed RDC Top	9097.83
BN & BH	**Average Packets Lost delayed RDC Top**	760.95
	Average Sink Packets delayed RDC Top	8860.38

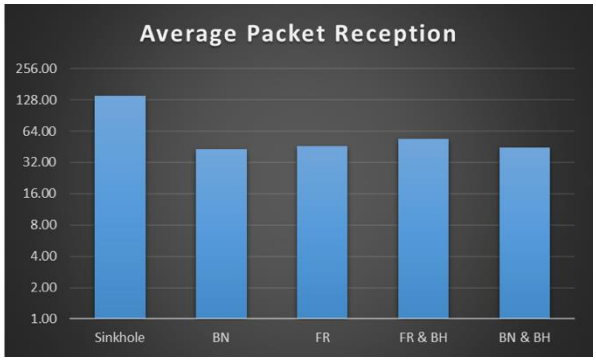
5.4.3 Σενάρια Rerouting

Για το σενάριο Rerouting, αναπτυχθήκαν 8 παραλλαγές σεναρίων και σε κάθε μία αλλάζει είτε το πρωτόκολλο κόμβου, είτε χρησιμοποιούνται επιθέσεις μετά από καθυστέρηση. Για κάθε παραλλαγή σεναρίου υλοποιήθηκαν 24 παραλλαγές πειραμάτων όπου σε κάθε ένα η επίθεση διεξάγεται σε διαφορετικό κόμβο. Σε κάθε παραλλαγή πραγματοποιούνται 5 εκτελέσεις πειραμάτων, μια για κάθε επίθεση. Στα σενάρια, δίνεται μια γραφική παράσταση που απεικονίζει τον μέσο όρο πακέτων που χάθηκαν και μια που απεικονίζει τον μέσο όρο πακέτων που παρέλαβε η κεντρική πύλη. Επιπρόσθετα, δίνεται ένας πίνακας ο οποίος δείχνει λεπτομερώς τα αποτελέσματα, μαζί με τον μέσο όρο χρόνου που χρειάστηκε ο μηχανισμός της επαναδρομολόγησης αλλά και τον μέσο όρο ποσοστού επιτυχούς αποκατάστασης.

5.4.3.1 Σενάριο Rerouting Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC. Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

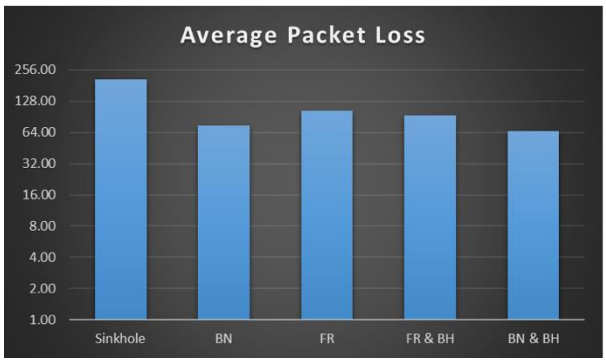


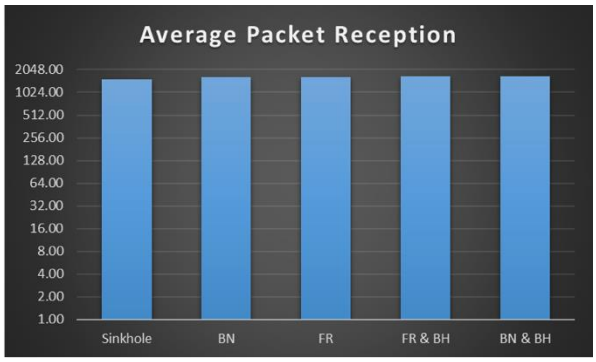


Sinkhole	**Average Packets Lost Mid**	128.41
	Average Sink Packets Mid	139.95
	Average Rerouting Time Mid (sec)	99.70
	Average Recovery Ratio Mid (%)	100.00
BN	**Average Packets Lost Mid**	39.91
	Average Sink Packets Mid	42.79
	Average Rerouting Time Mid (sec)	118.06
	Average Recovery Ratio Mid (%)	25.00
FR	**Average Packets Lost Mid**	9.16
	Average Sink Packets Mid	46.04
	Average Rerouting Time Mid (sec)	66.05
	Average Recovery Ratio Mid (%)	41.66
FR & BH	**Average Packets Lost Mid**	67.00
	Average Sink Packets Mid	53.66
	Average Rerouting Time Mid (sec)	160.40
	Average Recovery Ratio Mid (%)	54.16
BN & BH	**Average Packets Lost Mid**	53.87
	Average Sink Packets Mid	44.70
	Average Rerouting Time Mid (sec)	164.44
	Average Recovery Ratio Mid (%)	41.66

5.4.3.2 Σενάριο Rerouting Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

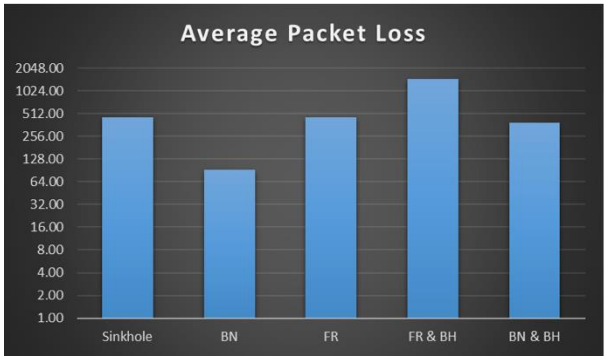


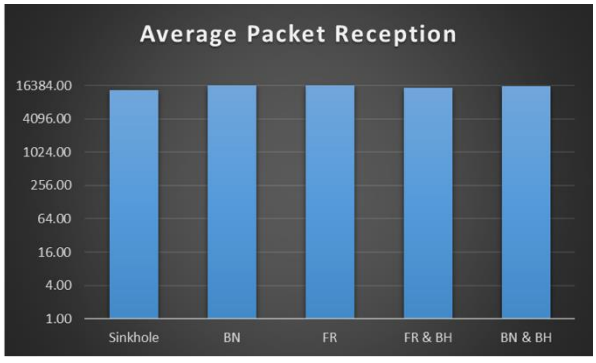


Sinkhole	**Average Packets Lost Top**	208.95
	Average Sink Packets Top	1523.00
	Average Rerouting Time Top (sec)	219.42
	Average Recovery Ratio Top (%)	87.50
BN	**Average Packets Lost Top**	74.33
	Average Sink Packets Top	1612.79
	Average Rerouting Time Top (sec)	163.63
	Average Recovery Ratio Top (%)	87.50
FR	**Average Packets Lost Top**	102.83
	Average Sink Packets Top	1621.38
	Average Rerouting Time Top (sec)	231.97
	Average Recovery Ratio Top (%)	91.66
FR & BH	**Average Packets Lost Top**	92.58
	Average Sink Packets Top	1651.79
	Average Rerouting Time Top (sec)	174.48
	Average Recovery Ratio Top (%)	79.16
BN & BH	**Average Packets Lost Top**	65.66
	Average Sink Packets Top	1681.62
	Average Rerouting Time Top (sec)	214.88
	Average Recovery Ratio Top (%)	75.00

5.4.3.3 Σενάριο Rerouting RDC Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.



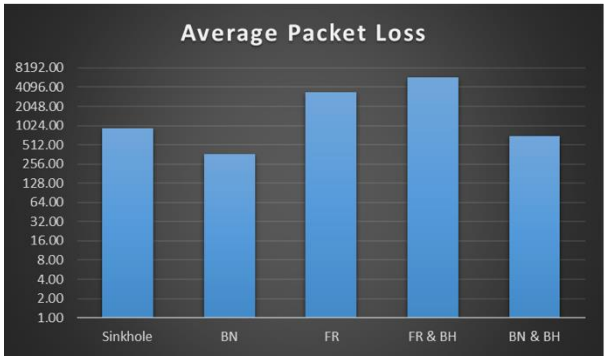


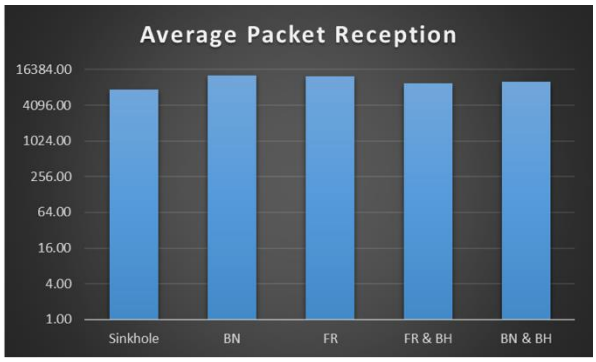
Sinkhole	**Average Packets Lost RDC Mid**	453.33
	Average Sink Packets RDC Mid	13430.80
	Average Rerouting Time RDC Mid (sec)	0.02
	Average Recovery Ratio RDC Mid (%)	100.00
BN	**Average Packets Lost RDC Mid**	92.54
	Average Sink Packets RDC Mid	16691.70
	Average Rerouting Time RDC Mid (sec)	0.02
	Average Recovery Ratio RDC Mid (%)	62.50
FR	**Average Packets Lost RDC Mid**	456.58
	Average Sink Packets RDC Mid	16281.80
	Average Rerouting Time RDC Mid (sec)	0.12
	Average Recovery Ratio RDC Mid (%)	41.66
FR & BH	**Average Packets Lost RDC Mid**	1480.08
	Average Sink Packets RDC Mid	14990.40
	Average Rerouting Time RDC Mid (sec)	0.20
	Average Recovery Ratio RDC Mid (%)	25.00
BN & BH	**Average Packets Lost RDC Mid**	390.25
	Average Sink Packets RDC Mid	15940.70
	Average Rerouting Time RDC Mid (sec)	0.08
	Average Recovery Ratio RDC Mid (%)	75.00

5.4.3.4 Σενάριο Rerouting RDC Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.

Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

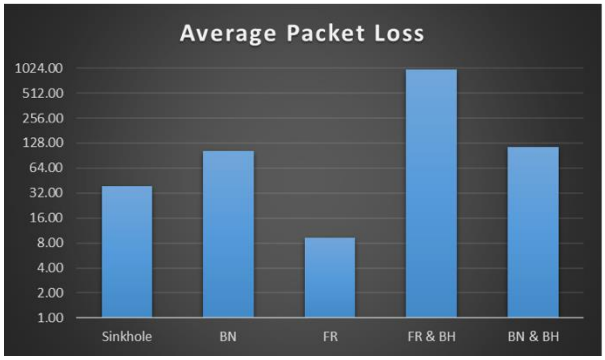


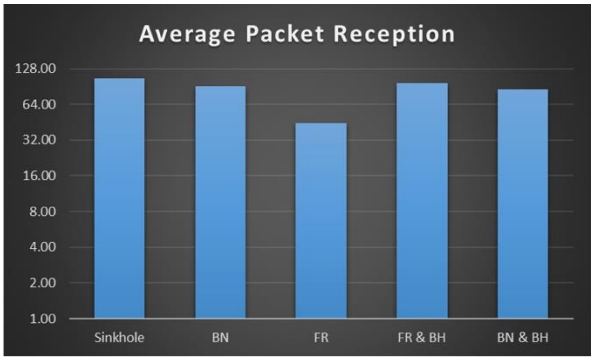


Sinkhole	**Average Packets Lost RDC Top**	920.75
	Average Sink Packets RDC Top	7576.42
	Average Rerouting Time RDC Top (sec)	0.24
	Average Recovery Ratio RDC Top (%)	100.00
BN	**Average Packets Lost RDC Top**	361.58
	Average Sink Packets RDC Top	12993.10
	Average Rerouting Time RDC Top (sec)	0.39
	Average Recovery Ratio RDC Top (%)	70.83
FR	**Average Packets Lost RDC Top**	3397.12
	Average Sink Packets RDC Top	12468.00
	Average Rerouting Time RDC Top (sec)	0.36
	Average Recovery Ratio RDC Top (%)	12.50
FR & BH	**Average Packets Lost RDC Top**	5814.21
	Average Sink Packets RDC Top	9626.46
	Average Rerouting Time RDC Top (sec)	0.00
	Average Recovery Ratio RDC Top (%)	0.00
BN & BH	**Average Packets Lost RDC Top**	696.33
	Average Sink Packets RDC Top	10320.40
	Average Rerouting Time RDC Top (sec)	0.04
	Average Recovery Ratio RDC Top (%)	54.16

5.4.3.5 Σενάριο Rerouting delayed Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

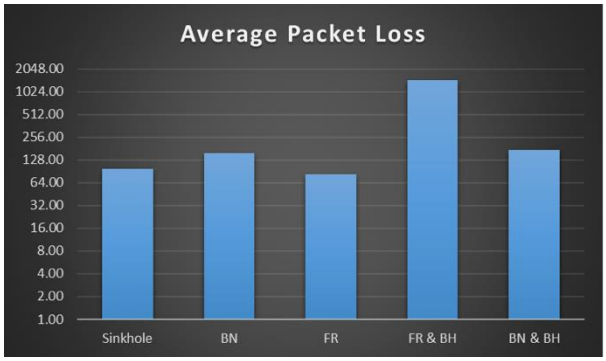


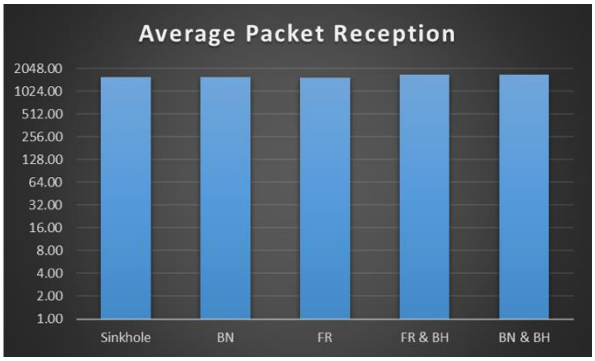


Sinkhole	**Average Packets Lost delayed Mid**	38.66
	Average Sink Packets delayed Mid	105.37
	Average Rerouting Time delayed Mid (sec)	256.61
	Average Recovery Ratio delayed Mid (%)	58.33
BN	**Average Packets Lost delayed Mid**	103.08
	Average Sink Packets delayed Mid	91.12
	Average Rerouting Time delayed Mid (sec)	295.23
	Average Recovery Ratio delayed Mid (%)	12.50
FR	**Average Packets Lost delayed Mid**	9.25
	Average Sink Packets delayed Mid	44.54
	Average Rerouting Time delayed Mid (sec)	62.09
	Average Recovery Ratio delayed Mid (%)	29.16
FR & BH	**Average Packets Lost delayed Mid**	983.54
	Average Sink Packets delayed Mid	97.54
	Average Rerouting Time delayed Mid (sec)	179.38
	Average Recovery Ratio delayed Mid (%)	8.33
BN & BH	**Average Packets Lost delayed Mid**	113.79
	Average Sink Packets delayed Mid	85.66
	Average Rerouting Time delayed Mid (sec)	354.92
	Average Recovery Ratio delayed Mid (%)	12.50

5.4.3.6 Σενάριο Rerouting delayed Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.



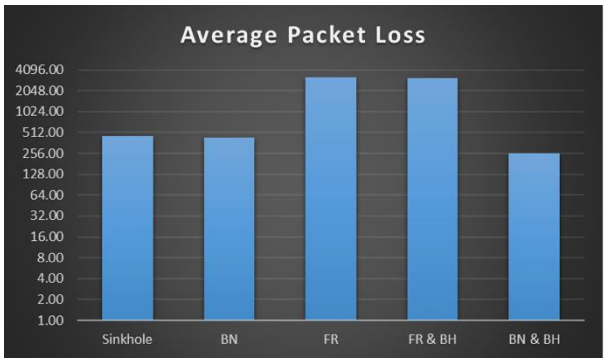


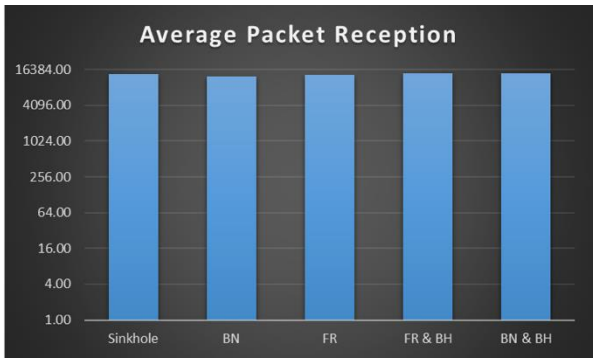
Sinkhole	**Average Packets Lost delayed Top**	98.75
	Average Sink Packets delayed Top	1576.71
	Average Rerouting Time delayed Top (sec)	217.02
	Average Recovery Ratio delayed Top (%)	79.16
BN	**Average Packets Lost delayed Top**	158.00
	Average Sink Packets delayed Top	1572.83
	Average Rerouting Time delayed Top (sec)	403.74
	Average Recovery Ratio delayed Top (%)	8.33
FR	**Average Packets Lost delayed Top**	83.25
	Average Sink Packets delayed Top	1544.58
	Average Rerouting Time delayed Top (sec)	259.92
	Average Recovery Ratio delayed Top (%)	75.00
FR & BH	**Average Packets Lost delayed Top**	1467.08
	Average Sink Packets delayed Top	1709.42
	Average Rerouting Time delayed Top (sec)	129.25
	Average Recovery Ratio delayed Top (%)	8.33
BN & BH	**Average Packets Lost delayed Top**	172.62
	Average Sink Packets delayed Top	1703.88
	Average Rerouting Time delayed Top (sec)	560.42
	Average Recovery Ratio delayed Top (%)	8.33

5.4.3.7 Σενάριο Rerouting delayed RDC Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.

Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

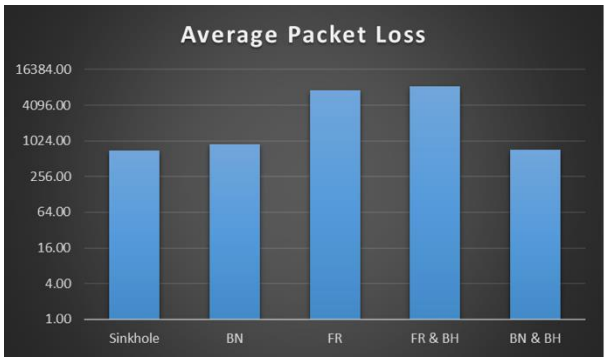


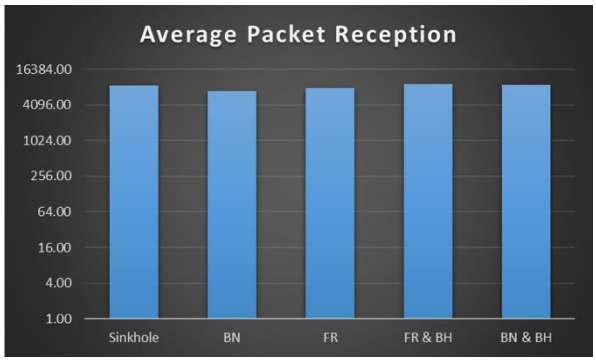


Sinkhole	**Average Packets Lost delayed RDC Mid**	452.12
	Average Sink Packets delayed RDC Mid	13594.80
	Average Rerouting Time delayed RDC Mid (sec)	0.07
	Average Recovery Ratio delayed RDC Mid (%)	100.00
BN	**Average Packets Lost delayed RDC Mid**	433.16
	Average Sink Packets delayed RDC Mid	12529.00
	Average Rerouting Time delayed RDC Mid (sec)	0.03
	Average Recovery Ratio delayed RDC Mid (%)	4.16
FR	**Average Packets Lost delayed RDC Mid**	3226.54
	Average Sink Packets delayed RDC Mid	13131.60
	Average Rerouting Time delayed RDC Mid (sec)	0.00
	Average Recovery Ratio delayed RDC Mid (%)	0.00
FR & BH	**Average Packets Lost delayed RDC Mid**	3125.12
	Average Sink Packets delayed RDC Mid	14194.80
	Average Rerouting Time delayed RDC Mid (sec)	0.00
	Average Recovery Ratio delayed RDC Mid (%)	0.00
BN & BH	**Average Packets Lost delayed RDC Mid**	258.29
	Average Sink Packets delayed RDC Mid	14218.50
	Average Rerouting Time delayed RDC Mid (sec)	0.03
	Average Recovery Ratio delayed RDC Mid (%)	4.16

5.4.3.8 Σενάριο Rerouting delayed RDC Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.





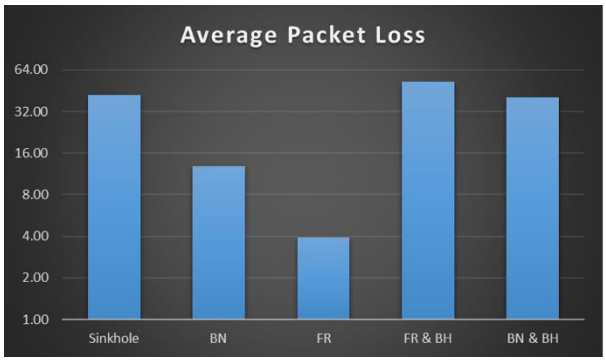
Sinkhole	**Average Packets Lost delayed RDC Top**	697.04
	Average Sink Packets delayed RDC Top	8785.25
	Average Rerouting Time delayed RDC Top (sec)	0.11
	Average Recovery Ratio delayed RDC Top (%)	100.00
BN	**Average Packets Lost delayed RDC Top**	886.95
	Average Sink Packets delayed RDC Top	7085.00
	Average Rerouting Time delayed RDC Top (sec)	0.00
	Average Recovery Ratio delayed RDC Top (%)	0.00
FR	**Average Packets Lost delayed RDC Top**	7279.75
	Average Sink Packets delayed RDC Top	7993.04
	Average Rerouting Time delayed RDC Top (sec)	0.00
	Average Recovery Ratio delayed RDC Top (%)	0.00
FR & BH	**Average Packets Lost delayed RDC Top**	8455.79
	Average Sink Packets delayed RDC Top	9108.25
	Average Rerouting Time delayed RDC Top (sec)	0.06
	Average Recovery Ratio delayed RDC Top (%)	4.16
BN & BH	**Average Packets Lost delayed RDC Top**	731.87
	Average Sink Packets delayed RDC Top	8974.46
	Average Rerouting Time delayed RDC Top (sec)	0.00
	Average Recovery Ratio delayed RDC Top (%)	0.00

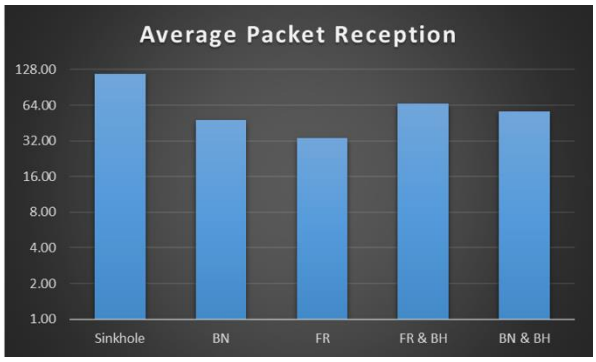
5.4.4 Σενάρια Rerouting and Reboot

Για το σενάριο Rerouting and Reboot, αναπτυχθήκαν 8 παραλλαγές σεναρίων και σε κάθε μία αλλάζει είτε το πρωτόκολλο κόμβου, είτε χρησιμοποιούνται επιθέσεις μετά από καθυστέρηση. Για κάθε παραλλαγή σεναρίου υλοποιήθηκαν 24 παραλλαγές πειραμάτων όπου σε κάθε ένα η επίθεση διεξάγεται σε διαφορετικό κόμβο. Σε κάθε παραλλαγή πραγματοποιούνται 5 εκτελέσεις πειραμάτων, μια για κάθε επίθεση. Στα σενάρια, δίνεται μια γραφική παράσταση που απεικονίζει τον μέσο όρο πακέτων που χάθηκαν και μια που απεικονίζει τον μέσο όρο πακέτων που παρέλαβε η κεντρική πύλη. Επιπρόσθετα, δίνεται ένας πίνακας ο οποίος δείχνει λεπτομερώς τα αποτελέσματα, μαζί με τον μέσο όρο χρόνου που χρειάστηκε ο μηχανισμός της επαναδρομολόγησης αλλά και τον μέσο όρο ποσοστού επιτυχούς αποκατάστασης.

5.4.4.1 Σενάριο Rerouting and Reboot Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

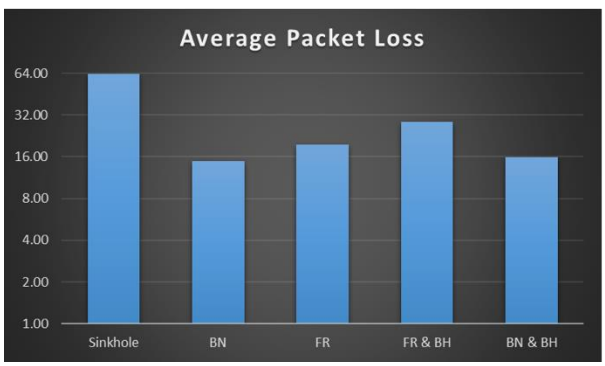


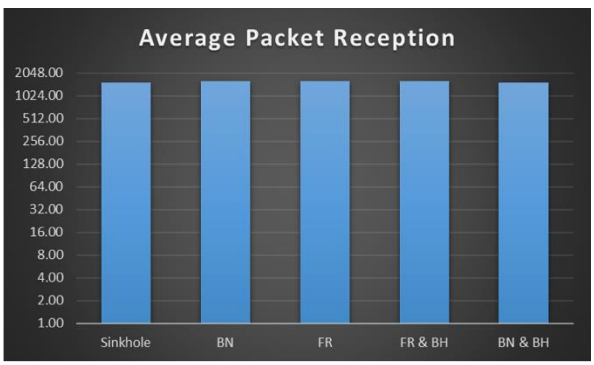


Sinkhole	**Average Packets Lost Mid**	42.08
	Average Sink Packets Mid	116.79
	Average Rerouting Time Mid (sec)	3.92
	Average Rebooting Time Mid (sec)	0.08
	Average Recovery Ratio Mid (%)	100.00
BN	**Average Packets Lost Mid**	12.87
	Average Sink Packets Mid	48.04
	Average Rerouting Time Mid (sec)	0.47
	Average Rebooting Time Mid (sec)	0.17
	Average Recovery Ratio Mid (%)	45.83
FR	**Average Packets Lost Mid**	3.95
	Average Sink Packets Mid	33.91
	Average Rerouting Time Mid (sec)	0.62
	Average Rebooting Time Mid (sec)	0.28
	Average Recovery Ratio Mid (%)	58.33
FR & BH	**Average Packets Lost Mid**	52.29
	Average Sink Packets Mid	65.91
	Average Rerouting Time Mid (sec)	16.62
	Average Rebooting Time Mid (sec)	0.28
	Average Recovery Ratio Mid (%)	87.50
BN & BH	**Average Packets Lost Mid**	40.41
	Average Sink Packets Mid	56.75
	Average Rerouting Time Mid (sec)	48.99
	Average Rebooting Time Mid (sec)	0.17
	Average Recovery Ratio Mid (%)	75

5.4.4.2 Σενάριο Rerouting and Reboot Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.



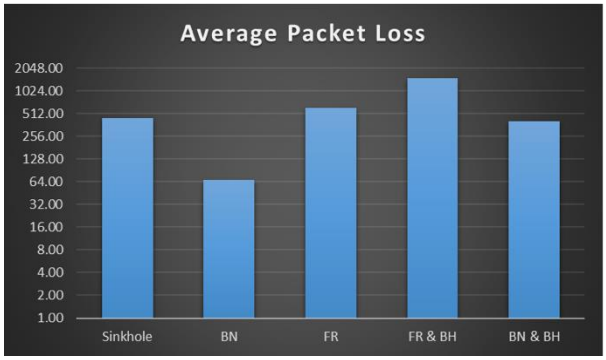


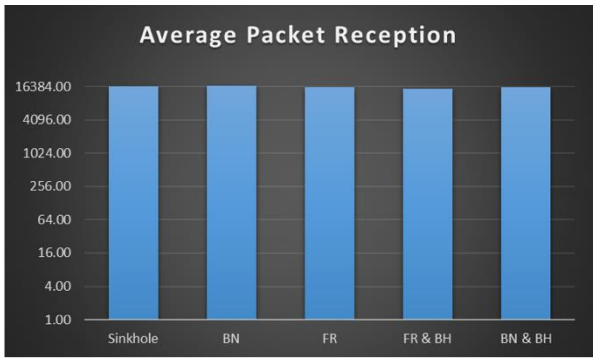
Sinkhole	**Average Packets Lost Top**	63.25
	Average Sink Packets Top	1514.04
	Average Rerouting Time Top (sec)	32.51
	Average Rebooting Time Top (sec)	0.28
	Average Recovery Ratio Top (%)	100.00
BN	**Average Packets Lost Top**	14.83
	Average Sink Packets Top	1594.38
	Average Rerouting Time Top (sec)	18.93
	Average Rebooting Time Top (sec)	0.37
	Average Recovery Ratio Top (%)	87.50
FR	**Average Packets Lost Top**	19.62
	Average Sink Packets Top	1599.42
	Average Rerouting Time Top (sec)	5.40
	Average Rebooting Time Top (sec)	0.37
	Average Recovery Ratio Top (%)	91.66
FR & BH	**Average Packets Lost Top**	28.37
	Average Sink Packets Top	1616.21
	Average Rerouting Time Top (sec)	13.42
	Average Rebooting Time Top (sec)	0.39
	Average Recovery Ratio Top (%)	100.00
BN & BH	**Average Packets Lost Top**	15.79
	Average Sink Packets Top	1527.75
	Average Rerouting Time Top (sec)	11.62
	Average Rebooting Time Top (sec)	0.31
	Average Recovery Ratio Top (%)	100.00

5.4.4.3 Σενάριο Rerouting and Reboot RDC Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.

Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.



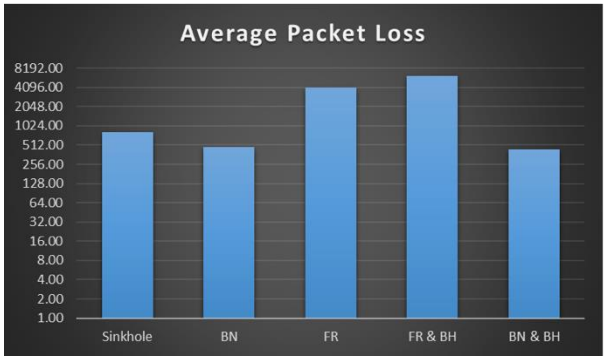


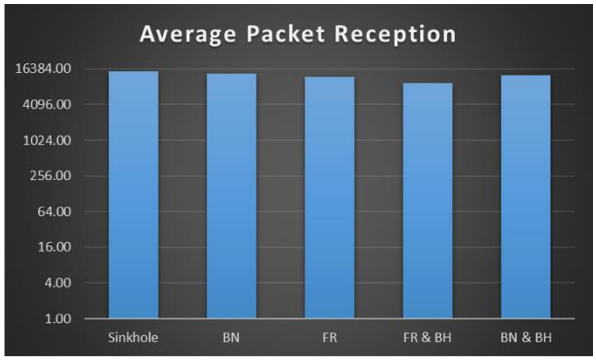
Sinkhole	**Average Packets Lost RDC Mid**	444.87
	Average Sink Packets RDC Mid	16675.30
	Average Rerouting Time RDC Mid (sec)	0.19
	Average Rebooting Time RDC Mid (sec)	0.08
	Average Recovery Ratio RDC Mid (%)	100.00
BN	**Average Packets Lost RDC Mid**	67.79
	Average Sink Packets RDC Mid	17073.90
	Average Rerouting Time RDC Mid (sec)	0.15
	Average Rebooting Time RDC Mid (sec)	0.08
	Average Recovery Ratio RDC Mid (%)	70.83
FR	**Average Packets Lost RDC Mid**	603.41
	Average Sink Packets RDC Mid	16050.90
	Average Rerouting Time RDC Mid (sec)	0.24
	Average Rebooting Time RDC Mid (sec)	0.10
	Average Recovery Ratio RDC Mid (%)	41.66
FR & BH	**Average Packets Lost RDC Mid**	1497.12
	Average Sink Packets RDC Mid	14832.30
	Average Rerouting Time RDC Mid (sec)	0.36
	Average Rebooting Time RDC Mid (sec)	0.09
	Average Recovery Ratio RDC Mid (%)	12.50
BN & BH	**Average Packets Lost RDC Mid**	405.95
	Average Sink Packets RDC Mid	16101.50
	Average Rerouting Time RDC Mid (sec)	0.17
	Average Rebooting Time RDC Mid (sec)	0.09
	Average Recovery Ratio RDC Mid (%)	62.50

5.4.4.4 Σενάριο Rerouting and Reboot RDC Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται από την αρχή και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.

Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.



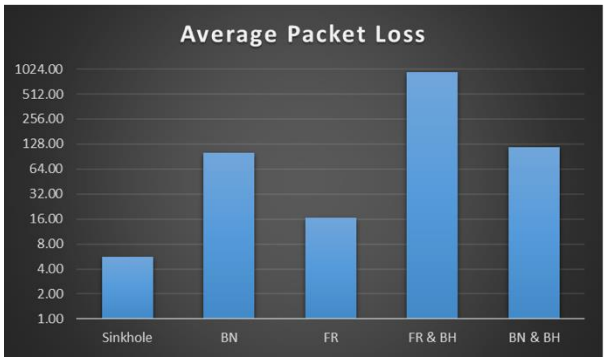


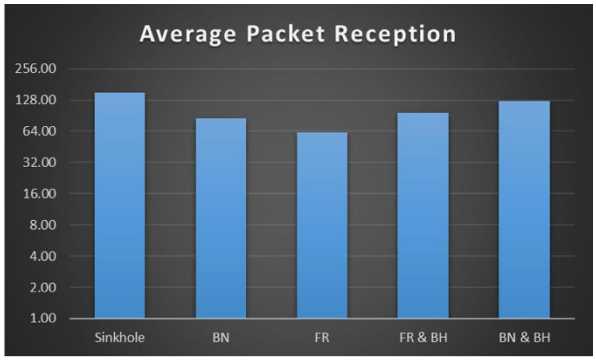
Sinkhole	**Average Packets Lost RDC Top**	818.08
	Average Sink Packets RDC Top	15036.10
	Average Rerouting Time RDC Top (sec)	0.11
	Average Rebooting Time RDC Top (sec)	0.08
	Average Recovery Ratio RDC Top (%)	100.00
BN	**Average Packets Lost RDC Top**	480.33
	Average Sink Packets RDC Top	13741.90
	Average Rerouting Time RDC Top (sec)	0.10
	Average Rebooting Time RDC Top (sec)	0.08
	Average Recovery Ratio RDC Top (%)	58.33
FR	**Average Packets Lost RDC Top**	4059.88
	Average Sink Packets RDC Top	11980.00
	Average Rerouting Time RDC Top (sec)	0.02
	Average Rebooting Time RDC Top (sec)	0.11
	Average Recovery Ratio RDC Top (%)	4.16
FR & BH	**Average Packets Lost RDC Top**	6251.71
	Average Sink Packets RDC Top	9427.83
	Average Rerouting Time RDC Top (sec)	0.00
	Average Rebooting Time RDC Top (sec)	0.00
	Average Recovery Ratio RDC Top (%)	0.00
BN & BH	**Average Packets Lost RDC Top**	437.04
	Average Sink Packets RDC Top	12924.90
	Average Rerouting Time RDC Top (sec)	0.27
	Average Rebooting Time RDC Top (sec)	0.09
	Average Recovery Ratio RDC Top (%)	70.83

5.4.4.5 Σενάριο Rerouting and Reboot delayed Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.

Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.



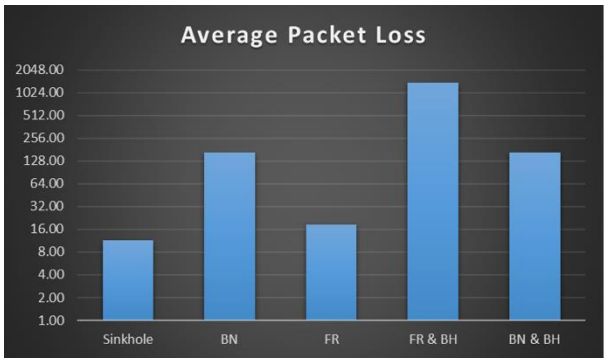


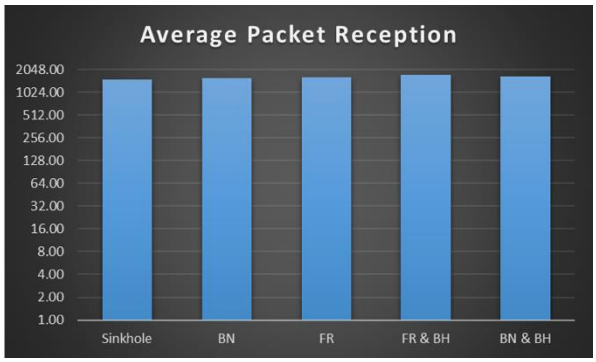
Sinkhole	**Average Packets Lost delayed Mid**	5.62
	Average Sink Packets delayed Mid	150.16
	Average Rerouting Time delayed Mid (sec)	142.10
	Average Rebooting Time delayed Mid (sec)	0.15
	Average Recovery Ratio delayed Mid (%)	100.00
BN	**Average Packets Lost delayed Mid**	100.75
	Average Sink Packets delayed Mid	85.04
	Average Rerouting Time delayed Mid (sec)	45.42
	Average Rebooting Time delayed Mid (sec)	0.16
	Average Recovery Ratio delayed Mid (%)	12.50
FR	**Average Packets Lost delayed Mid**	16.41
	Average Sink Packets delayed Mid	61.79
	Average Rerouting Time delayed Mid (sec)	36.36
	Average Rebooting Time delayed Mid (sec)	0.25
	Average Recovery Ratio delayed Mid (%)	54.16
FR & BH	**Average Packets Lost delayed Mid**	930.37
	Average Sink Packets delayed Mid	96.58
	Average Rerouting Time delayed Mid (sec)	66.37
	Average Rebooting Time delayed Mid (sec)	0.25
	Average Recovery Ratio delayed Mid (%)	12.50
BN & BH	**Average Packets Lost delayed Mid**	116.50
	Average Sink Packets delayed Mid	124.08
	Average Rerouting Time delayed Mid (sec)	107.36
	Average Rebooting Time delayed Mid (sec)	0.11
	Average Recovery Ratio delayed Mid (%)	12.50

5.4.4.6 Σενάριο Rerouting and Reboot delayed Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC ContikiMAC.

Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

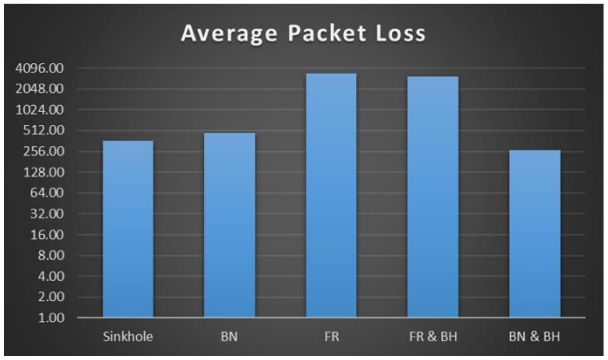


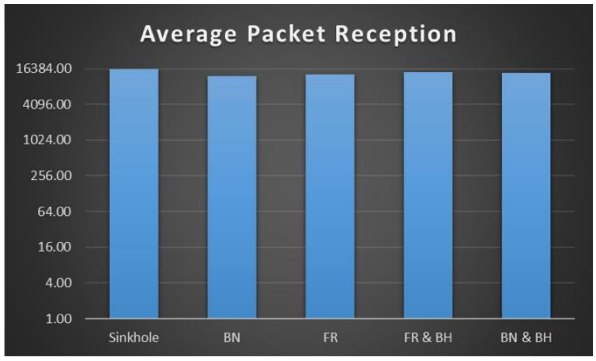


Sinkhole	**Average Packets Lost delayed Top**	11.37
	Average Sink Packets delayed Top	1518.83
	Average Rerouting Time delayed Top (sec)	191.82
	Average Rebooting Time delayed Top (sec)	0.16
	Average Recovery Ratio delayed Top (%)	100.00
BN	**Average Packets Lost delayed Top**	165.16
	Average Sink Packets delayed Top	1601.92
	Average Rerouting Time delayed Top (sec)	146.57
	Average Rebooting Time delayed Top (sec)	0.08
	Average Recovery Ratio delayed Top (%)	4.16
FR	**Average Packets Lost delayed Top**	18.62
	Average Sink Packets delayed Top	1614.38
	Average Rerouting Time delayed Top (sec)	104.24
	Average Rebooting Time delayed Top (sec)	0.28
	Average Recovery Ratio delayed Top (%)	87.50
FR & BH	**Average Packets Lost delayed Top**	1377.46
	Average Sink Packets delayed Top	1747.17
	Average Rerouting Time delayed Top (sec)	63.01
	Average Rebooting Time delayed Top (sec)	0.37
	Average Recovery Ratio delayed Top (%)	8.33
BN & BH	**Average Packets Lost delayed Top**	166.12
	Average Sink Packets delayed Top	1641.50
	Average Rerouting Time delayed Top (sec)	548.56
	Average Rebooting Time delayed Top (sec)	0.08
	Average Recovery Ratio delayed Top (%)	4.16

5.4.4.7 Σενάριο Rerouting and Reboot delayed RDC Mid

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο κέντρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.

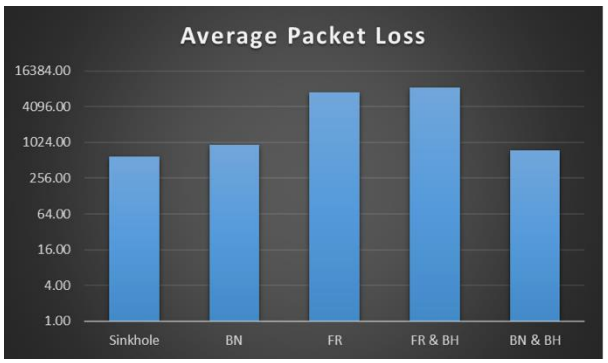


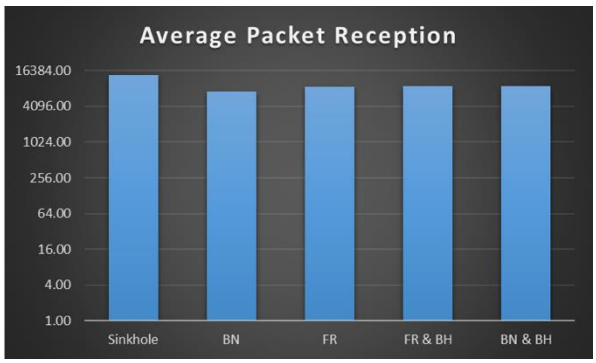


Sinkhole	**Average Packets Lost delayed RDC Mid**	363.91
	Average Sink Packets delayed RDC Mid	16272.20
	Average Rerouting Time delayed RDC Mid (sec)	0.15
	Average Rebooting Time delayed RDC Mid (sec)	0.08
	Average Recovery Ratio delayed RDC Mid (%)	100.00
BN	**Average Packets Lost delayed RDC Mid**	473.79
	Average Sink Packets delayed RDC Mid	12220.00
	Average Rerouting Time delayed RDC Mid (sec)	0.00
	Average Rebooting Time delayed RDC Mid (sec)	0.00
	Average Recovery Ratio delayed RDC Mid (%)	0.00
FR	**Average Packets Lost delayed RDC Mid**	3389.54
	Average Sink Packets delayed RDC Mid	12936.80
	Average Rerouting Time delayed RDC Mid (sec)	0.00
	Average Rebooting Time delayed RDC Mid (sec)	0.00
	Average Recovery Ratio delayed RDC Mid (%)	0.00
FR & BH	**Average Packets Lost delayed RDC Mid**	3081.50
	Average Sink Packets delayed RDC Mid	14157.10
	Average Rerouting Time delayed RDC Mid (sec)	0.02
	Average Rebooting Time delayed RDC Mid (sec)	0.08
	Average Recovery Ratio delayed RDC Mid (%)	8.33
BN & BH	**Average Packets Lost delayed RDC Mid**	264.75
	Average Sink Packets delayed RDC Mid	14091.20
	Average Rerouting Time delayed RDC Mid (sec)	0.00
	Average Rebooting Time delayed RDC Mid (sec)	0.00
	Average Recovery Ratio delayed RDC Mid (%)	0.00

5.4.4.8 Σενάριο Rerouting and Reboot delayed RDC Top

Σε αυτό το σενάριο η κεντρική πύλη βρίσκεται στο άκρο του δικτύου, η επίθεση εμφανίζεται με καθυστέρηση και χρησιμοποιείται πρωτόκολλο κόμβου RDC Null.
Σημείωση: οι αριθμοί στην γραφική παράσταση είναι της δύναμης του 2.





Sinkhole	**Average Packets Lost delayed RDC Top**	588.83
	Average Sink Packets delayed RDC Top	13847.00
	Average Rerouting Time delayed RDC Top (sec)	0.36
	Average Rebooting Time delayed RDC Top (sec)	0.08
	Average Recovery Ratio delayed RDC Top (%)	100.00
BN	**Average Packets Lost delayed RDC Top**	920.37
	Average Sink Packets delayed RDC Top	7259.25
	Average Rerouting Time delayed RDC Top (sec)	0.00
	Average Rebooting Time delayed RDC Top (sec)	0.00
	Average Recovery Ratio delayed RDC Top (%)	0.00
FR	**Average Packets Lost delayed RDC Top**	7028.38
	Average Sink Packets delayed RDC Top	8607.75
	Average Rerouting Time delayed RDC Top (sec)	0.00
	Average Rebooting Time delayed RDC Top (sec)	0.00
	Average Recovery Ratio delayed RDC Top (%)	0.00
FR & BH	**Average Packets Lost delayed RDC Top**	8518.62
	Average Sink Packets delayed RDC Top	8848.21
	Average Rerouting Time delayed RDC Top (sec)	0.00
	Average Rebooting Time delayed RDC Top (sec)	0.00
	Average Recovery Ratio delayed RDC Top (%)	0.00
BN & BH	**Average Packets Lost delayed RDC Top**	741.16
	Average Sink Packets delayed RDC Top	9059.08
	Average Rerouting Time delayed RDC Top (sec)	0.00
	Average Rebooting Time delayed RDC Top (sec)	0.00
	Average Recovery Ratio delayed RDC Top (%)	0.00

Κεφάλαιο 6

Συμπεράσματα

6.1 Επισκόπηση
6.2 Μελλοντική Δουλεία
6.3 Τελικά Συμπεράσματα

6.1 Επισκόπηση

Το πρώτο παράρτημα αναφέρει προτάσεις που μπορούν να εφαρμοστούν κατ' επέκταση της παρούσας διπλωματικής εργασίας ούτως ώστε να αξιολογηθεί περεταίρω η προτεινόμενη λύση. Επίσης, αναφέρονται προτάσεις η οποίες μπορούν να υλοποιηθούν για να υπάρξει βελτίωση στην αντιμετώπιση επιθέσεων αλλά και στην γενίκευση της προτεινόμενης λύσης σε άλλα πρωτόκολλα κόμβου και δρομολόγησης.

Το δεύτερο παράρτημα παρουσιάζει τα συμπεράσματα που εξάγονται από την παρούσα διπλωματική εργασία όσο αφορά την υλοποίηση. Επιπρόσθετα, αναγράφονται συμπεράσματα σχετικά με τα αποτελέσματα των πειραμάτων που διεξαχθήκαν με βάση τα σενάρια αξιολόγησης.

6.2 Μελλοντική Δουλειά

Σε αυτό το παράρτημα περιγράφω κάποια επιπρόσθετη δουλειά που θα μπορούσε να πραγματοποιηθεί στην προτεινόμενη πρόταση, ούτως ώστε να βελτιστοποιηθεί. Αρχικά, θα ήταν αρκετά χρήσιμο το σύστημα εισβολής mIDS να εκπαιδευτεί και στο πρωτόκολλο κόμβου RDC Null. Τα πειράματα που διεξαχθήκαν στην παρούσα διπλωματική εργασία στηρίχθηκαν στα δύο πρωτόκολλα κόμβου RDC ContikiMAC και Null. Με την εκπαίδευση του συστήματος mIDS στο πρωτόκολλο κόμβου RDC Null, τα αποτελέσματα των πειραμάτων που θα εκτελεστούν δύναται να έχουν διαφορές με αυτά της παρούσας διπλωματικής εργασίας.

Επιπρόσθετα, καλό θα ήταν εάν η προτεινόμενη λύση αξιολογείτο και με το πρωτόκολλο δρομολόγησης RPL [30]. Το συγκεκριμένο πρωτόκολλο δρομολογεί πακέτα χρησιμοποιώντας ένα κατευθυνόμενο "άκυκλο γράφο" ως αναπαράσταση του δικτύου, όπου κάθε κόμβος προωθεί πακέτα πληροφορίας στον κόμβο "πατέρα" με τελικό προορισμό των πακέτων την κεντρική πύλη. Επίσης, κάθε κόμβος γνωρίζει τους ενεργούς γείτονες του και επιλέγει ως κόμβο "πατέρα" του τον κόμβο που βρίσκεται πιο κοντά στην κεντρική πύλη. Αυτό έχει ως αποτέλεσμα σε συγκεκριμένες περιπτώσεις, ένας κόμβος να έχει διαφορετικό κόμβο "πατέρα" σε διαφορετική χρονική στιγμή. Συνεπώς, η προτεινόμενη λύση δύναται να παρουσιάσει διαφορετικά αποτελέσματα όταν πραγματοποιείται χρήση αυτού του πρωτόκολλου.

Ακόμη, καλό θα ήταν εάν στην προτεινόμενη λύση αναπτυχθούν περεταίρω τα σενάρια αξιολόγησης όπου ο κακόβουλος κόμβος εμφανίζεται μετά από καθυστέρηση μέσα στο δίκτυο. Θα μπορούσαν να αναπτυχθούν ποικίλα σενάρια με μεταβλητούς χρόνους εμφάνισης του κακόβουλου κόμβου στο δίκτυο ούτως ώστε να αξιολογηθεί περαιτέρω η προτεινόμενη λύση. Η απρόβλεπτη εμφάνιση ενός κακόβουλου κόμβου μέσα στο δίκτυο μπορεί να έχει επιδράσεις στο σύστημα ανίχνευσης εισβολής mIDS το οποίο εντοπίζει τις επιθέσεις που διεξάγονται σε ένα κόμβο. Επίσης, εάν η εμφάνιση του κακόβουλου κόμβου είναι απρόβλεπτη μπορεί να έχει επιρροή και στους μηχανισμούς αποκατάστασης του δικτύου.

Επίσης, σημαντικό θα ήταν εάν πραγματοποιείτο ανάπτυξη σεναρίων όπου υπάρχουν περισσότεροι από ένα κακόβουλο κόμβο μέσα στο δίκτυο. Με την εμφάνιση περαιτέρω κακόβουλων κόμβων μπορεί να παρουσιαστεί περισσότερη συμφόρηση μέσα στο δίκτυο από τα πακέτα συνδέσμου ασφαλείας που θα στέλνουν οι κακόβουλοι κόμβοι. Συνεπώς, δύναται να υπάρξει ανάγκη για αλλαγή του χρόνου που στέλνεται το συγκεκριμένο πακέτο μέσα στο δίκτυο καθώς και η ποσότητα του. Ίσως, τα συγκεκριμένα πακέτα θα μπορούσαν να προωθούνται μέσα στο δίκτυο από ένα κεντρικό σύστημα υπεύθυνο για τον συγκεκριμένο μηχανισμό. Δηλαδή, αντί το κάθε πακέτο να στέλνεται από τον κάθε κακόβουλο κόμβο τοπικά, ο κόμβος να στέλνει ένα μήνυμα ενημέρωσης στο κεντρικό σύστημα το οποίο με την σειρά του θα ενεργοποιήσει τον μηχανισμό ενημέρωσης.

Τέλος, η προτεινόμενη λύση θα μπορούσε να αξιολογηθεί στην πλατφόρμα FIT-IOT η οποία είναι ανοιχτή και δοκιμασμένη. Αποτελείται από 2728 ασύρματους κόμβους χαμηλής ισχύος και 117 φορητά ρομπότ διαθέσιμα για πειραματισμό με ασύρματες τεχνολογίες Διαδικτύου των Πραγμάτων. Η τεχνολογίες αυτές είναι μεγάλης κλίμακας, που κυμαίνονται από πρωτόκολλα χαμηλού επιπέδου έως προηγμένες υπηρεσίες διαδικτύου.

6.3 Τελικά Συμπεράσματα

Στην παρούσα διπλωματική εργασία προτάθηκαν και υλοποιήθηκαν δύο μηχανισμοί αποκατάστασης. Οι μηχανισμοί της επαναδρομολόγησης και της επανεκκίνησης, αξιολογήθηκαν σε ποικίλα σενάρια αξιολόγησης όπου πραγματοποιείτο χρήση δύο διαφορετικών πρωτοκόλλων κόμβου, του RDC ContikiMAC και Null. Αξιολογήθηκαν σε σενάρια όπου η επίθεση που διεξαγόταν σε κάποιο κακόβουλο κόμβο εμφανιζόταν μετά από καθυστέρηση και σε σενάρια όπου η θέση της κεντρικής πύλης άλλαζε στο δίκτυο. Τέλος, οι δύο αυτοί μηχανισμοί αξιολογήθηκαν σε 5 διαφορετικά είδη επιθέσεων.

Από τα πειράματα που εκτελέστηκαν, μπορούμε εύκολα να εντοπίσουμε πως η προτεινόμενη λύση αναδεικνύεται όταν πραγματοποιείται χρήση του πρωτόκολλου κόμβου RDC Null. Η κεντρική πύλη παραλαμβάνει πολύ μεγαλύτερο αριθμό πακέτων όταν χρησιμοποιείται το πρωτόκολλο κόμβου RDC Null παρά το RDC ContikiMAC. Αυτό συμβαίνει λόγω του ότι το RDC ContikiMAC προωθεί το ίδιο πακέτο μέχρι να γίνει επιτυχής η παραλαβή του από τον κόμβο παραλήπτη. Με αυτό τον τρόπο πραγματοποιείται τεράστια συμφόρηση στο δίκτυο, πράγμα που δεν εμφανίζεται στο πρωτόκολλο κόμβου RDC Null το οποίο δεν χρησιμοποιεί αναμετάδοση πακέτων.

Ακόμη, παρατηρήθηκε πως η προτεινόμενη λύση λειτουργεί ορθά στην αποκατάσταση κόμβου και δικτύου όταν ο κακόβουλος κόμβος εμφανίζεται στο $3^{ο}$ λεπτό μιας προσομοίωσης. Αυτό σημαίνει πως δεν εμφανίζεται κάποια αρνητική επίπτωση στην παραλαβή πακέτων από την κεντρική πύλη ή στους μηχανισμούς επαναδρομολόγησης και επανεκκίνησης.

Επιπρόσθετα, εντοπίσθηκε πως η θέση της κεντρικής πύλης στην τοπολογία του δικτύου δύναται να επηρεάσει την παραλαβή πακέτων. Αυτό συμβαίνει λόγω του ότι εάν η κεντρική πύλη βρίσκεται στο άκρο του δικτύου έχει διαθέσιμους μόνο δύο γείτονες που μπορούν να προωθήσουν πακέτα πληροφορίας σε αυτή. Αντιθέτως, εάν βρίσκεται στο κέντρο του δικτύου, η κεντρική πύλη μπορεί να παραλάβει πακέτα από τέσσερεις γείτονες.

Σημαντικό ρόλο έχει και το είδος επίθεσης που διεξάγεται σε κάποιο κακόβουλο κόμβο. Σύμφωνα με τα αποτελέσματα που παράχθηκαν από τα πειράματα που εκτελέστηκαν, είναι εύκολο να εντοπίσουμε πως το είδος επίθεσης επηρεάζει την επιτυχή παραλαβή πακέτων από την κεντρική πύλη. Συνεπώς, οι επιθέσεις που διεξάγονται διαφέρουν σε κρισιμότητα και στις επιπτώσεις που μπορούν να επιφέρουν σε κάποιο δίκτυο.

Βιβλιογραφία

[1] R. Samson Jr, «Prevention Vs Detection-Based Security Approach,».

[2] A. Salihefendic, «Reactive vs. proactive development,» December 11, 2015.

[3] V. Nkosi, «Top 10 Biggest IoT Security Issues,» July 30, 2020.

[4] A. Rawat, «Binary Logistic Regression,» October 31, 2017.

[5] S. Paul, K. Sabnani, H. Lin και S. Bhattacharyya, «Reliable multicast transport protocol (RMTP),» April 1997.

[6] H. Patil και T. Chen, «Computer and Information Security Handbook (Third Edition),» 2017.

[7] E. Fazeldehkordi και O. Akanbi, «A Study of Black Hole Attack Solutions,» 2016.

[8] K. Gaurav, «Programming Internet of Things using Contiki and Cooja,» June 17, 2017.

[9] Dunkels, Adam and Gronvall, Bjorn and Voigt, Thiemo, «Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors,» σε Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, USA, 2004.

[10] F. Österlind, J. Eriksson και A. Dunkels, «Cooja TimeLine: A Power Visualizer for Sensor Network Simulation,» σε Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems, New York, NY, USA, 2010.

[11] A. Dunkels, «The ContikiMAC Radio Duty Cycling Protocol,» σε SICS Technical Report T2011:13, ISSN 1100-31542017, December 2011.

[12] Pedro, «MAC protocols in ContikiOS,» November 8, 2014.

[13] C. Ioannou και V. Vassiliou, «The Impact of Network Layer Attacks in Wireless Sensor Networks,» σε International Workshop on Secure Internet of Things (SIoT 2016), Crete, 2016.

[14] C. Ioannou και V. Vassiliou, «Classifying Security Attacks in IoT Networks Using Supervised Learning,» σε 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2019.

[15] C. Ioannou και V. Vassiliou, «An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression,» σε Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Montreal, 2018.

[16] Da Silva, A. P. R. and Martins, M. H. T. and Rocha, B. P. S. and Loureiro, A. A. F. and Ruiz, L. B. and Wong, H. C., «Decentralized Intrusion Detection in Wireless Sensor Networks,» σε Proceedings of the 1st ACM International Workshop on Quality of Service &Amp; Security in Wireless and Mobile Networks, New York, NY, USA, 2005.

[17] P. Konstantinides, «Αποκατάσταση κόμβου και δικτύου στο Διαδίκτυο των Πραγμάτων,» May, 2020.

[18] E. Stavrou και A. Pitsillides, «Recovering from the selective forwarding attack in WSNs - enhancing the recovery benefits of blacklisting and rerouting using directional antennas,» σε 2014 Internation.

[19] F. Song και B. Zhao, «Trust-Based LEACH Protocol for Wireless Sensor Networks,» σε 2008 Second International Conference on Future Generation Communication and Networking, 2008.

[20] G. Ma, X. Li, Q. Pei και Z. Li, «A Security Routing Protocol for Internet of Things Based on RPL,» σε 2017 International Conference on Networking and Network Applications (NaNA), 2017.

[21] Nadeem, Adnan and Howarth, Michael P, «An Intrusion Detection & Adaptive Response Mechanism for MANETs,» Ad Hoc Networks, τόμ. 13, p. 368–380, 2014.

[22] S. Raza, L. Wallgren και T. Voigt, «SVELTE: Real-time Intrusion Detection in the Internet of Things,» Ad hoc networks, τόμ. 11, p. 2661–2674, 2013.

[23] S. Tanachaiwiwat, P. Dave, R. Bhindwale και A. Helmy, «Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks,» σε IEEE Interna.

[24] Wang, Shiau-Huey and Tseng, Chinyang Henry and Levitt, Karl and Bishop, Matthew, «Cost-Sensitive Intrusion Responses For Mobile Ad Hoc Networks,» σε International Workshop on Recent Advances in Intrusion Detection, 2007.

[25] Z. Cao, J. Hu, Z. Chen, M. Xu και X. Zhou, «Feedback: Towards Dynamic Behavior and Secure Routing forWireless Sensor Networks,» 2006.

[26] Z. Zhao, H. Hu, G. Ahn και R. Wu, «Risk-Aware Response for Mitigating MANET Routing Attack.

[27] A.-u. Rehman, S. U. Rehman και H. Raheem, «Sinkhole Attacks in Wireless Sensor Networks: A Survey,» Wireless Personal Communications, τόμ. 106, p. 2291–2313, 016 2019.

[28] C. Karlof και D. Wagner, «Secure routing in wireless sensor networks: attacks and countermeasures,» Ad Hoc Networks, τόμ. 1, pp. 293-315, 2003.

[29] L. Bysani και A. Turuk, «A Survey on Selective Forwarding Attack in Wireless Sensor Networks,» σε 2011 International Conference on Devices and Communications (ICDeCom), March 24, 2011.

[30] M. Efthymiou, «ΑΝΙΧΝΕΥΣΗ ΕΠΙΘΕΣΕΩΝ RPL ΣΕ ΔΙΚΤΥΑ IOT,» May, 2011.

Παράρτημα Α

Σε αυτό το παράρτημα παρατίθεται κομμάτι του κώδικα που χρησιμοποιήθηκε για τους μηχανισμούς αποκατάστασης οι οποίοι ενεργοποιούνται από το σύστημα ανίχνευσης εισβολής mIDS.

```
/*Selective Forward - Forwarding Ratio*/
   if(select_FR>= 1){
      printf("WSP: Virus Selective Forward Forwarding Ratio %ld.%03u \n",
(long)select_FR,(unsigned)((select_FR-floor(select_FR))*1000));
      mids_wsp_attack.alert=2;
   }


   /*Selective Forward - Block Node*/
   if(select_BN>=1){
      printf("WSP: Virus Selective Forward Block Node %ld.%03u \n", (long)select_BN,(unsigned)((select_BN-
floor(select_BN))*1000));
      mids_wsp_attack.alert=3;
   }

   /*Selective Forward - in general*/
   if(selective_forward >=1){
      printf("WSP: Virus Selective Forward Attack %ld.%03u \n",
(long)selective_forward,(unsigned)((selective_forward-floor(selective_forward))*1000));
      mids_wsp_attack.alert=4;
   }
   /*Selective Forward & Blackhole - Forwarding Ratio*/
   if(select_bl_FR>= 1){
      printf("WSP: Virus Selective Forward + Blackhole Forwarding Ratio %ld.%03u \n",
(long)select_bl_FR,(unsigned)((select_bl_FR-floor(select_bl_FR))*1000));

      mids_wsp_attack.alert=5;

   }
   /*Selective Forward & Blackhole - Block Node*/
   if(select_bl_BN>=1){
      printf("WSP: Virus Selective Forward + Blackhole Block Node %ld.%03u \n",
(long)select_bl_BN,(unsigned)((select_bl_BN-floor(select_bl_BN))*1000));
      mids_wsp_attack.alert=6;

   }
   /*Selective Forward & Blackhole*/
   if(selective_blackhole>=1){
      printf("WSP: Virus Selective Forward + Blackhole Attacks %ld.%03u \n",
(long)selective_blackhole,(unsigned)((selective_blackhole-floor(selective_blackhole))*1000));
      mids_wsp_attack.alert=7;

   }
```

```
   /*Sinkhole attack*/
   if(sinkhole_BLR>=1){
      printf("WSP: Virus Sinkhole %ld.%03u \n", (long)sinkhole_BLR,(unsigned)((sinkhole_BLR-
floor(sinkhole_BLR))*1000));
      mids_wsp_attack.alert=1;
   }

      if (mids_wsp_attack.alert >= 1) {
         if(mids_wsp_stats.reboot == 1)
            process_start(&recovery_malicious_transimision_reboot,NULL);
         else if (mids_wsp_stats.reroute == 1)
            process_start(&recovery_malicious,NULL);
         else
            printf("No Recovery \n");
      }

   mids_wsp_attack.alert=0;
```

Παράρτημα Β

Σε αυτό το παράρτημα παρατίθεται ο κώδικας που χρησιμοποιήθηκε για την επεξεργασία των μετρήσεων απόδοσης από τα αρχεία αποτελεσμάτων των πειραμάτων που εκτελέστηκαν.

```
#!/bin/bash

my_solutions=(
benign
benign_rdc
benign_top
benign_rdc_top

malicious_no_recovery
malicious_no_recovery_rdc
malicious_no_recovery_delayed
malicious_no_recovery_rdc_delayed
malicious_no_recovery_top
malicious_no_recovery_rdc_top
malicious_no_recovery_delayed_top
malicious_no_recovery_rdc_delayed_top

rerouting_only
rerouting_only_rdc
rerouting_only_delayed
rerouting_only_rdc_delayed
rerouting_only_top
rerouting_only_rdc_top
rerouting_only_delayed_top
rerouting_only_rdc_delayed_top

trans_with_reboot
trans_with_reboot_rdc
trans_with_reboot_delayed
trans_with_reboot_rdc_delayed
trans_with_reboot_top
trans_with_reboot_rdc_top
trans_with_reboot_delayed_top
trans_with_reboot_rdc_delayed_top
)

my_attacks=(SinkHole ForwardingAlgorithm-BlockNode ForwardingAlgorithm-SelectiveForward
ForwardingAlgorithm-SelectiveForward-Blackhole ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole)

for s in "${my_solutions[@]}"
do

shopt -s extglob
echo "${s//@(_rdc|_top|_delayed)}_scenario"
cd "${s//@(_rdc|_top|_delayed)}_scenario"
```

```
cd $s

if [ ${s//@(_rdc|_delayed)} == benign ]
then
rm benign-packetData.txt
for c in {1..10}
do
grep -c "packets_received_by_sink" benign-middle$c.log >> benign-packetData.txt
done
awk '{sum+=$1} END { print "Average Sink Packets = ",sum/(NR-1)}' benign-packetData.txt >> benign-
packetData.txt
cd ..
cd ..
elif [ ${s//@(_rdc|_delayed)} == benign_top ]
then
rm benign-packetData.txt
for c in {1..10}
do
grep -c "packets_received_by_sink" benign-top$c.log >> benign-packetData.txt
done
awk '{sum+=$1} END { print "Average Sink Packets = ",sum/(NR-1)}' benign-packetData.txt >> benign-
packetData.txt
cd ..
cd ..
else

for a in "${my_attacks[@]}"
do

if [[ $s == *"top"* ]]
then
cd "${a}_top_logs"
else
cd "${a}_logs"
fi

for c in {2..25}
do

if [ $a == ForwardingAlgorithm-BlockNode ]
then
if [[ $s == *"top"* ]]
then
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
```

```
fi
mal2=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-BlockNode-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
mal=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-BlockNode-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-top-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-BlockNode-stats.txt
else
grep -c "You have been blocked" malicious-top-ID$c.log >> ForwardingAlgorithm-BlockNode-stats.txt
fi
else
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-BlockNode-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1}')
mal=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-BlockNode-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-middle-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-BlockNode-
stats.txt
else
grep -c "You have been blocked" malicious-middle-ID$c.log >> ForwardingAlgorithm-BlockNode-stats.txt
fi
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward ]
then
if [[ $s == *"top"* ]]
then
if [[ $s != *"no_recovery"* ]]
then
```

```
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-SelectiveForward-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
mal=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-SelectiveForward-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-top-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-SelectiveForward-
stats.txt
else
grep -c -E "did not find a neighbor to foward to" malicious-top-ID$c.log >> ForwardingAlgorithm-
SelectiveForward-stats.txt
fi
else
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-SelectiveForward-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1}')
mal=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-SelectiveForward-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-middle-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-
SelectiveForward-stats.txt
else
```

```
grep -c -E "did not find a neighbor to foward to" malicious-middle-ID$c.log >> ForwardingAlgorithm-
SelectiveForward-stats.txt
fi
fi
fi

if [ $a == SinkHole ]
then
if [[ $s == *"top"* ]]
then
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" "$mal2">> SinkHole-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
mal=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" >> SinkHole-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-top-ID$c.log | sort -n | tail -n 1 >> SinkHole-stats.txt
else
grep -c "SinkHole received" malicious-top-ID$c.log >> SinkHole-stats.txt
fi
else
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" "$mal2" >> SinkHole-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1}')
```

```
mal=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" >> SinkHole-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-middle-ID$c.log | sort -n | tail -n 1 >> SinkHole-stats.txt
else
grep -c "SinkHole received" malicious-middle-ID$c.log >> SinkHole-stats.txt
fi
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-Blackhole ]
then
if [[ $s == *"top"* ]]
then
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-SelectiveForward-Blackhole-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
mal=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-SelectiveForward-Blackhole-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-top-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-SelectiveForward-
Blackhole-stats.txt
else
grep -c "did not find a neighbor to foward to" malicious-top-ID$c.log >> ForwardingAlgorithm-SelectiveForward-
Blackhole-stats.txt
fi
else
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
```

```
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-SelectiveForward-Blackhole-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1}')
mal=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print
$1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-SelectiveForward-Blackhole-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-middle-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-
SelectiveForward-Blackhole-stats.txt
else
grep -c "did not find a neighbor to foward to" malicious-middle-ID$c.log >> ForwardingAlgorithm-
SelectiveForward-Blackhole-stats.txt
fi
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole ]
then
if [[ $s == *"top"* ]]
then
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{
if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-top-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
mal=$(grep "\- trusted bit 0" malicious-top-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-top-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-SelectiveForward-
BlockNode-Blackhole-stats.txt
```

```
else
grep -c "You have been blocked" malicious-top-ID$c.log >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats.txt
fi
else
if [[ $s != *"no_recovery"* ]]
then
if [[ $s == *"reboot"* ]]
then
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
if [[ $s == *"delayed"* ]]
then
mal=$(grep ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk -v norm="$norm" '{ if($1>norm) print $1 }' | head -n 1)
else
mal=$(grep -m1 ":$c:Broadcasting Alert Benign" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1 }')
fi
mal2=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" "$mal2" >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats2.txt
else
norm=$(grep -m1 ":$c:Broadcasting Alert for Malicious" malicious-middle-ID$c.log | sed 's/:.*//' | awk '{ print $1}')
mal=$(grep "\- trusted bit 0" malicious-middle-ID$c.log | awk -F':' '!seen[$2]++' | tail -1 | sed 's/:.*//' | awk '{ print $1}')
echo "$norm" "$mal" >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats2.txt
fi
fi
if [[ $s == *"delayed"* ]]
then
grep -oP "pckdrop\s+\K\w+" malicious-middle-ID$c.log | sort -n | tail -n 1 >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats.txt
else
grep -c "You have been blocked" malicious-middle-ID$c.log >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats.txt
fi
fi
fi

done

for c in {2..25}
do

if [ $a == ForwardingAlgorithm-BlockNode ]
then
if [[ $s == *"top"* ]]
then
grep -c "packets_received_by_sink" malicious-top-ID$c.log >> ForwardingAlgorithm-BlockNode-stats.txt
else
grep -c "packets_received_by_sink" malicious-middle-ID$c.log >> ForwardingAlgorithm-BlockNode-stats.txt
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward ]
```

```
then
if [[ $s == *"top"* ]]
then
grep -c "packets_received_by_sink" malicious-top-ID$c.log >> ForwardingAlgorithm-SelectiveForward-stats.txt
else
grep -c "packets_received_by_sink" malicious-middle-ID$c.log >> ForwardingAlgorithm-SelectiveForward-
stats.txt
fi
fi

if [ $a == SinkHole ]
then
if [[ $s == *"top"* ]]
then
grep -c "packets_received_by_sink" malicious-top-ID$c.log >> SinkHole-stats.txt
else
grep -c "packets_received_by_sink" malicious-middle-ID$c.log >> SinkHole-stats.txt
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-Blackhole ]
then
if [[ $s == *"top"* ]]
then
grep -c "packets_received_by_sink" malicious-top-ID$c.log >> ForwardingAlgorithm-SelectiveForward-Blackhole-
stats.txt
else
grep -c "packets_received_by_sink" malicious-middle-ID$c.log >> ForwardingAlgorithm-SelectiveForward-
Blackhole-stats.txt
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole ]
then
if [[ $s == *"top"* ]]
then
grep -c "packets_received_by_sink" malicious-top-ID$c.log >> ForwardingAlgorithm-SelectiveForward-
BlockNode-Blackhole-stats.txt
else
grep -c "packets_received_by_sink" malicious-middle-ID$c.log >> ForwardingAlgorithm-SelectiveForward-
BlockNode-Blackhole-stats.txt
fi
fi

done

if [ $a == ForwardingAlgorithm-BlockNode ]
then
pr -2 -t ForwardingAlgorithm-BlockNode-stats.txt > ForwardingAlgorithm-BlockNode-packetData.txt
rm ForwardingAlgorithm-BlockNode-stats.txt
awk '{sum+=$1} END { print "Average Packets Lost = ",sum/NR}' ForwardingAlgorithm-BlockNode-packetData.txt
>> ForwardingAlgorithm-BlockNode-packetData.txt
if [[ $s != *"no_recovery"* ]]
then
```

```
awk 'NF > 1' ForwardingAlgorithm-BlockNode-stats2.txt > ForwardingAlgorithm-BlockNode-recoveryData.txt
if [[ $s == *"reboot"* ]]
then
awk '{if($3>0) sum+=$3-$1} END { print "Average Rerouting Time = ",sum/NR/1000000}' ForwardingAlgorithm-
BlockNode-recoveryData.txt >> ForwardingAlgorithm-BlockNode-recoveryData.txt
awk '{sum+=$2-$1} END { print "Average Reboot Time = ",sum/(NR-1)/1000000 - 10}' ForwardingAlgorithm-
BlockNode-recoveryData.txt >> ForwardingAlgorithm-BlockNode-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-2)/24}' ForwardingAlgorithm-BlockNode-
recoveryData.txt >> ForwardingAlgorithm-BlockNode-recoveryData.txt
else
awk '{sum+=$2-$1} END { print "Average Rerouting Time = ",sum/(NR)/1000000}' ForwardingAlgorithm-
BlockNode-recoveryData.txt >> ForwardingAlgorithm-BlockNode-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-1)/24}' ForwardingAlgorithm-BlockNode-
recoveryData.txt >> ForwardingAlgorithm-BlockNode-recoveryData.txt
fi
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward ]
then
pr -2 -t ForwardingAlgorithm-SelectiveForward-stats.txt > ForwardingAlgorithm-SelectiveForward-packetData.txt
rm ForwardingAlgorithm-SelectiveForward-stats.txt
awk '{sum+=$1} END { print "Average Packets Lost = ",sum/NR}' ForwardingAlgorithm-SelectiveForward-
packetData.txt >> ForwardingAlgorithm-SelectiveForward-packetData.txt
if [[ $s != *"no_recovery"* ]]
then
awk 'NF > 1' ForwardingAlgorithm-SelectiveForward-stats2.txt > ForwardingAlgorithm-SelectiveForward-
recoveryData.txt
if [[ $s == *"reboot"* ]]
then
awk '{ if($3>0) sum+=$3-$1} END { print "Average Rerouting Time = ",sum/NR/1000000}' ForwardingAlgorithm-
SelectiveForward-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-recoveryData.txt
awk '{sum+=$2-$1} END { print "Average Reboot Time = ",sum/(NR-1)/1000000 - 10}' ForwardingAlgorithm-
SelectiveForward-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-2)/24}' ForwardingAlgorithm-SelectiveForward-
recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-recoveryData.txt
else
awk '{sum+=$2-$1} END { print "Average Rerouting Time = ",sum/(NR)/1000000}' ForwardingAlgorithm-
SelectiveForward-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-1)/24}' ForwardingAlgorithm-SelectiveForward-
recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-recoveryData.txt
fi
fi
fi

if [ $a == SinkHole ]
then
pr -2 -t SinkHole-stats.txt > SinkHole-packetData.txt
rm SinkHole-stats.txt
awk '{sum+=$1} END { print "Average Packets Lost = ",sum/NR}' SinkHole-packetData.txt >> SinkHole-
packetData.txt
if [[ $s != *"no_recovery"* ]]
then
awk 'NF > 1' SinkHole-stats2.txt > SinkHole-recoveryData.txt
```

```
if [[ $s == *"reboot"* ]]
then
awk '{if($3>0) sum+=$3-$1} END { print "Average Rerouting Time = ",sum/NR/1000000}' SinkHole-recoveryData.txt >> SinkHole-recoveryData.txt
awk '{sum+=$2-$1} END { print "Average Reboot Time = ",sum/(NR-1)/1000000 - 10}' SinkHole-recoveryData.txt >> SinkHole-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-2)/24}' SinkHole-recoveryData.txt >> SinkHole-recoveryData.txt
else
awk '{sum+=$2-$1} END { print "Average Rerouting Time = ",sum/(NR)/1000000}' SinkHole-recoveryData.txt >> SinkHole-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-1)/24}' SinkHole-recoveryData.txt >> SinkHole-recoveryData.txt
fi
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-Blackhole ]
then
pr -2 -t ForwardingAlgorithm-SelectiveForward-Blackhole-stats.txt > ForwardingAlgorithm-SelectiveForward-Blackhole-packetData.txt
rm ForwardingAlgorithm-SelectiveForward-Blackhole-stats.txt
awk '{sum+=$1} END { print "Average Packets Lost = ",sum/NR}' ForwardingAlgorithm-SelectiveForward-Blackhole-packetData.txt >> ForwardingAlgorithm-SelectiveForward-Blackhole-packetData.txt
if [[ $s != *"no_recovery"* ]]
then
awk 'NF > 1' ForwardingAlgorithm-SelectiveForward-Blackhole-stats2.txt > ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt
if [[ $s == *"reboot"* ]]
then
awk '{if($3>0) sum+=$3-$1} END { print "Average Rerouting Time = ",sum/NR/1000000}' ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt
awk '{sum+=$2-$1} END { print "Average Reboot Time = ",sum/(NR-1)/1000000 - 10}' ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-2)/24}' ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt
else
awk '{sum+=$2-$1} END { print "Average Rerouting Time = ",sum/(NR)/1000000}' ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-1)/24}' ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-Blackhole-recoveryData.txt
fi
fi
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole ]
then
pr -2 -t ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats.txt > ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-packetData.txt
rm ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats.txt
```

```
awk '{sum+=$1} END { print "Average Packets Lost = ",sum/NR}' ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-packetData.txt >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-packetData.txt
if [[ $s != *"no_recovery"* ]]
then
awk 'NF > 1' ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-stats2.txt > ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt
if [[ $s == *"reboot"* ]]
then
awk '{if($3>0) sum+=$3-$1} END { print "Average Rerouting Time = ",sum/NR/1000000}' ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt
awk '{sum+=$2-$1} END { print "Average Reboot Time = ",sum/(NR-1)/1000000 - 10}' ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-2)/24}' ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt
else
awk '{sum+=$2-$1} END { print "Average Rerouting Time = ",sum/(NR)/1000000}' ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt
awk 'END { print "Successful Recovery Ratio(%) = ",100*(NR-1)/24}' ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-recoveryData.txt
fi
fi
fi

if [ $a == ForwardingAlgorithm-BlockNode ]
then
    awk '{sum+=$2} END { print "Average Sink Packets = ",sum/(NR-1)}' ForwardingAlgorithm-BlockNode-packetData.txt >> ForwardingAlgorithm-BlockNode-packetData.txt
fi

if [ $a == ForwardingAlgorithm-SelectiveForward ]
then
    awk '{sum+=$2} END { print "Average Sink Packets = ",sum/(NR-1)}' ForwardingAlgorithm-SelectiveForward-packetData.txt >> ForwardingAlgorithm-SelectiveForward-packetData.txt
fi

if [ $a == SinkHole ]
then
    awk '{sum+=$2} END { print "Average Sink Packets = ",sum/(NR-1)}' SinkHole-packetData.txt >> SinkHole-packetData.txt
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-Blackhole ]
then
    awk '{sum+=$2} END { print "Average Sink Packets = ",sum/(NR-1)}' ForwardingAlgorithm-SelectiveForward-Blackhole-packetData.txt >> ForwardingAlgorithm-SelectiveForward-Blackhole-packetData.txt
fi

if [ $a == ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole ]
```

```
then
    awk '{sum+=$2} END { print "Average Sink Packets = ",sum/(NR-1)}' ForwardingAlgorithm-SelectiveForward-
BlockNode-Blackhole-packetData.txt >> ForwardingAlgorithm-SelectiveForward-BlockNode-Blackhole-
packetData.txt
fi

if [[ $s != *"no_recovery"* ]]
then
rm *stats2*
fi

cd ..

done

cd ..
cd ..

fi

done
```

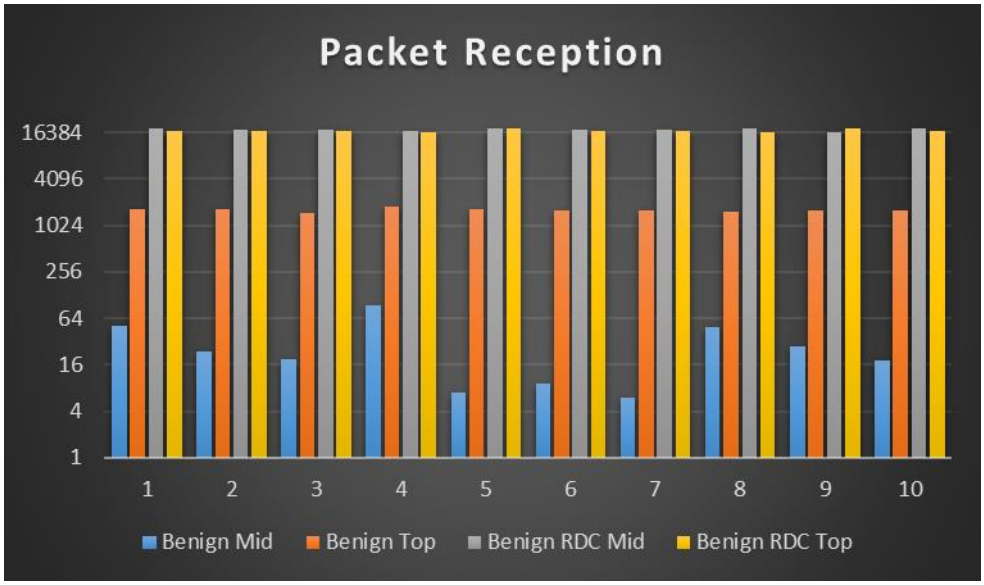
Παράρτημα Γ

Σε αυτό το παράρτημα παρατίθενται λεπτομερείς μετρήσεις για κάθε ξεχωριστό σενάριο Benign, No Recovery, Rerouting και Rerouting and Reboot. Για το σενάριο Benign παρουσιάζεται μια γραφική παράσταση που απεικονίζει τα πακέτα που παρέλαβε η κεντρική πύλη σε κάθε εκτέλεση των τεσσάρων παραλλαγών.

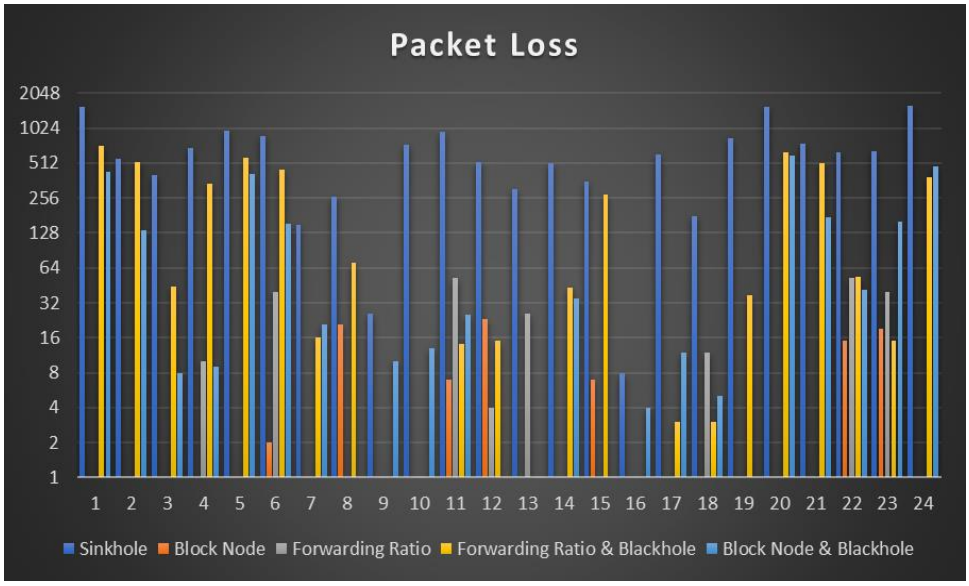
Συγκεκριμένα, για κάθε άλλο ξεχωριστό σενάριο, παρουσιάζεται μια γραφική παράσταση που απεικονίζει τα πακέτα που χάθηκαν αλλά και μια που απεικονίζει τα πακέτα που παρέλαβε η κεντρική πύλη για κάθε παραλλαγή.

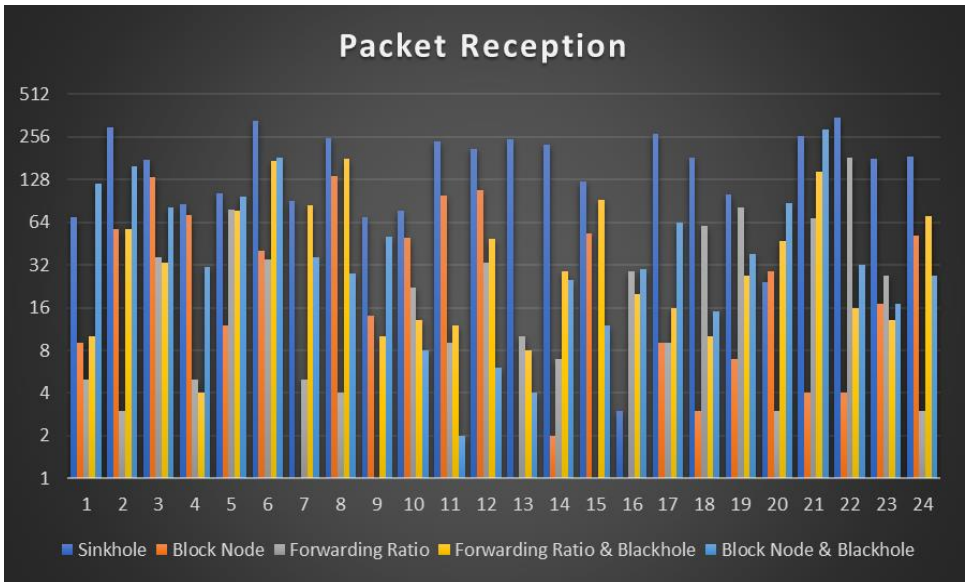
Επιπρόσθετα, δίνεται ένας πίνακας ο οποίος δείχνει λεπτομερώς τα αποτελέσματα με τα πακέτα που χάθηκαν και παραλήφθηκαν από την κεντρική πύλη για κάθε παραλλαγή και διαφορετική επίθεση.

Run	Benign Mid	Benign Top	Benign RDC Mid	Benign RDC Top
1	51	1664	18700	17333
2	24	1678	17914	17009
3	19	1494	17914	17007
4	93	1818	17327	16589
5	7	1669	18693	18689
6	9	1599	17920	17065
7	6	1580	17836	17074
8	49	1532	18692	16281
9	28	1584	16369	18209
10	18	1626	18622	17170

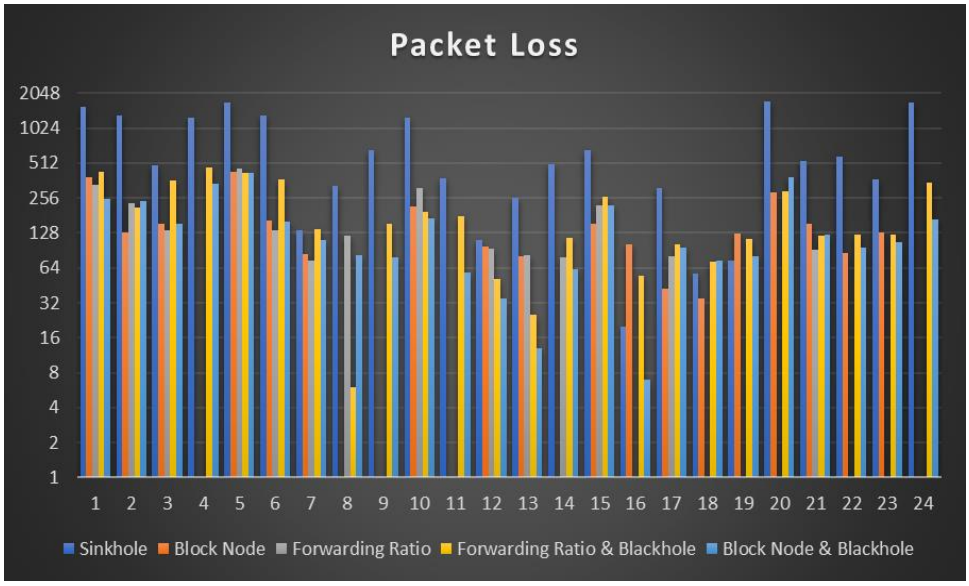


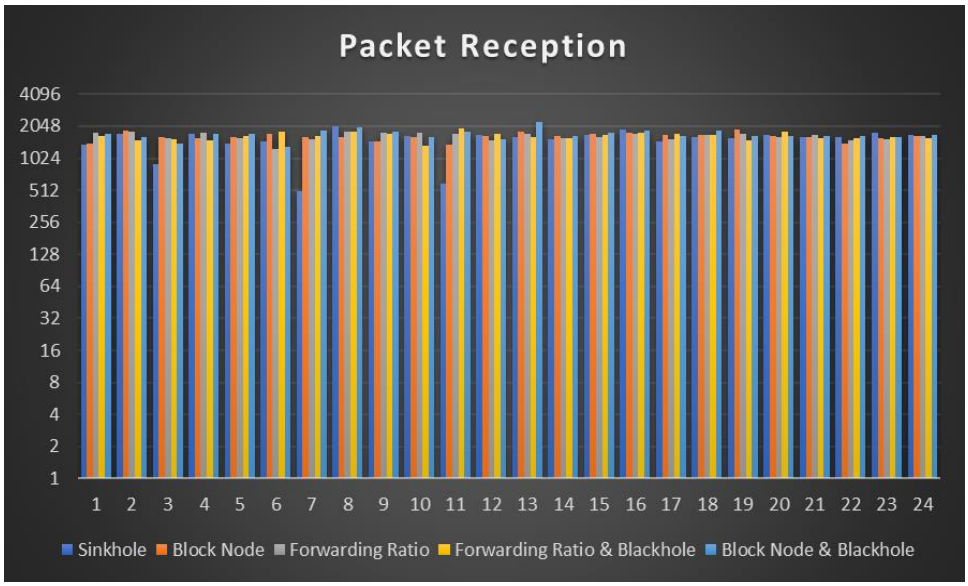
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	1558	70	0	9	0	5	719	10	427	120
	2	555	297	0	57	1	3	517	57	136	160
	3	406	175	0	133	0	36	44	33	8	81
	4	684	86	0	72	10	5	337	4	9	31
	5	975	102	0	12	0	79	564	77	410	97
	6	881	332	2	40	40	35	445	173	152	183
	7	149	91	0	1	0	5	16	85	21	36
	8	263	249	21	136	0	4	71	181	0	28
	9	26	70	0	14	0	0	0	10	10	51
	10	732	77	0	50	0	22	0	13	13	8
	11	961	237	7	98	52	9	14	12	25	2
	12	525	209	23	107	4	33	15	49	0	6
	13	304	247	0	1	26	10	0	8	0	4
	14	514	224	0	2	0	7	43	29	35	25
	15	358	124	7	53	0	1	272	92	0	12
	16	8	3	0	1	0	29	1	20	4	30
	17	613	269	0	9	1	9	3	16	12	64
	18	179	183	0	3	12	60	3	10	5	15
	19	843	101	0	7	0	81	37	27	0	38
	20	1565	24	0	29	0	3	627	47	598	88
	21	755	261	0	4	0	68	508	145	176	287
	22	635	351	15	4	52	184	54	16	41	32
	23	646	180	19	17	40	27	15	13	161	17
	24	1582	186	0	52	0	3	384	71	480	27



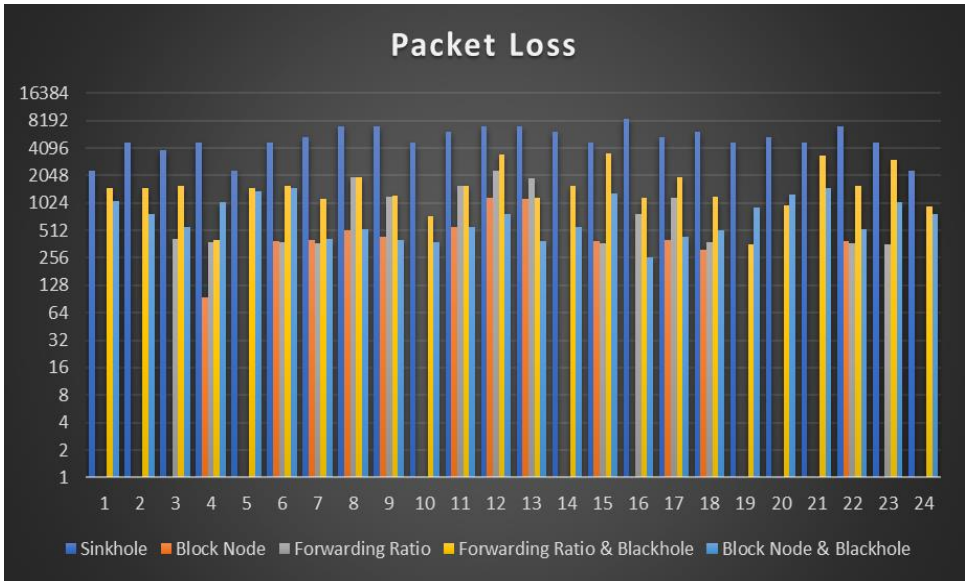


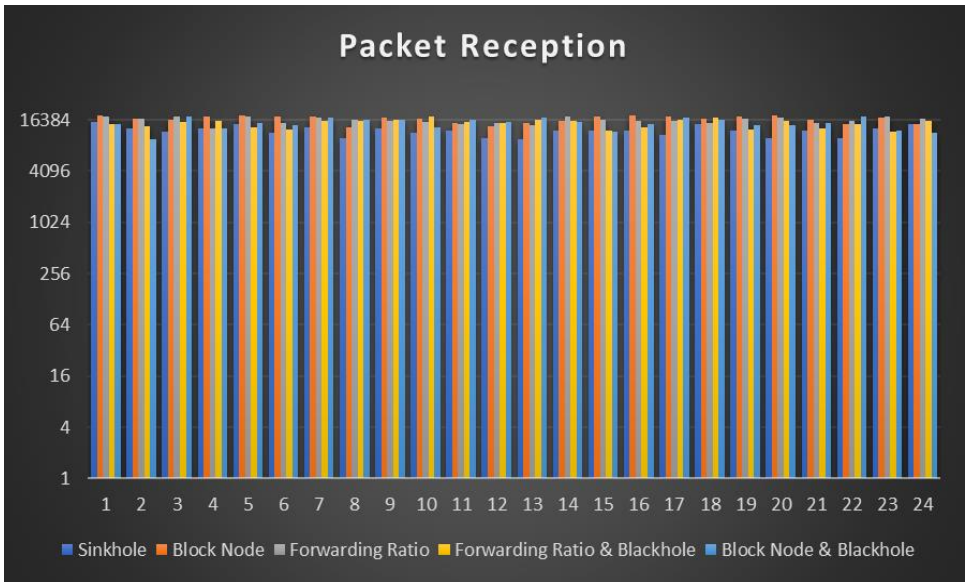
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	1555	1376	383	1414	330	1787	426	1654	251	1718
	2	1325	1744	130	1869	232	1808	211	1521	239	1603
	3	494	902	152	1617	134	1596	365	1547	152	1403
	4	1248	1754	0	1586	0	1762	470	1525	339	1740
	5	1704	1396	434	1626	456	1573	419	1645	423	1720
	6	1303	1479	164	1718	135	1251	372	1840	159	1303
	7	136	504	84	1608	74	1553	137	1670	111	1881
	8	322	2045	0	1635	120	1817	6	1807	83	1986
	9	667	1461	0	1459	0	1775	154	1722	79	1818
	10	1255	1645	218	1609	313	1770	194	1335	170	1612
	11	382	584	0	1379	0	1736	177	1958	58	1815
	12	112	1677	97	1672	94	1491	51	1724	35	1539
	13	257	1605	81	1827	82	1727	25	1626	13	2250
	14	505	1548	0	1671	79	1596	115	1591	62	1646
	15	662	1703	153	1726	219	1610	260	1712	220	1769
	16	20	1900	102	1791	0	1731	55	1796	7	1863
	17	313	1475	42	1709	80	1557	103	1725	96	1661
	18	57	1620	35	1685	0	1713	73	1691	74	1860
	19	74	1595	126	1900	0	1736	113	1496	81	1659
	20	1729	1677	286	1661	0	1610	290	1807	385	1660
	21	536	1619	155	1614	92	1704	122	1598	124	1672
	22	579	1626	86	1422	0	1508	125	1592	96	1662
	23	367	1759	129	1564	0	1529	125	1602	107	1629
	24	1717	1690	0	1664	0	1642	345	1562	169	1699



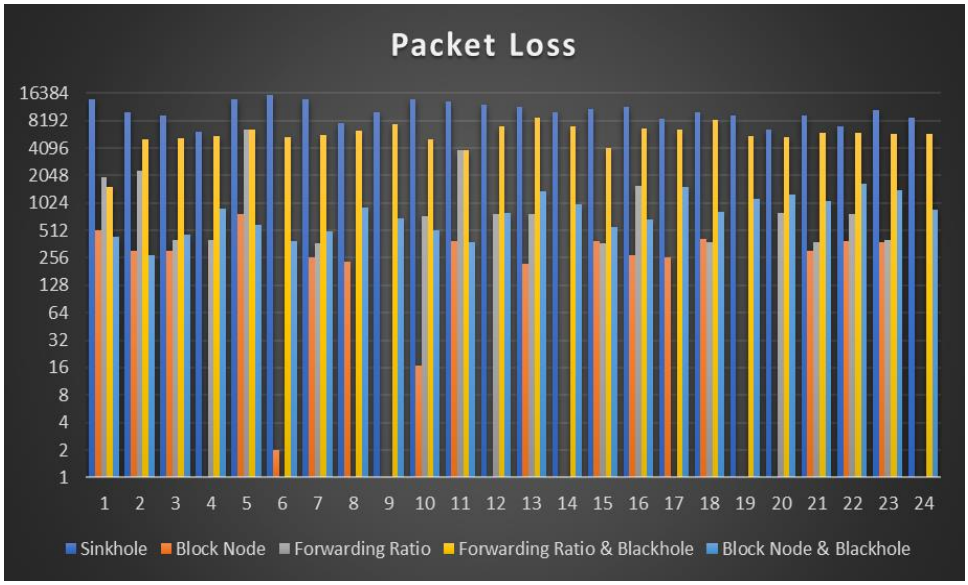


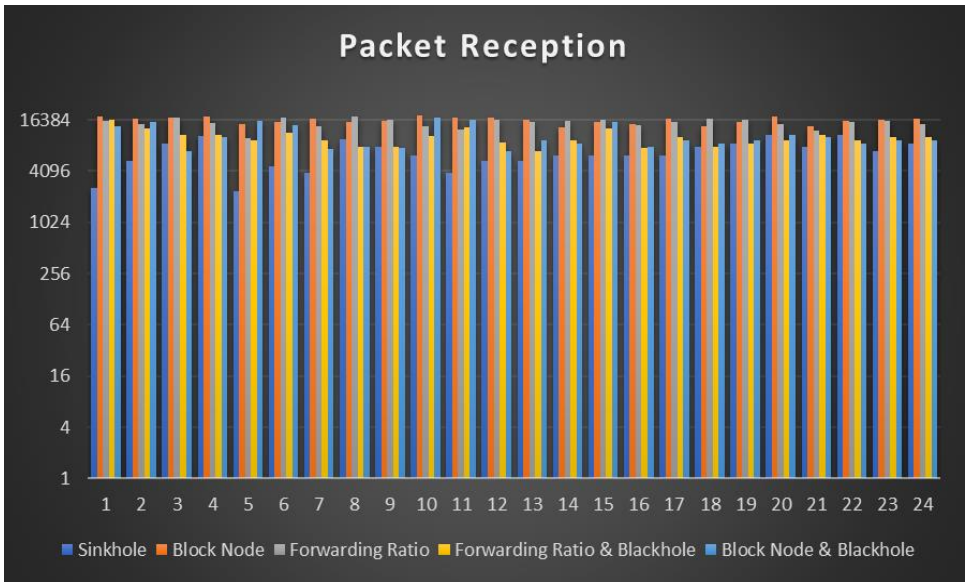
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery RDC Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	2340	15407	0	18488	0	17708	1502	14622	1071	14641
	2	4678	12869	0	16958	0	16950	1488	13872	785	9700
	3	3902	11817	0	16266	409	18029	1581	15389	555	17928
	4	4677	13096	95	17735	380	13153	401	15789	1057	12992
	5	2338	14633	0	18489	0	17713	1485	13184	1382	15005
	6	4678	11563	390	18102	377	15047	1587	12596	1490	14269
	7	5399	13282	407	18086	373	17346	1139	16069	409	17317
	8	7011	10020	516	13264	1964	16490	1969	15758	532	16180
	9	7016	13101	431	17359	1191	16122	1217	16586	407	16550
	10	4673	11560	0	16956	0	15414	742	17742	385	13499
	11	6238	12325	554	14871	1556	14638	1563	15281	555	16399
	12	7014	10019	1164	13883	2321	14852	3474	15051	782	15407
	13	7007	9638	1123	14830	1909	14288	1152	16578	389	17323
	14	6230	12315	0	15736	0	17722	1563	15795	556	15578
	15	4678	12333	389	17765	375	16578	3602	12329	1303	11888
	16	8578	12175	0	18384	767	16138	1163	13429	258	14607
	17	5456	10782	400	18093	1176	15723	1961	16544	432	17290
	18	6239	14636	310	16658	380	15029	1188	17316	518	16259
	19	4677	12323	0	17719	0	17065	356	12758	906	14178
	20	5460	10020	0	18485	0	17376	974	16140	1261	14226
	21	4676	12329	0	16540	0	14815	3435	13102	1487	14956
	22	7013	10014	390	14619	366	15937	1562	14671	534	17910
	23	4679	13093	0	17278	362	18070	3035	12047	1049	12340
	24	2338	14641	0	14455	0	16953	940	16063	772	11577



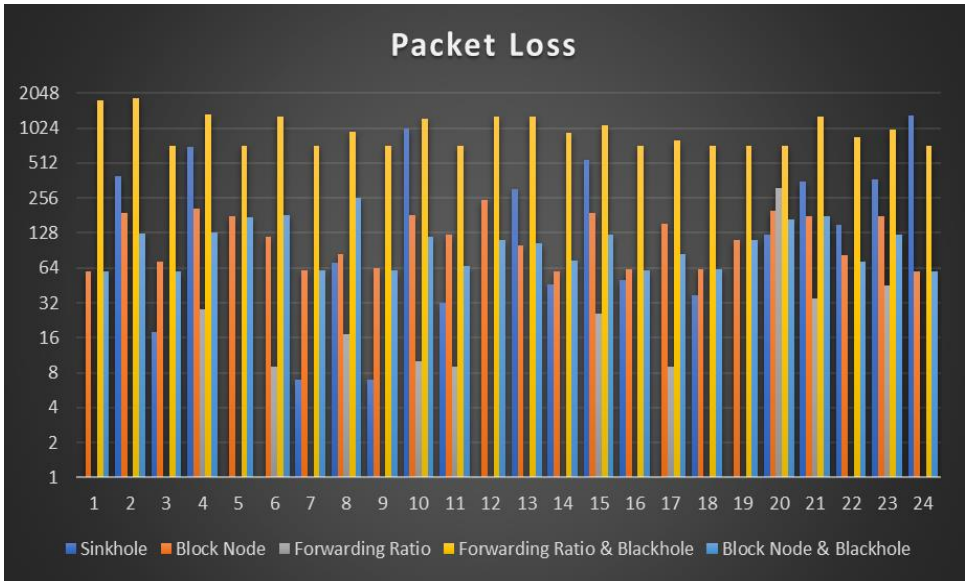


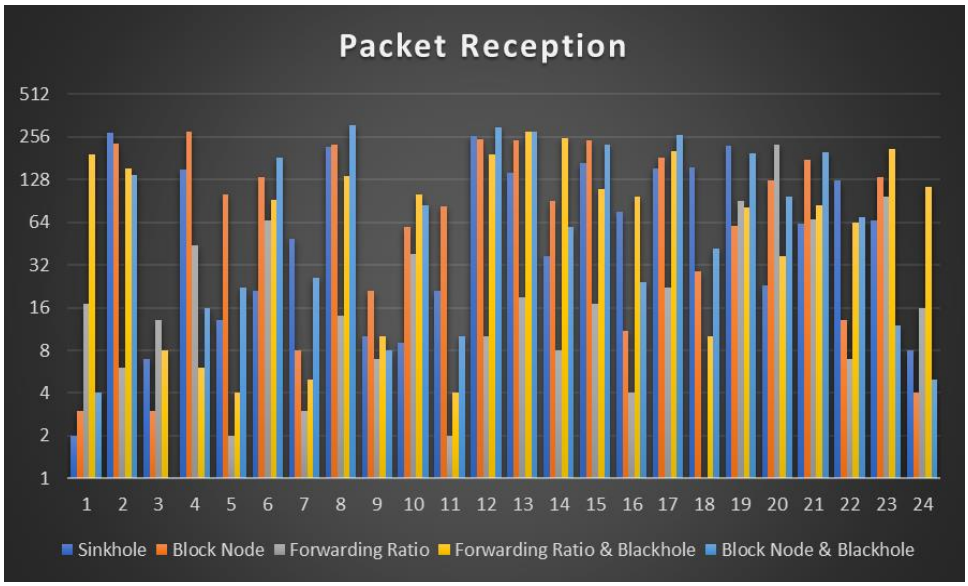
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery RDC Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	14027	2596	514	18090	1946	15858	1552	16360	431	13730
	2	10133	5463	302	16846	2340	14740	5084	12948	275	15655
	3	9355	8556	306	17611	401	17151	5289	10878	463	7016
	4	6239	10685	0	18062	401	15070	5517	10911	891	10132
	5	14022	2340	771	14649	6549	10096	6504	9392	587	15772
	6	15591	4677	2	15538	0	17241	5435	11385	393	13986
	7	14016	3897	260	16874	369	13705	5689	9316	498	7499
	8	7797	9772	230	15480	0	17904	6273	7922	906	7794
	9	10124	7800	0	15816	0	16492	7514	7790	691	7736
	10	14025	6233	17	18533	743	13700	5064	10529	509	17255
	11	13372	3899	386	17328	3906	12688	3924	13183	384	16469
	12	12352	5458	0	17134	780	16609	7179	8857	802	6943
	13	11688	5458	223	16382	772	15267	8791	7014	1371	9333
	14	10139	6239	0	13254	0	15816	7131	9353	979	8577
	15	10905	6246	389	15540	375	16579	4078	13014	563	15557
	16	11690	6237	272	14442	1581	14000	6651	7601	669	7787
	17	8583	6240	261	16986	0	15412	6578	10135	1537	9356
	18	10129	7797	409	13879	380	16894	8307	7794	828	8560
	19	9350	8572	0	15428	0	16377	5492	8572	1142	9343
	20	6446	10905	0	17902	798	14596	5398	9499	1276	10915
	21	9355	7796	308	13921	383	12240	6098	10906	1083	10232
	22	7009	10901	390	16098	766	15589	5971	9358	1669	8572
	23	10668	7018	385	16577	405	15998	5817	10132	1395	9296
	24	8810	8574	0	17122	0	14667	5824	10132	855	9508



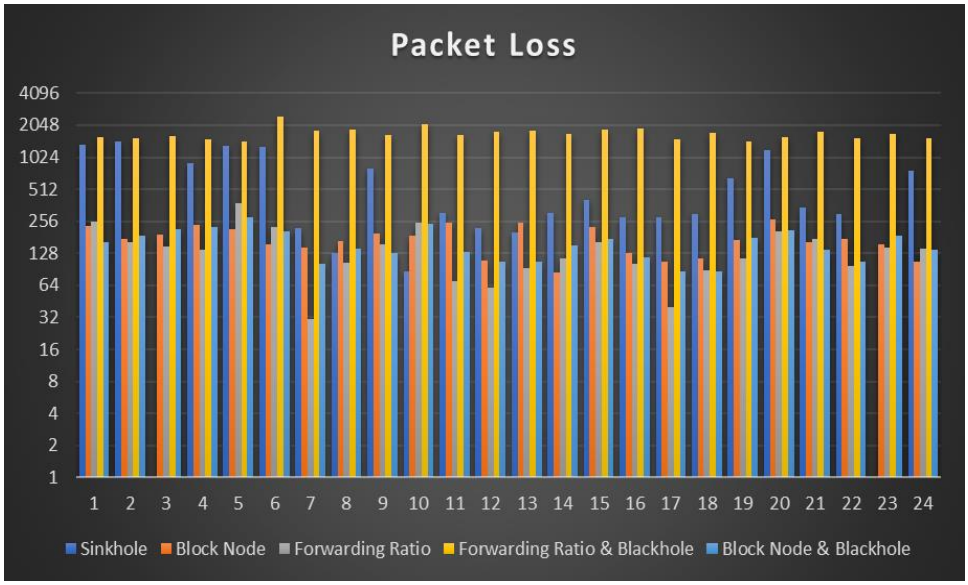


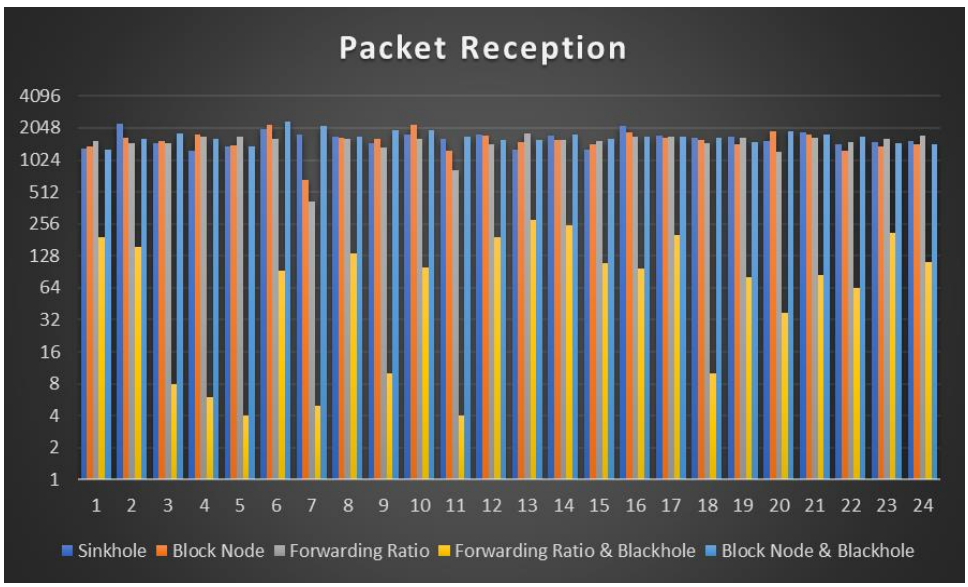
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery delayed Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	0	2	60	3	0	17	1785	194	60	4
	2	398	276	191	231	0	6	1849	154	126	137
	3	18	7	72	3	0	13	725	8	60	0
	4	699	150	208	279	28	44	1347	6	128	16
	5	0	13	180	101	0	2	719	4	176	22
	6	0	21	119	134	9	66	1277	92	181	183
	7	7	49	61	8	1	3	721	5	61	26
	8	71	217	84	227	17	14	962	136	258	309
	9	7	10	63	21	1	7	726	10	61	8
	10	1014	9	181	59	10	38	1229	100	119	85
	11	32	21	124	83	9	2	724	4	67	10
	12	0	259	245	245	0	10	1274	193	111	297
	13	308	142	100	242	1	19	1284	279	104	278
	14	46	37	60	91	0	8	930	250	74	59
	15	542	166	189	242	26	17	1087	110	124	225
	16	50	76	62	11	0	4	726	97	61	24
	17	0	154	153	183	9	22	795	202	85	263
	18	37	156	62	29	0	1	724	10	62	42
	19	0	222	111	60	0	91	719	81	110	197
	20	125	23	200	127	309	226	720	37	169	97
	21	351	63	180	176	35	67	1277	85	178	200
	22	149	127	82	13	1	7	847	64	73	70
	23	373	66	180	134	45	97	999	209	123	12
	24	1316	8	60	4	0	16	720	113	60	5



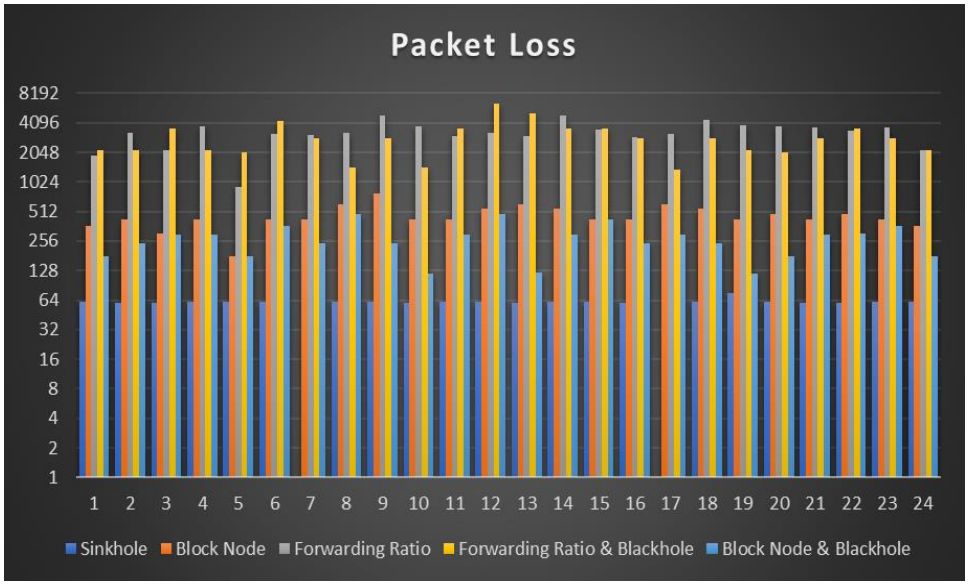


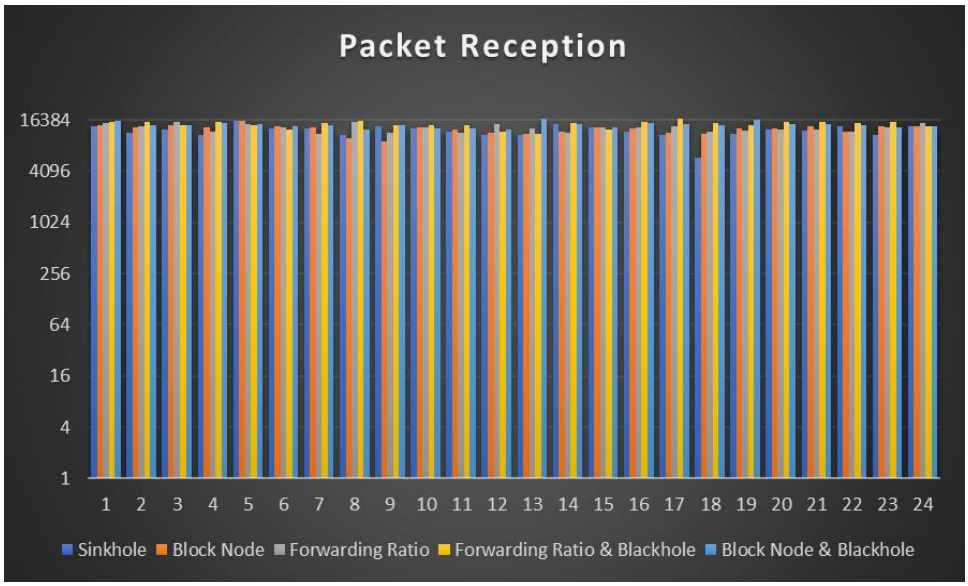
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery delayed Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	1340	1311	230	1366	255	1551	1598	194	164	1272
	2	1453	2240	175	1659	164	1457	1561	154	187	1620
	3	0	1483	194	1541	149	1475	1619	8	217	1828
	4	909	1253	236	1769	139	1705	1491	6	226	1620
	5	1316	1371	214	1408	379	1689	1449	4	280	1376
	6	1289	1981	157	2195	225	1634	2459	92	208	2343
	7	220	1780	144	660	31	417	1799	5	103	2144
	8	128	1688	167	1668	105	1632	1844	136	142	1708
	9	809	1463	196	1634	157	1353	1637	10	128	1952
	10	87	1790	186	2219	249	1612	2112	100	244	1950
	11	309	1603	247	1254	70	822	1672	4	132	1706
	12	221	1769	110	1736	61	1429	1784	193	106	1589
	13	200	1272	246	1500	93	1816	1798	279	107	1577
	14	306	1738	85	1565	114	1596	1685	250	150	1774
	15	404	1290	224	1450	164	1543	1882	110	176	1600
	16	277	2123	130	1842	101	1703	1889	97	117	1687
	17	279	1737	107	1657	40	1695	1491	202	86	1699
	18	299	1644	114	1566	88	1474	1737	10	87	1648
	19	645	1711	171	1452	114	1660	1441	81	180	1503
	20	1190	1537	265	1908	207	1226	1568	37	210	1922
	21	346	1876	162	1763	173	1657	1786	85	139	1768
	22	300	1448	175	1246	97	1510	1546	64	106	1708
	23	0	1500	155	1381	145	1611	1677	209	188	1484
	24	757	1561	106	1449	141	1742	1535	113	138	1447



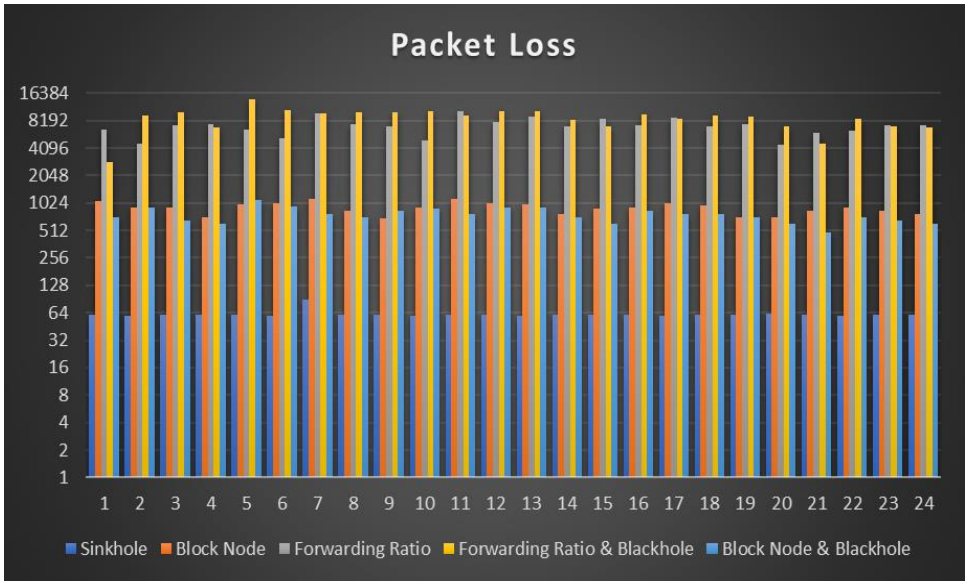


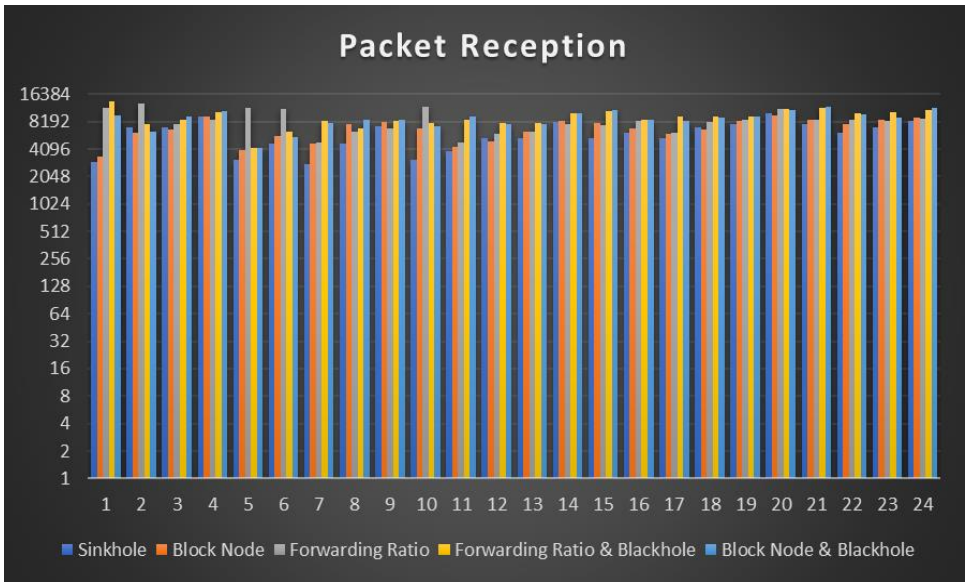
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery delayed RDC Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	61	13778	361	14327	1891	14977	2156	15473	181	16107
	2	60	11635	421	13169	3231	13609	2151	15404	241	14193
	3	60	12475	302	13966	2165	15689	3586	14257	301	14235
	4	61	10923	421	13535	3768	12024	2155	15685	301	14855
	5	61	15991	181	15959	905	14614	2036	14219	181	14576
	6	61	12929	421	13561	3164	13187	4291	12498	361	13781
	7	0	12974	421	13179	3096	11364	2871	15149	241	14021
	8	61	10889	601	9971	3263	15387	1439	15859	482	12580
	9	61	13880	782	9161	4897	11446	2877	14044	241	14165
	10	60	13074	421	13464	3787	13410	1437	14149	120	12865
	11	61	11947	421	12747	3022	11390	3598	14068	301	13049
	12	61	10893	543	11447	3221	14705	6474	12045	482	12453
	13	60	10798	600	11342	2971	12844	5048	11115	121	16962
	14	61	14671	541	12012	4896	11650	3578	15034	301	14499
	15	61	13222	422	13547	3521	13390	3580	12547	421	13403
	16	60	11738	421	12889	2906	13355	2874	15659	241	14853
	17	0	10724	601	11465	3166	13941	1378	17003	301	14502
	18	61	5868	541	11209	4408	11817	2868	14912	241	14124
	19	75	11243	421	12893	3871	12317	2156	14149	120	16172
	20	61	12641	481	12845	3716	12538	2036	15619	180	14668
	21	60	12105	421	13568	3704	12639	2868	15673	301	14627
	22	60	13931	480	11997	3432	11832	3590	15074	302	13968
	23	61	10916	422	13656	3667	13371	2866	15585	361	13505
	24	61	13777	361	13787	2141	14855	2152	13590	181	13820



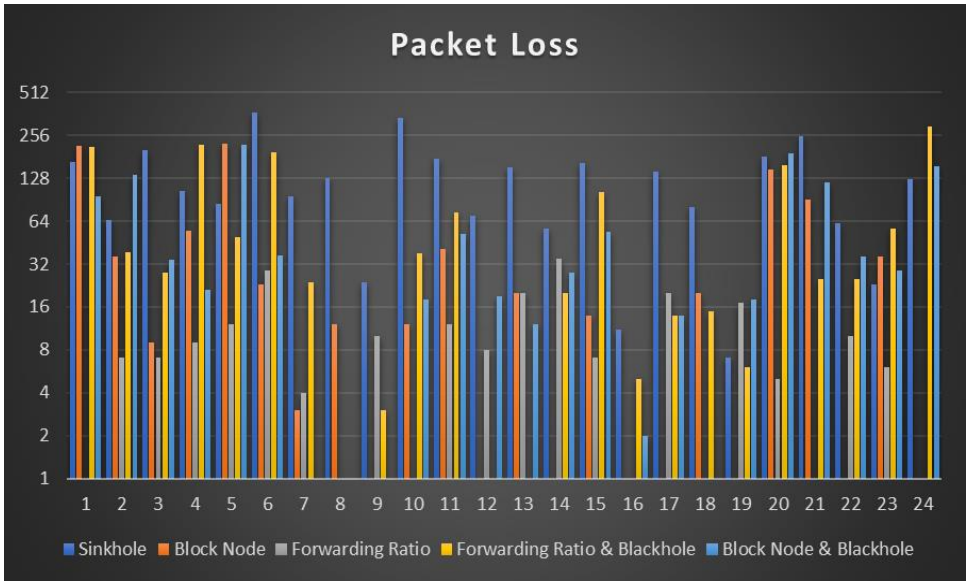


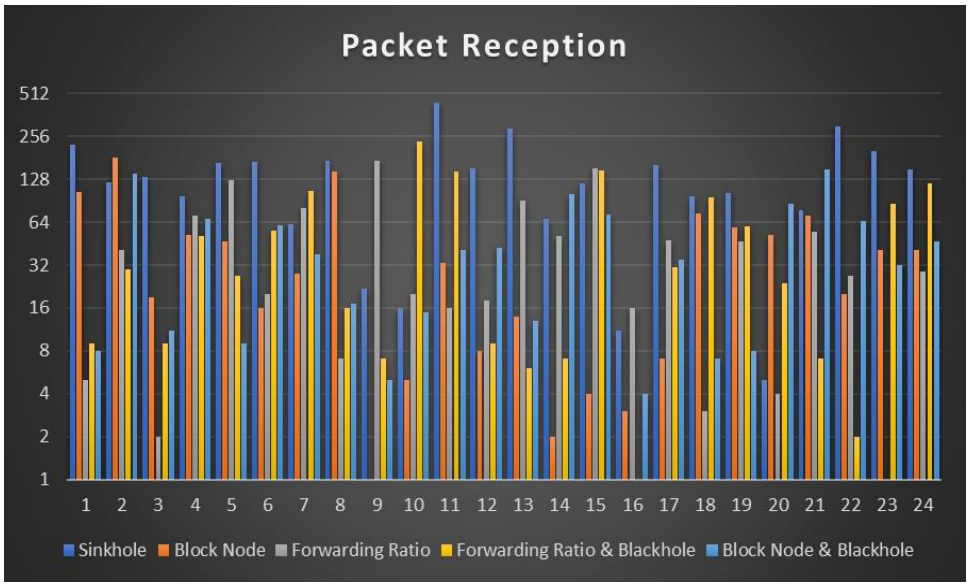
		Sinkhole		BN		FR		FR & BH		BN & BH	
NoRecovery delayed RDC Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	61	2935	1081	3346	6494	11513	2878	13823	721	9707
	2	60	7014	901	6187	4578	13013	9354	7733	901	6368
	3	61	7005	902	6798	7307	7628	10006	8539	661	9213
	4	61	9347	717	9259	7448	8529	6976	10350	601	10671
	5	61	3103	1001	4023	6502	11454	14003	4235	1092	4205
	6	60	4666	1019	5675	5283	11232	10541	6369	937	5575
	7	90	2761	1140	4698	9858	4833	9810	8391	783	7812
	8	61	4689	841	7692	7558	6334	10047	6851	721	8521
	9	61	7312	703	8089	7122	6987	10020	8329	842	8545
	10	60	3091	901	6915	5016	12038	10533	7849	899	7378
	11	61	3899	1142	4386	10355	4872	9386	8525	781	9229
	12	61	5396	1023	5007	7925	6036	10496	7951	901	7782
	13	60	5394	986	6324	9141	6296	10383	7958	901	7768
	14	61	8031	782	8413	7173	7685	8399	10001	722	10028
	15	61	5466	900	7909	8550	7534	7008	10803	601	11105
	16	61	6232	902	6988	7383	8413	9672	8494	842	8538
	17	60	5456	1022	6074	8928	6253	8506	9200	782	8465
	18	61	7004	962	6693	7062	8043	9207	9369	781	9191
	19	61	7791	722	8456	7401	8548	9131	9257	722	9196
	20	62	10170	721	9641	4447	11267	7168	11253	602	11026
	21	61	7789	842	8487	6087	8488	4563	11638	486	11818
	22	60	6166	902	7764	6345	8510	8496	10016	721	9947
	23	61	7010	842	8559	7250	8341	7177	10335	662	9090
	24	61	8381	781	9126	7195	8867	6944	11079	601	11471



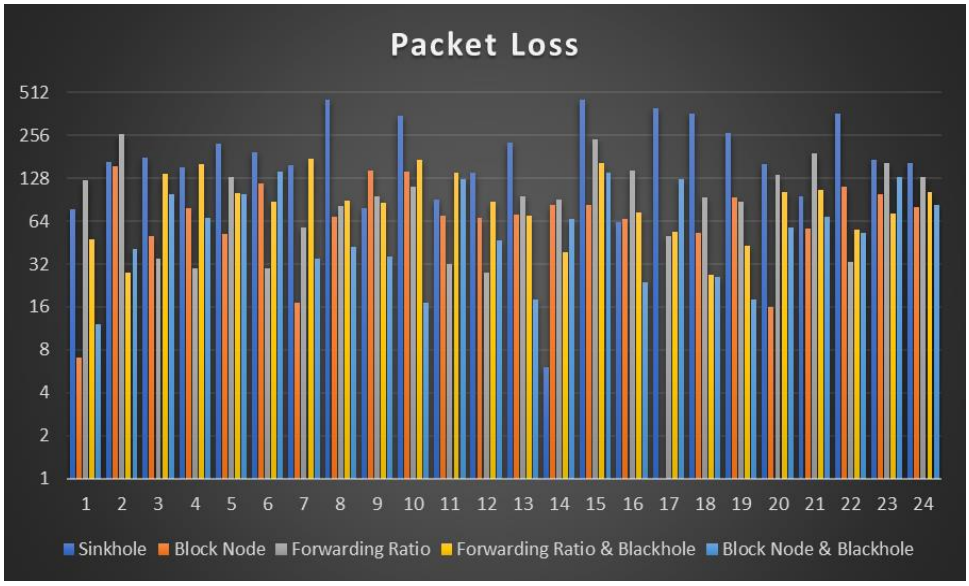


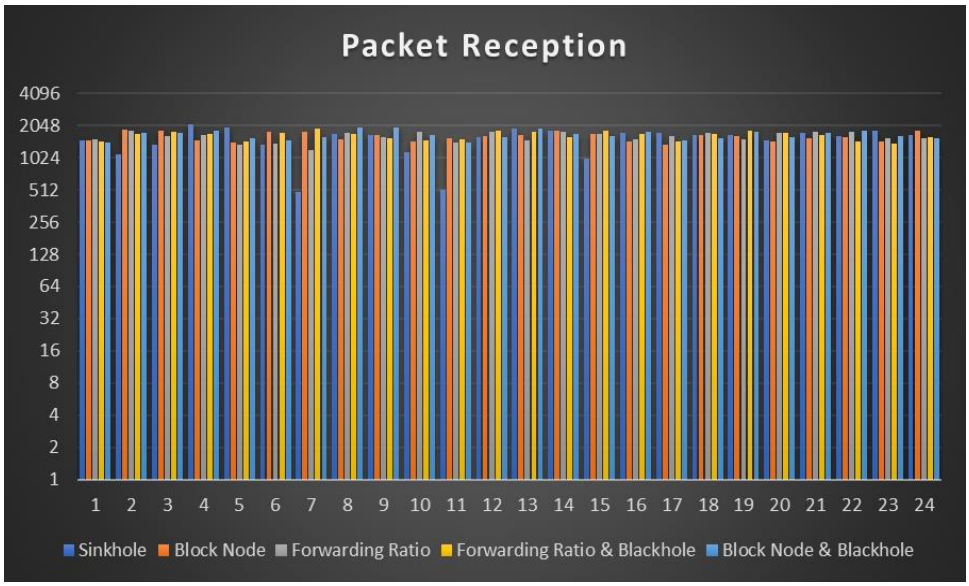
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	167	222	217	105	0	5	213	9	95	8
	2	65	121	36	182	7	41	39	30	135	140
	3	202	132	9	19	7	2	28	9	34	11
	4	104	98	55	52	9	71	219	51	21	68
	5	84	168	223	47	12	127	49	27	220	9
	6	368	170	23	16	29	20	194	56	37	61
	7	96	62	3	28	4	80	24	106	1	38
	8	128	171	12	144	0	7	0	16	0	17
	9	24	22	0	1	10	173	3	7	0	5
	10	339	16	12	5	1	20	38	236	18	15
	11	174	441	41	33	12	16	74	144	52	41
	12	70	154	0	8	8	18	1	9	19	42
	13	152	288	20	14	20	91	0	6	12	13
	14	57	68	0	2	35	51	20	7	28	100
	15	165	120	14	4	7	153	103	148	54	72
	16	11	11	0	3	1	16	5	1	2	4
	17	142	160	0	7	20	48	14	31	14	35
	18	81	98	20	73	0	3	15	96	0	7
	19	7	102	0	59	17	47	6	60	18	8
	20	182	5	147	52	5	4	158	24	192	86
	21	252	77	90	71	0	55	25	7	120	149
	22	62	301	0	20	10	27	25	2	36	65
	23	23	201	36	41	6	1	57	86	29	32
	24	127	151	0	41	0	29	298	120	156	47



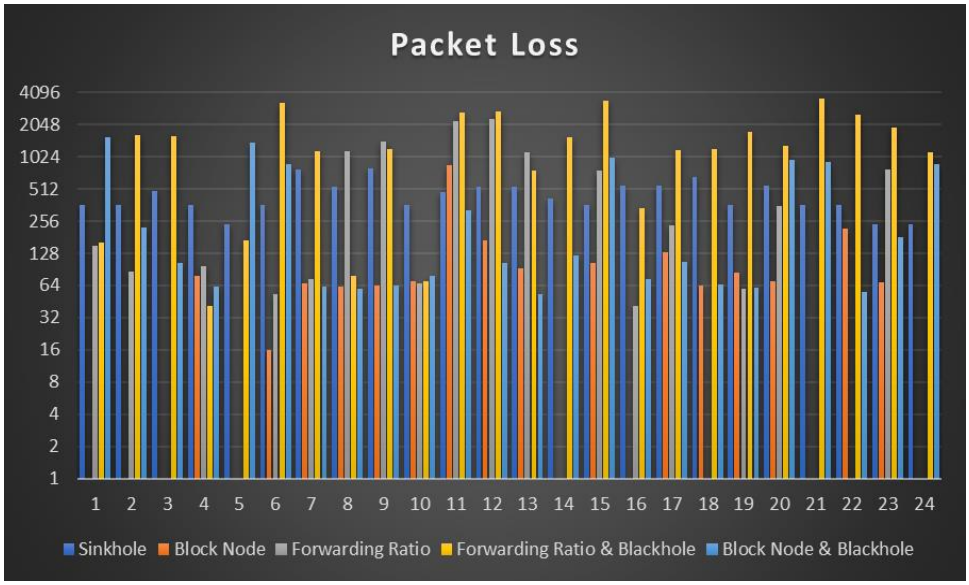


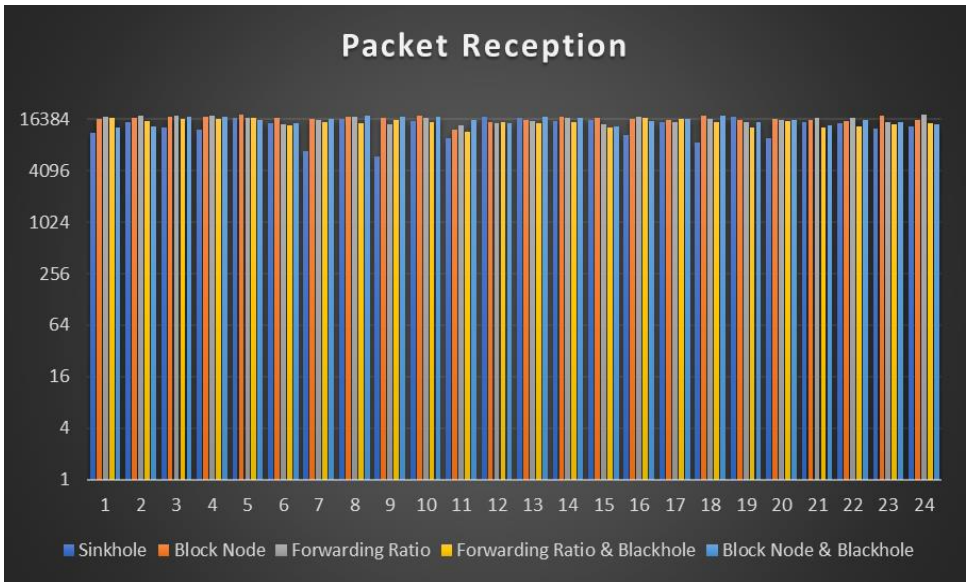
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	78	1508	7	1489	123	1540	48	1448	12	1424
	2	168	1108	155	1862	263	1855	28	1699	41	1747
	3	179	1356	50	1824	35	1623	137	1781	99	1738
	4	154	2111	79	1482	30	1682	161	1696	68	1823
	5	223	1978	52	1435	131	1368	101	1470	99	1579
	6	196	1363	117	1793	30	1376	87	1738	142	1492
	7	159	490	17	1791	58	1215	176	1918	35	1583
	8	456	1715	69	1529	82	1735	89	1703	42	1987
	9	79	1691	144	1677	95	1592	86	1572	36	1966
	10	352	1150	143	1451	111	1812	172	1502	17	1683
	11	91	515	70	1554	32	1424	139	1530	126	1412
	12	140	1584	67	1641	28	1783	88	1818	47	1615
	13	226	1909	71	1660	95	1499	70	1785	18	1905
	14	6	1821	83	1816	91	1785	39	1587	66	1726
	15	459	1014	83	1724	238	1712	163	1819	141	1642
	16	63	1734	66	1450	144	1528	74	1699	24	1805
	17	399	1760	0	1360	50	1639	54	1453	126	1506
	18	364	1668	53	1664	94	1768	27	1700	26	1570
	19	267	1656	94	1618	87	1537	43	1829	18	1812
	20	162	1507	16	1465	135	1761	103	1768	58	1592
	21	96	1758	57	1544	190	1790	106	1686	69	1738
	22	361	1630	111	1590	33	1777	56	1448	53	1848
	23	172	1834	99	1469	163	1547	72	1403	130	1620
	24	165	1692	81	1819	130	1565	103	1591	83	1546



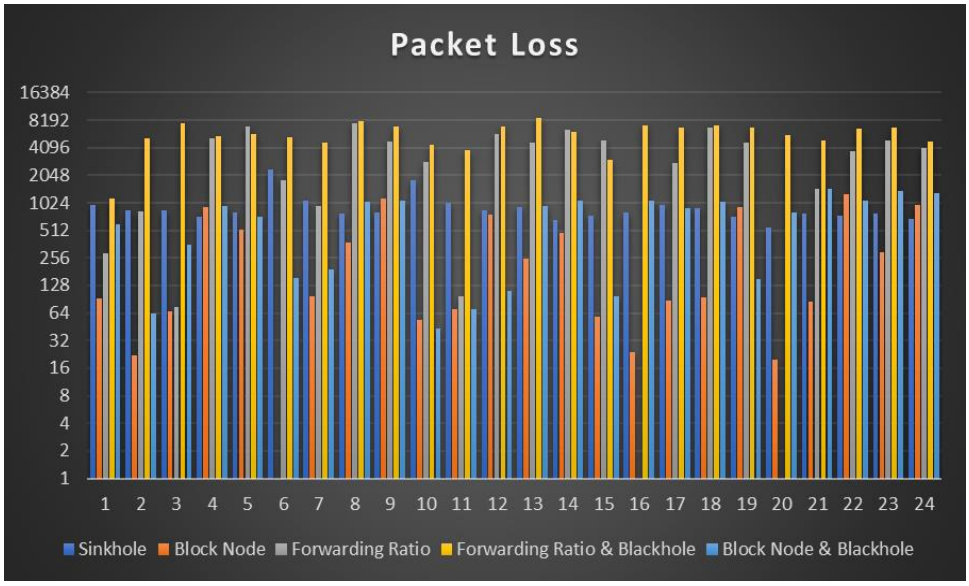


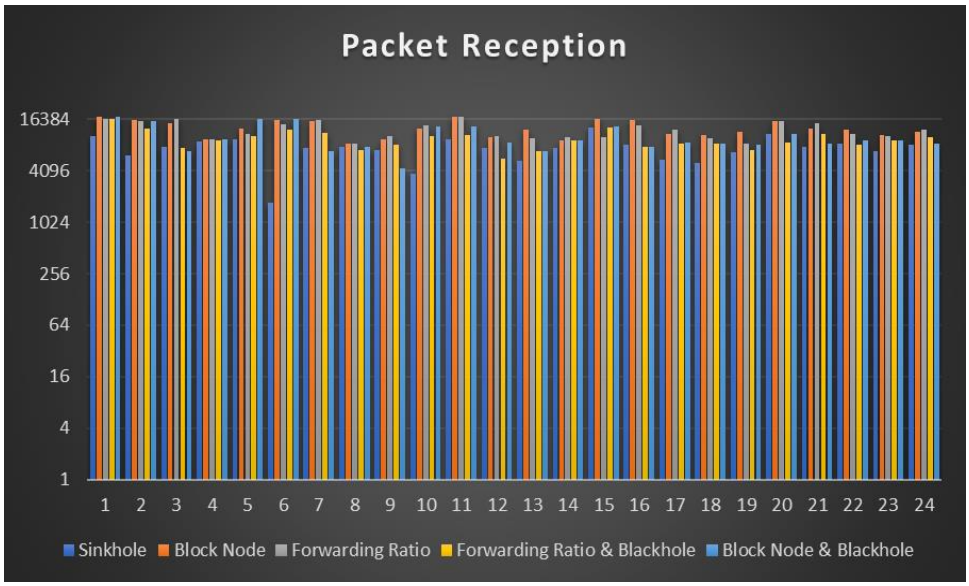
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting RDC Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	361	11219	0	16715	150	17308	163	17098	1553	12987
	2	364	15273	0	17149	86	17885	1647	15409	224	13658
	3	487	12922	0	17425	0	17916	1580	16503	103	17703
	4	361	12434	78	17735	98	18004	41	16766	63	17367
	5	241	16955	0	18391	0	16825	168	16953	1399	16204
	6	362	14902	16	17148	53	14325	3296	13894	866	14859
	7	787	6946	67	16537	74	15829	1145	15118	62	16608
	8	540	16673	63	17546	1160	17411	78	14819	60	18017
	9	789	5928	64	16848	1423	14259	1204	16108	64	17411
	10	365	15728	70	17813	67	17160	70	14949	78	17652
	11	484	9733	859	12451	2189	13838	2654	11694	325	16038
	12	542	17307	169	15303	2316	14687	2696	15196	104	14821
	13	544	16835	92	16030	1116	15718	753	14593	53	17654
	14	420	15810	0	17604	0	17019	1576	15322	122	17014
	15	364	15926	104	16912	762	14138	3418	13130	994	13369
	16	545	10605	0	16291	41	17500	340	16867	74	15592
	17	546	14975	131	16152	234	15291	1189	16614	106	16610
	18	665	8862	64	17955	0	16362	1198	14962	65	18151
	19	363	17295	85	16109	60	15218	1758	13016	61	15094
	20	545	9841	70	16752	358	16190	1304	15399	955	15993
	21	362	15160	0	16230	0	16778	3626	12938	925	13786
	22	362	14785	220	15719	0	17175	2565	13302	56	16183
	23	239	12895	69	17792	771	15235	1918	14440	181	15357
	24	242	13329	0	15994	0	18692	1135	14680	873	14449



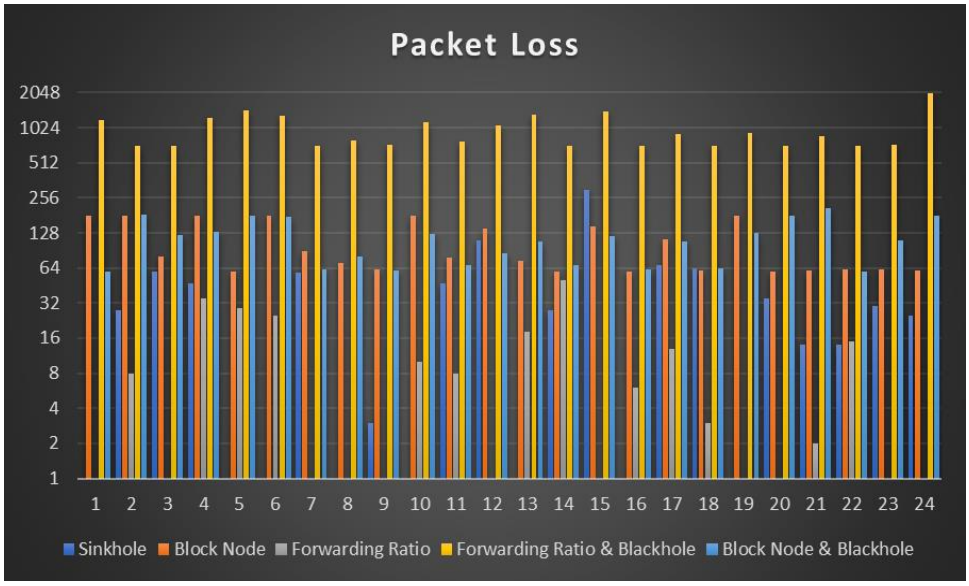


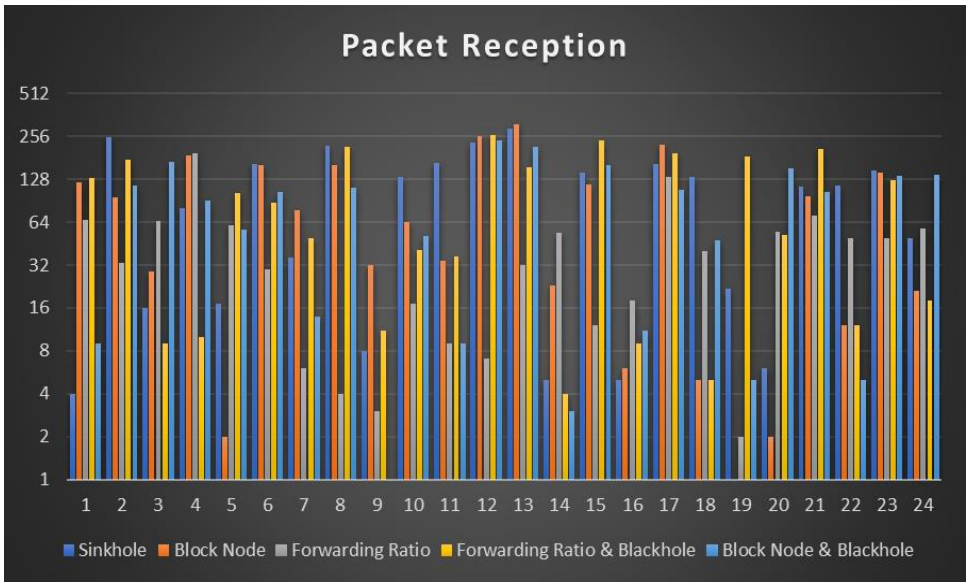
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting RDC Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	975	10469	92	17317	291	16647	1151	16484	601	17336
	2	857	6095	22	16195	826	15755	5227	12698	63	15790
	3	847	7747	66	14792	74	16738	7645	7503	354	7017
	4	724	8921	920	9603	5128	9580	5408	9346	953	9469
	5	804	9420	522	12628	6968	11041	5803	10499	719	16663
	6	2342	1725	0	16130	1788	14143	5278	12206	153	16516
	7	1086	7491	97	15374	946	15955	4603	11467	190	7011
	8	779	7727	380	8439	7553	8477	7875	7189	1062	7790
	9	801	7195	1134	9488	4832	10486	7020	8214	1068	4421
	10	1785	3780	54	12804	2858	13757	4415	10499	43	13434
	11	1011	9491	70	17683	97	17408	3882	10775	71	13680
	12	844	7555	753	10131	5735	10523	6978	5608	111	8628
	13	913	5330	254	12549	4648	9893	8670	6893	931	7014
	14	667	7663	478	9226	6409	10116	6065	9206	1092	9348
	15	737	13020	59	16741	4913	10022	3031	12945	97	13464
	16	812	8151	24	16116	0	13804	7169	7789	1094	7786
	17	966	5452	88	11007	2810	12470	6706	8451	886	8806
	18	903	5101	94	10857	6814	9825	7092	8572	1051	8570
	19	722	6774	907	11674	4680	8483	6811	7202	151	8330
	20	552	11165	20	15656	0	15603	5669	8811	803	10923
	21	780	7785	86	12684	1461	14635	4951	11051	1449	8512
	22	730	8555	1286	12397	3736	11164	6611	8329	1071	9351
	23	781	7015	296	10663	4919	10363	6709	9178	1379	9353
	24	680	8207	976	11680	4045	12345	4772	10120	1320	8478



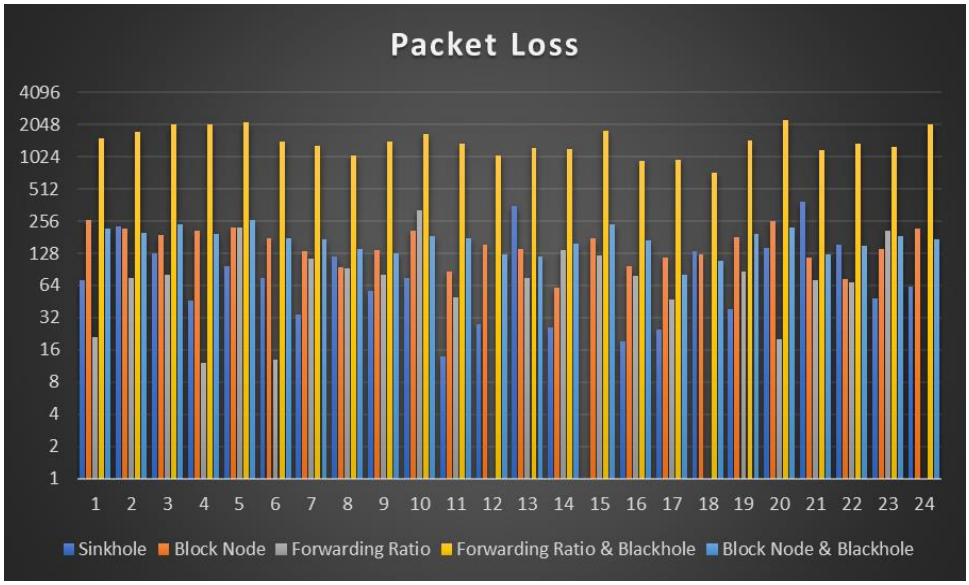


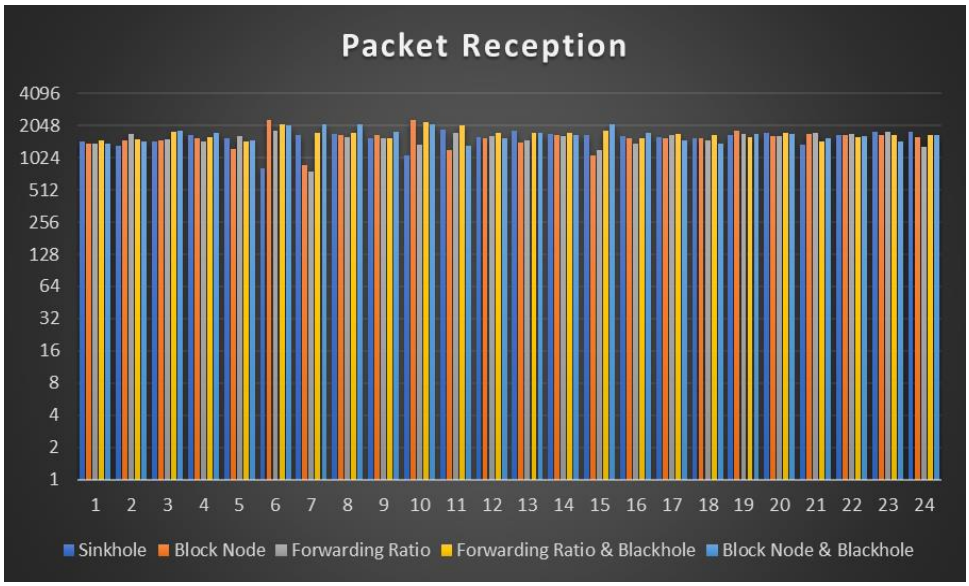
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting delayed Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	0	4	178	121	0	66	1176	131	60	9
	2	28	254	179	96	8	33	718	174	182	116
	3	59	16	81	29	0	65	720	9	123	170
	4	47	80	181	189	35	196	1228	10	130	90
	5	0	17	60	2	29	61	1453	102	181	57
	6	0	164	178	162	25	30	1303	88	175	104
	7	58	36	90	78	0	6	718	49	62	14
	8	0	221	71	160	0	4	788	218	81	112
	9	3	8	62	32	0	3	726	11	61	1
	10	0	134	181	64	10	17	1145	41	124	51
	11	47	168	78	34	8	9	783	37	68	9
	12	111	232	138	256	0	7	1060	260	85	239
	13	0	289	73	310	18	32	1325	155	108	215
	14	28	5	60	23	50	54	719	4	68	3
	15	298	143	144	118	0	12	1411	239	121	160
	16	0	5	60	6	6	18	719	9	62	11
	17	67	165	112	225	13	132	904	195	109	107
	18	64	134	61	5	3	40	721	5	63	48
	19	0	22	181	1	0	2	924	185	127	5
	20	35	6	60	2	0	55	718	52	180	152
	21	14	114	61	98	2	71	857	210	209	105
	22	14	115	62	12	15	49	720	12	60	5
	23	30	148	62	143	0	49	734	127	111	135
	24	25	49	61	21	0	58	2035	18	181	138



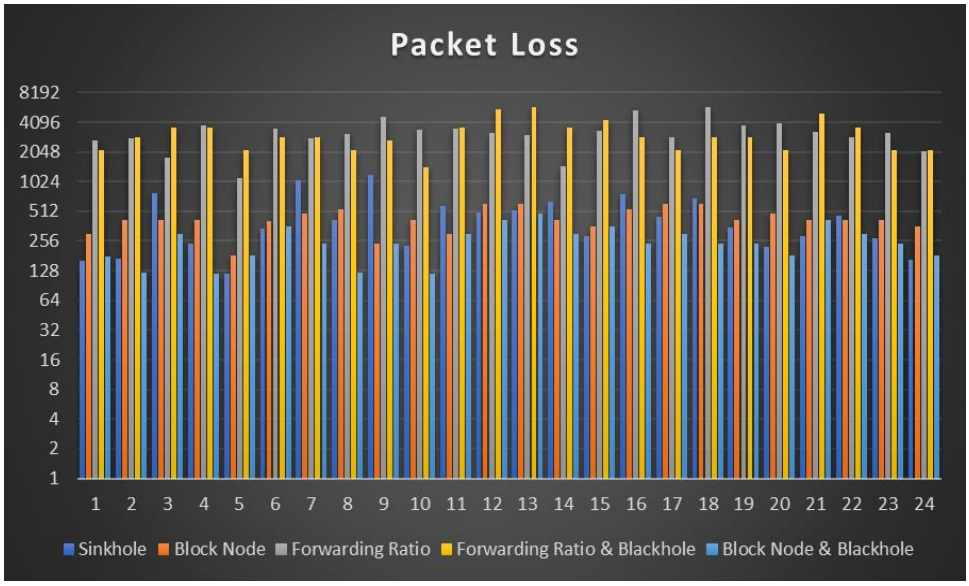


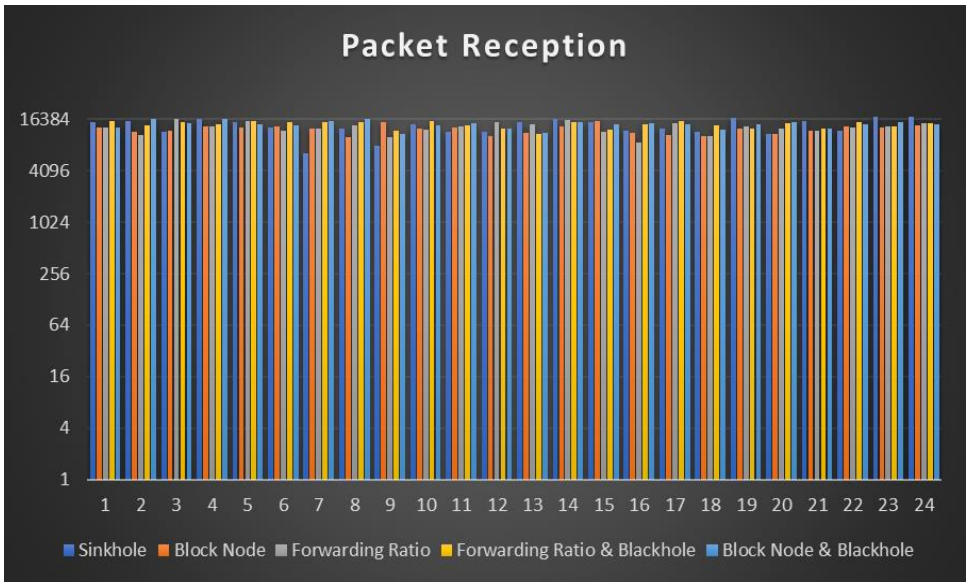
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting delayed Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	71	1450	260	1386	21	1391	1525	1478	216	1402
	2	229	1343	216	1503	75	1709	1756	1531	198	1454
	3	128	1467	189	1491	81	1524	2046	1798	240	1856
	4	46	1656	207	1575	12	1471	2063	1598	196	1743
	5	98	1550	221	1229	222	1637	2139	1445	261	1482
	6	76	812	175	2311	13	1834	1429	2113	176	2084
	7	34	1663	135	883	113	761	1286	1768	173	2107
	8	120	1705	94	1666	92	1602	1046	1741	141	2103
	9	57	1567	136	1678	80	1579	1428	1545	128	1790
	10	76	1077	209	2307	325	1353	1671	2186	185	2117
	11	14	1888	86	1201	50	1739	1359	2057	179	1330
	12	28	1592	153	1548	0	1643	1052	1753	124	1554
	13	355	1820	139	1424	76	1497	1238	1749	119	1762
	14	26	1694	61	1660	138	1644	1197	1745	158	1659
	15	0	1688	179	1074	121	1207	1779	1824	241	2096
	16	19	1645	97	1569	79	1383	933	1548	170	1752
	17	25	1588	117	1554	47	1693	962	1721	80	1487
	18	134	1574	125	1547	0	1503	720	1677	108	1400
	19	38	1692	183	1825	87	1706	1472	1602	195	1709
	20	144	1761	259	1625	20	1647	2261	1756	222	1697
	21	388	1351	117	1731	71	1744	1175	1460	126	1562
	22	153	1668	74	1677	68	1704	1370	1602	149	1632
	23	48	1779	140	1683	207	1788	1259	1655	184	1440
	24	63	1811	220	1601	0	1311	2044	1674	174	1675



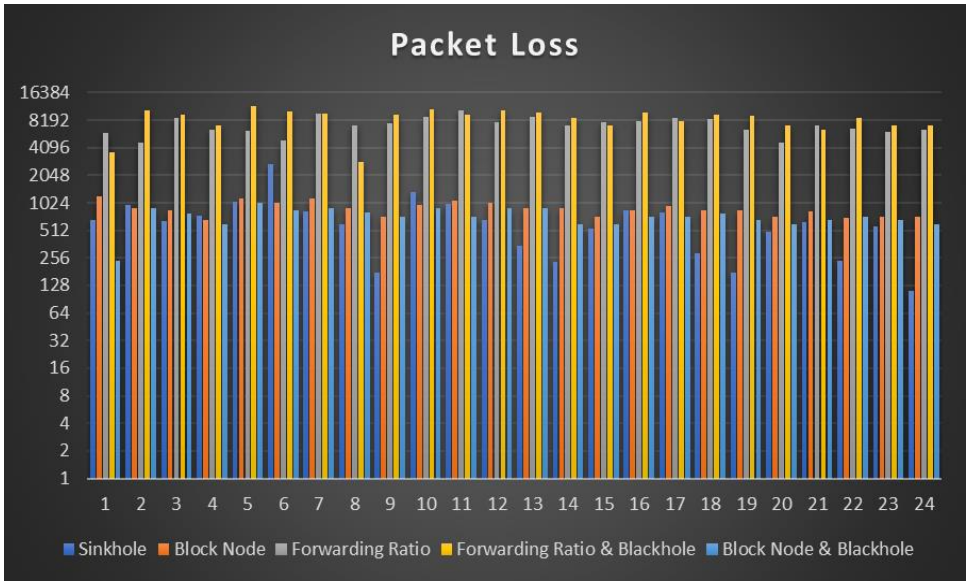


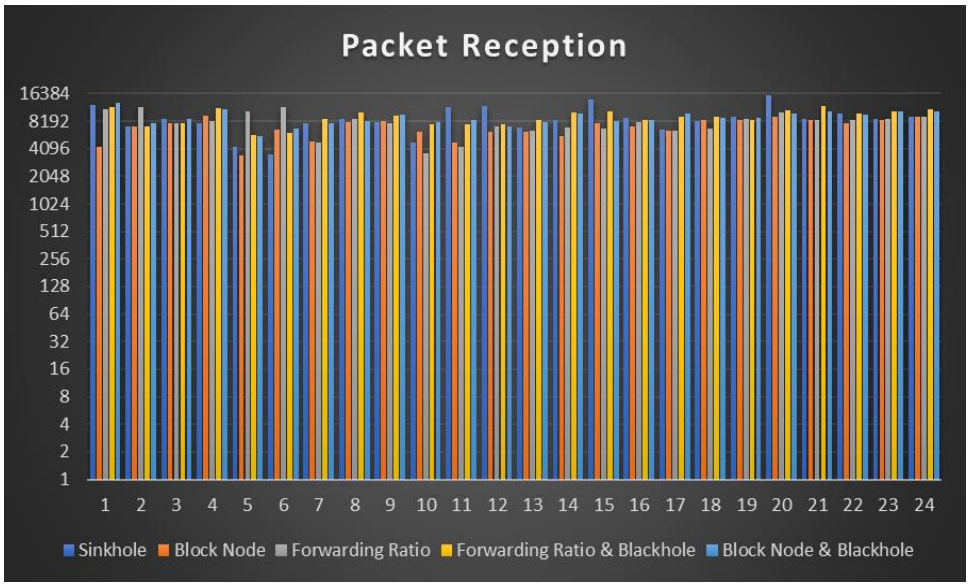
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting delayed RDC Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	162	15097	301	13209	2703	13210	2150	15635	180	13010
	2	168	15655	421	11517	2789	10860	2873	14035	121	16476
	3	775	11522	422	12064	1792	16588	3576	15098	301	14775
	4	238	16660	421	13548	3830	13366	3597	14210	120	16523
	5	120	15249	181	13288	1114	15532	2155	15640	181	14125
	6	339	13123	407	13408	3548	11961	2868	15098	361	14073
	7	1047	6594	481	12604	2798	12878	2871	15227	241	15606
	8	417	12902	541	10023	3083	14093	2158	15193	121	16329
	9	1193	8001	241	15327	4651	10149	2689	11989	240	11075
	10	226	14352	421	12795	3439	12393	1435	15766	120	14019
	11	575	11528	302	13243	3498	13500	3594	13962	301	14831
	12	493	11536	603	10255	3190	15307	5566	12706	421	12747
	13	520	15335	603	11280	3036	14265	5745	11119	481	11376
	14	646	16477	421	13536	1464	16257	3582	15046	301	14981
	15	285	15349	358	15585	3334	11627	4306	12291	361	14154
	16	761	11862	543	11477	5380	8760	2876	14344	241	14630
	17	453	12761	602	10694	2854	14552	2157	15402	301	14133
	18	682	11716	602	10530	5770	10409	2878	13899	241	12451
	19	350	17069	420	12620	3829	13362	2871	12750	241	14167
	20	221	10886	481	11017	3966	12721	2156	14825	181	15041
	21	286	15500	421	12192	3228	12063	5010	12837	421	12623
	22	461	11860	421	13528	2866	13180	3587	15107	300	14288
	23	270	17682	421	13248	3200	13535	2151	13674	241	15310
	24	163	17559	361	13709	2075	14590	2152	14823	181	14500



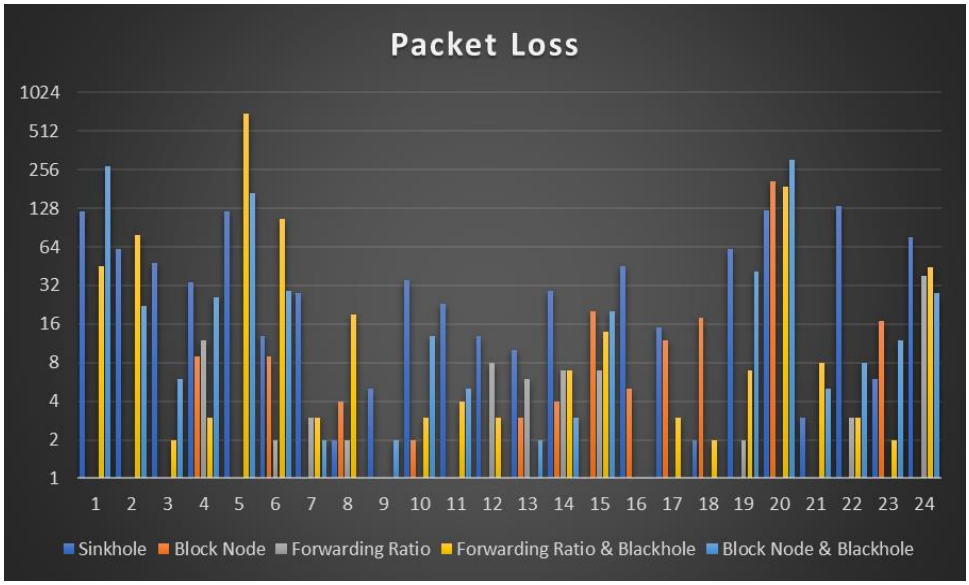


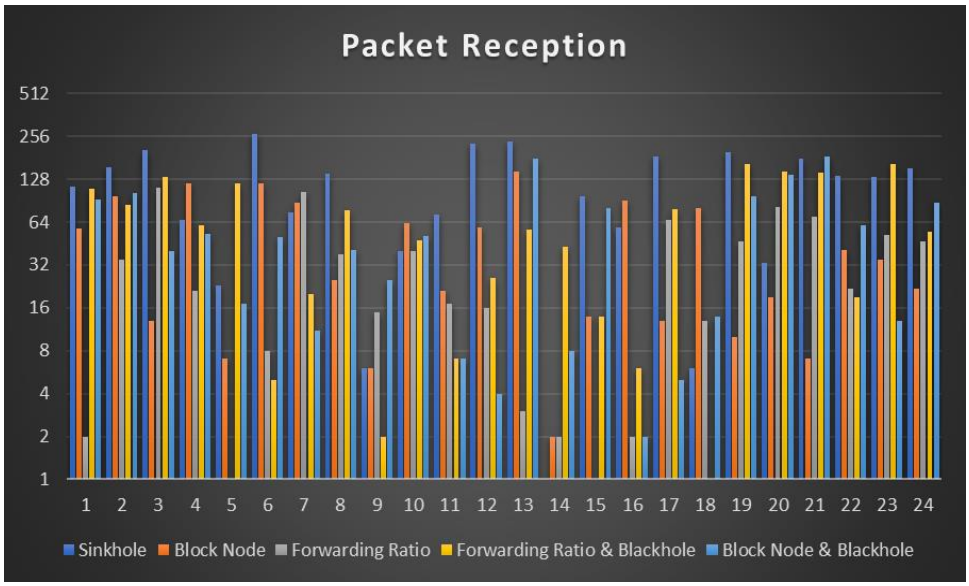
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting delayed RDC Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	664	12331	1198	4278	5969	10948	3598	11664	241	12945
	2	963	7236	901	7170	4633	11680	10457	7110	901	7742
	3	655	8594	842	7830	8593	7798	9383	7741	782	8537
	4	743	7777	663	9318	6344	8294	7176	11340	601	11090
	5	1058	4303	1142	3461	6328	10523	11555	5693	1022	5580
	6	2732	3578	1021	6528	4933	11757	10151	6124	840	6779
	7	817	7762	1140	4911	9736	4767	9630	8581	893	7749
	8	597	8717	902	7880	7162	8652	2855	10073	797	8221
	9	178	7957	721	8253	7463	7735	9259	9288	722	9738
	10	1357	4818	975	6301	8796	3661	10758	7580	902	7902
	11	1009	11578	1083	4818	10361	4312	9330	7624	723	8436
	12	660	12086	1021	6217	7846	7118	10539	7474	900	7161
	13	348	6903	901	6338	8948	6392	9961	8479	902	7914
	14	232	8354	903	5589	7241	7059	8599	10041	603	9917
	15	542	13996	723	7833	7809	6798	7182	10469	601	8244
	16	840	8983	843	7148	7899	7961	9873	8449	722	8461
	17	808	6539	934	6375	8679	6404	7886	9133	722	9953
	18	291	8095	842	8506	8444	6804	9318	9183	781	8958
	19	179	9025	841	8349	6404	8589	9020	8310	661	8962
	20	500	15739	722	9124	4650	10067	7120	10626	601	9965
	21	635	8698	825	8519	7228	8347	6348	12048	661	10500
	22	240	9855	700	7726	6628	8477	8585	9983	722	9598
	23	568	8681	721	8394	6162	8579	7215	10509	662	10566
	24	113	9241	723	9174	6458	9111	7141	11076	603	10469



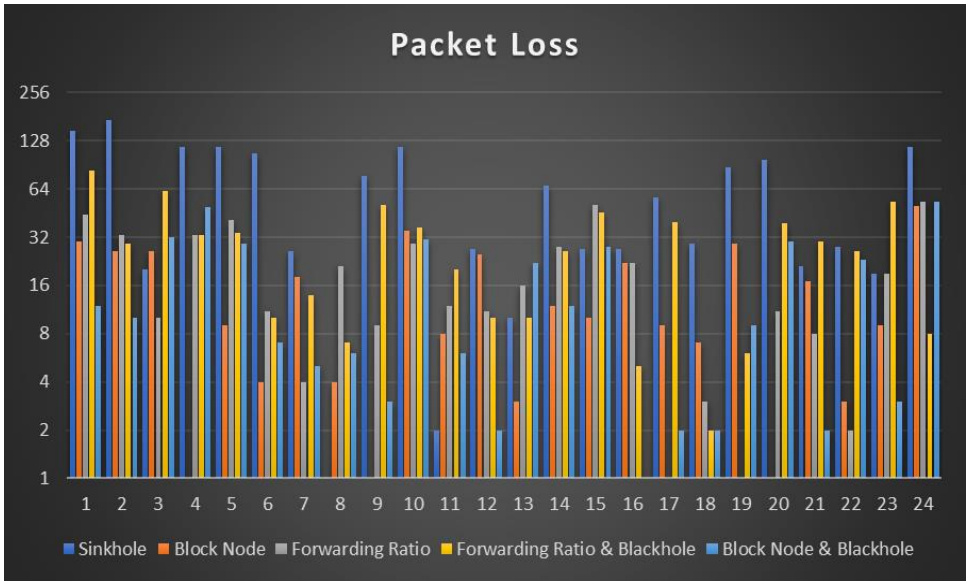


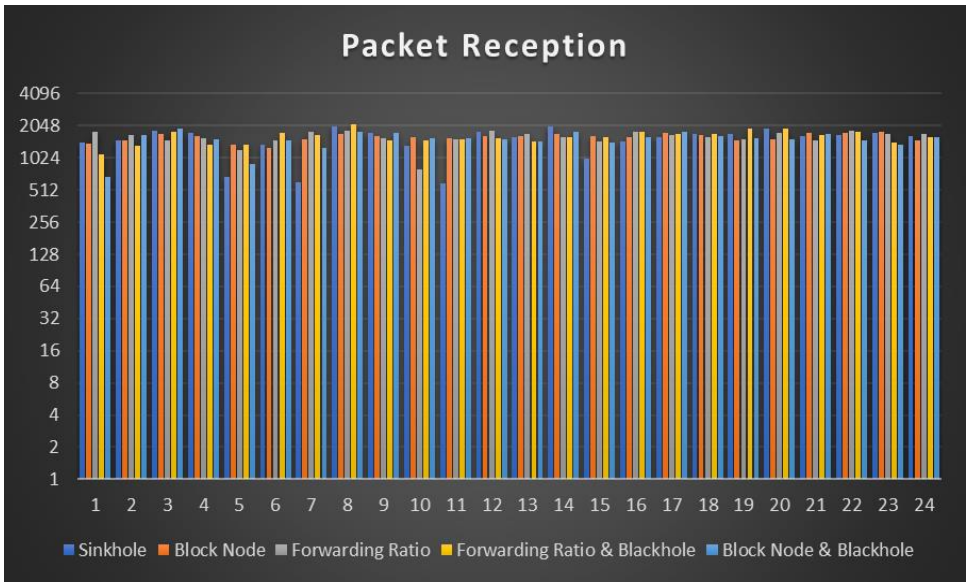
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	122	113	0	58	0	2	45	110	272	93
	2	61	156	0	97	0	35	79	84	22	102
	3	48	204	0	13	0	111	2	133	6	40
	4	34	66	9	119	12	21	3	61	26	53
	5	122	23	0	7	0	0	706	120	169	17
	6	13	265	9	119	2	8	105	5	29	50
	7	28	75	0	88	3	104	3	20	2	11
	8	2	139	4	25	2	38	19	78	0	41
	9	5	6	0	6	1	15	1	2	2	25
	10	35	40	2	63	1	40	3	48	13	51
	11	23	72	0	21	1	17	4	7	5	7
	12	13	226	0	59	8	16	3	26	0	4
	13	10	237	3	144	6	3	1	57	2	177
	14	29	1	4	2	7	2	7	43	3	8
	15	0	98	20	14	7	1	14	14	20	80
	16	45	59	5	91	0	2	1	6	0	2
	17	15	184	12	13	1	66	3	79	1	5
	18	2	6	18	80	0	13	2	0	1	14
	19	62	198	0	10	2	47	7	163	41	98
	20	123	33	206	19	0	82	190	146	303	137
	21	3	180	0	7	0	70	8	142	5	185
	22	133	136	0	41	3	22	3	19	8	61
	23	6	132	17	35	1	52	2	164	12	13
	24	76	154	0	22	38	47	44	55	28	88



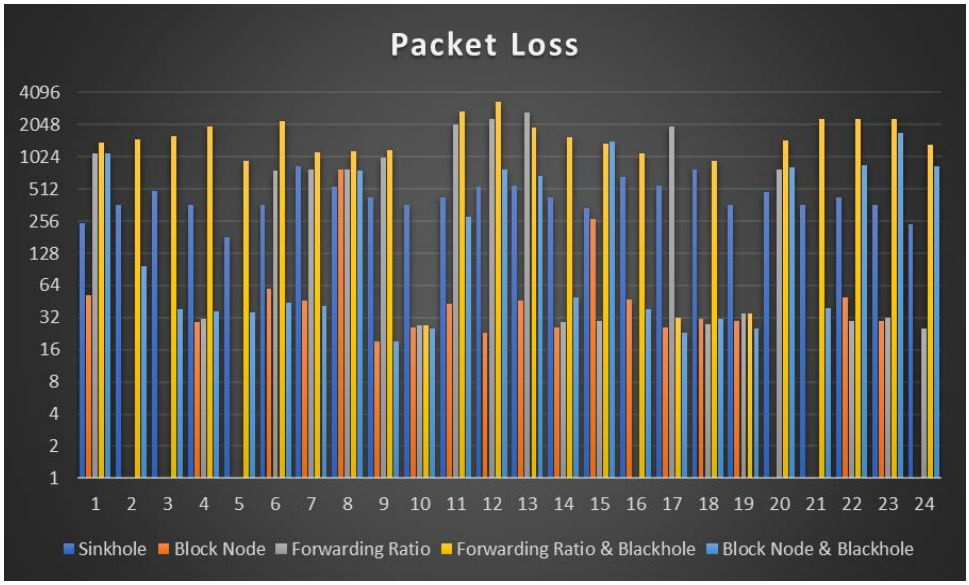


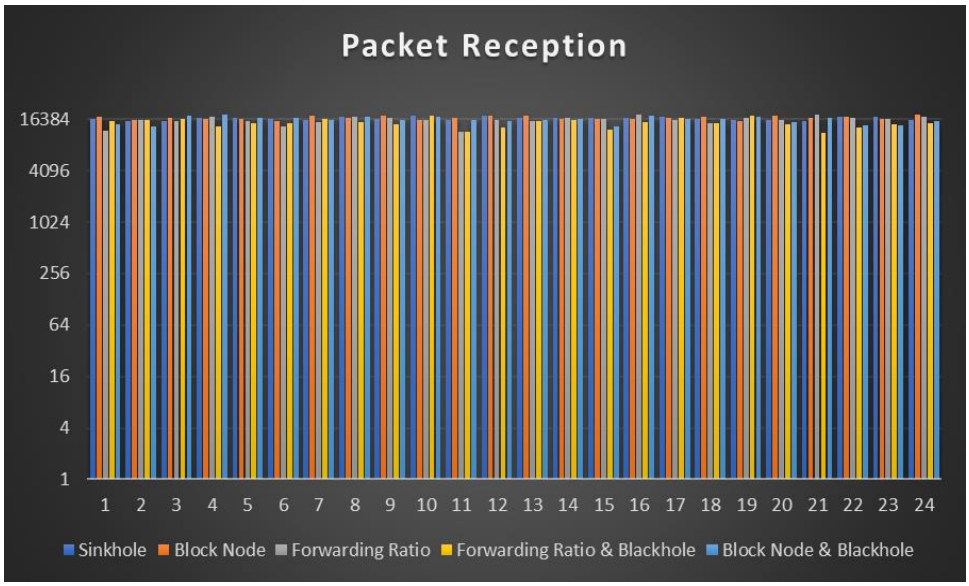
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	147	1414	30	1400	44	1798	83	1093	12	682
	2	172	1507	26	1475	33	1657	29	1332	10	1667
	3	20	1818	26	1707	10	1493	62	1782	32	1932
	4	118	1738	0	1642	33	1547	33	1353	49	1538
	5	117	684	9	1365	41	1205	34	1344	29	891
	6	107	1352	4	1273	11	1503	10	1742	7	1485
	7	26	606	18	1518	4	1796	14	1672	5	1274
	8	1	2020	4	1702	21	1827	7	2127	6	1812
	9	77	1764	0	1640	9	1568	51	1507	3	1743
	10	117	1316	35	1612	29	806	37	1507	31	1564
	11	2	593	8	1552	12	1528	20	1532	6	1558
	12	27	1782	25	1642	11	1827	10	1575	2	1508
	13	10	1608	3	1629	16	1712	10	1461	22	1457
	14	67	2021	12	1705	28	1593	26	1610	12	1790
	15	27	1015	10	1622	51	1442	46	1594	28	1431
	16	27	1455	22	1613	22	1802	5	1799	1	1599
	17	57	1580	9	1736	0	1670	40	1715	2	1811
	18	29	1731	7	1690	3	1590	2	1709	2	1652
	19	87	1711	29	1478	0	1517	6	1919	9	1568
	20	97	1917	0	1517	11	1757	39	1924	30	1542
	21	21	1629	17	1750	8	1481	30	1673	2	1696
	22	28	1671	3	1743	2	1822	26	1774	23	1494
	23	19	1771	9	1776	19	1720	53	1435	3	1372
	24	118	1634	50	1478	53	1725	8	1610	53	1600



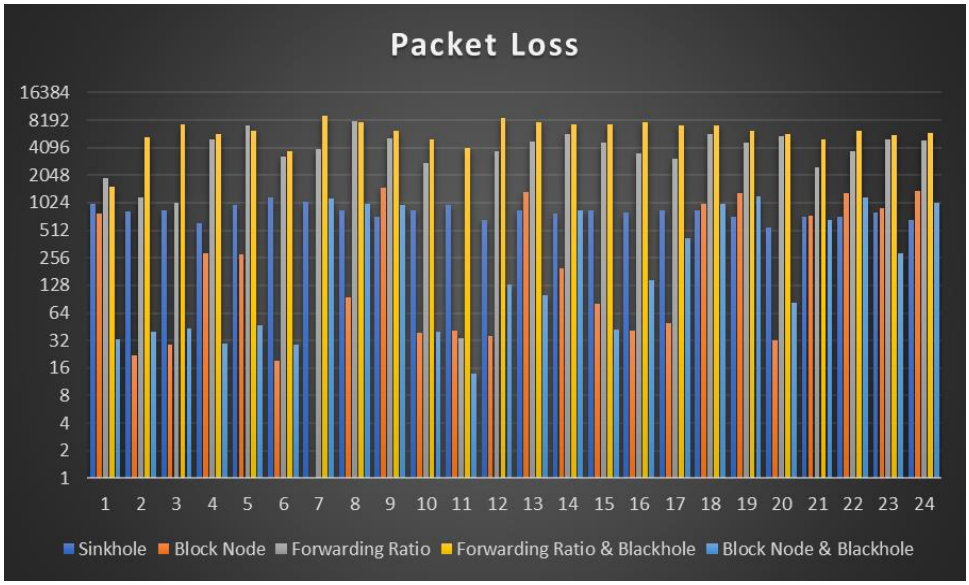


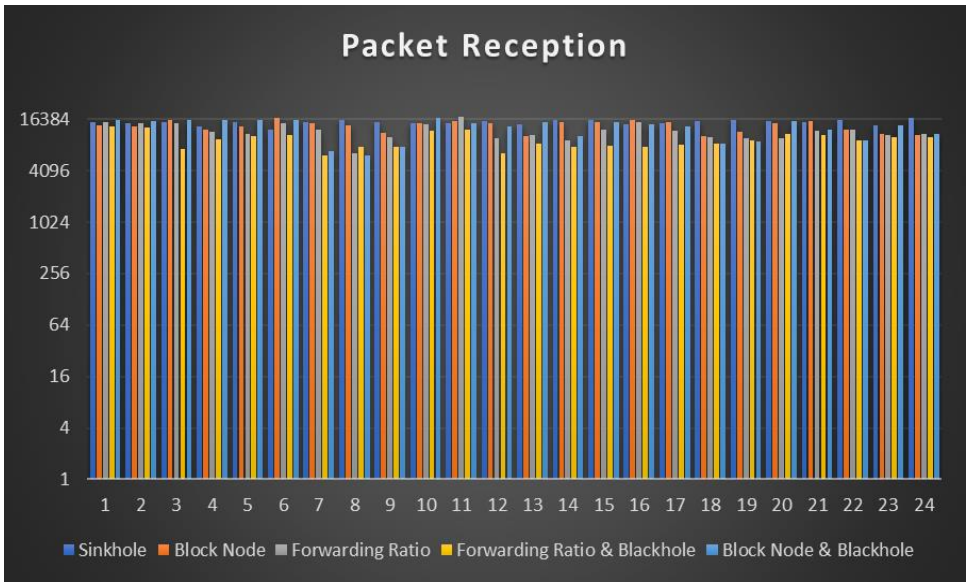
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot RDC Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	242	16677	52	17393	1091	11899	1389	15424	1113	14279
	2	360	15619	0	16281	0	15985	1498	15859	97	13550
	3	485	15609	0	17198	0	15705	1594	16322	38	17936
	4	365	17044	29	16457	31	17763	1990	13426	37	18303
	5	182	16811	0	16744	0	15654	937	14827	36	17004
	6	361	16598	60	15723	757	13650	2218	14593	44	16846
	7	843	16110	46	17814	779	15318	1127	16694	41	15931
	8	542	17518	777	17205	787	17448	1168	15258	768	17539
	9	425	16477	19	18057	1001	16880	1175	14470	19	16121
	10	362	17987	26	16109	27	16095	27	17883	25	17379
	11	427	16246	43	17023	2080	11735	2744	11820	278	16051
	12	542	17776	23	18190	2324	16052	3380	13032	778	15386
	13	546	16899	46	18227	2658	15536	1901	15481	675	15959
	14	426	17240	26	16617	29	17121	1555	16067	50	16486
	15	337	16785	267	16725	30	16462	1370	12502	1408	13471
	16	668	16793	47	16579	0	18308	1112	15251	38	17785
	17	547	17452	26	16949	1960	16215	32	16943	23	16577
	18	785	16352	31	17630	28	14701	946	14852	31	16510
	19	363	16063	30	15562	35	17024	35	17938	25	17683
	20	481	16008	0	17846	778	15919	1469	14161	812	15013
	21	361	15677	0	16973	0	18500	2317	11281	39	16918
	22	425	17293	49	17288	30	17085	2321	13133	845	14027
	23	362	17264	30	16734	32	16461	2304	14241	1693	13940
	24	240	15910	0	18450	25	17706	1322	14517	830	15742



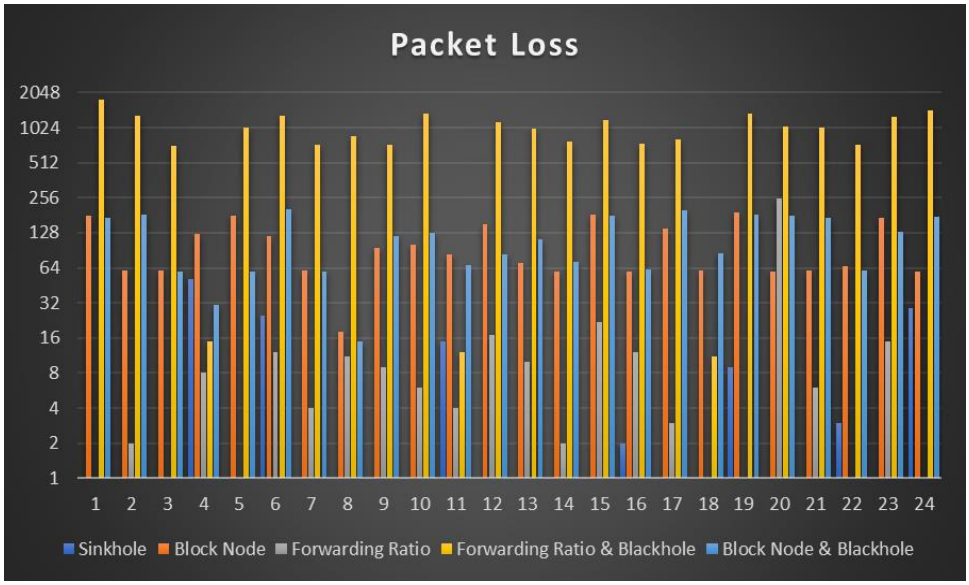


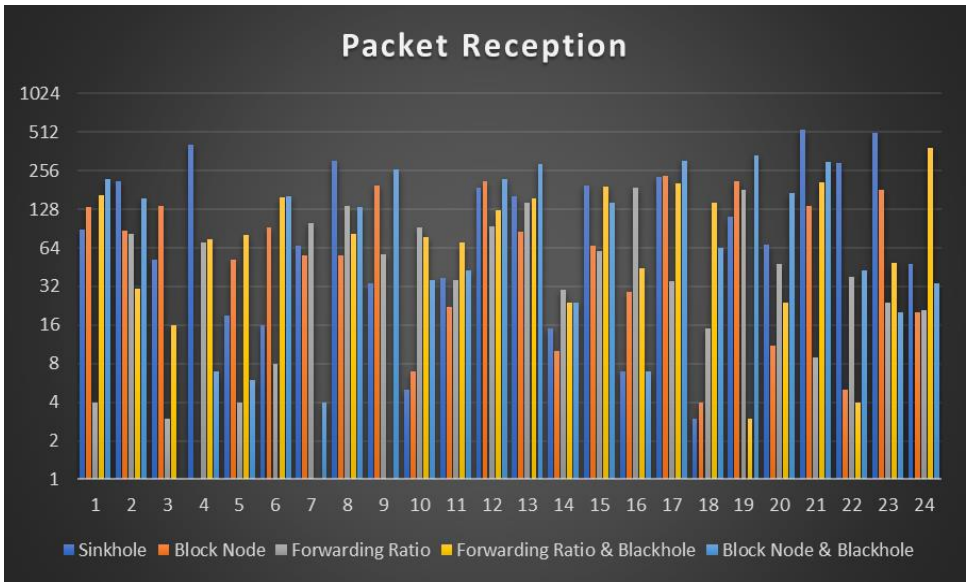
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot RDC Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	982	15107	779	13808	1917	14965	1535	13321	33	16133
	2	823	14591	22	13410	1169	14690	5355	13060	40	15441
	3	848	15016	29	16280	1020	14529	7358	7394	43	16013
	4	606	13399	289	12494	4993	11559	5703	9620	30	16142
	5	977	14949	283	13316	7184	11085	6276	10519	47	15949
	6	1172	12514	19	17133	3261	14646	3767	10571	29	15850
	7	1042	15126	0	14747	3926	12429	9141	6233	1125	7015
	8	842	15893	96	14087	8028	6506	7756	7675	995	6237
	9	726	14960	1490	11466	5193	9998	6271	7802	981	7794
	10	843	14893	39	14869	2757	14482	4975	12140	40	17030
	11	960	14625	41	15688	34	17263	4106	12383	14	14792
	12	668	15562	36	14811	3791	9924	8671	6632	131	13685
	13	854	14240	1338	10406	4821	10763	7714	8385	101	15269
	14	786	15861	197	15075	5830	9351	7307	7737	856	10454
	15	842	15922	81	15018	4674	12378	7318	7947	42	14984
	16	791	14464	41	15972	3505	15056	7753	7796	145	14436
	17	845	14514	49	14958	3072	12060	7175	8212	421	13457
	18	842	15655	1005	10265	5839	10008	7108	8569	983	8572
	19	729	16134	1321	11675	4682	9888	6177	9217	1212	8896
	20	549	15405	32	14760	5527	9746	5715	10902	83	15705
	21	722	15139	748	15539	2467	12178	5011	10640	669	12320
	22	726	16063	1311	12425	3757	12292	6262	9348	1168	9208
	23	792	13845	902	10894	5087	10832	5621	10041	289	13917
	24	667	16989	1380	10710	4903	10892	5966	10124	1012	10899



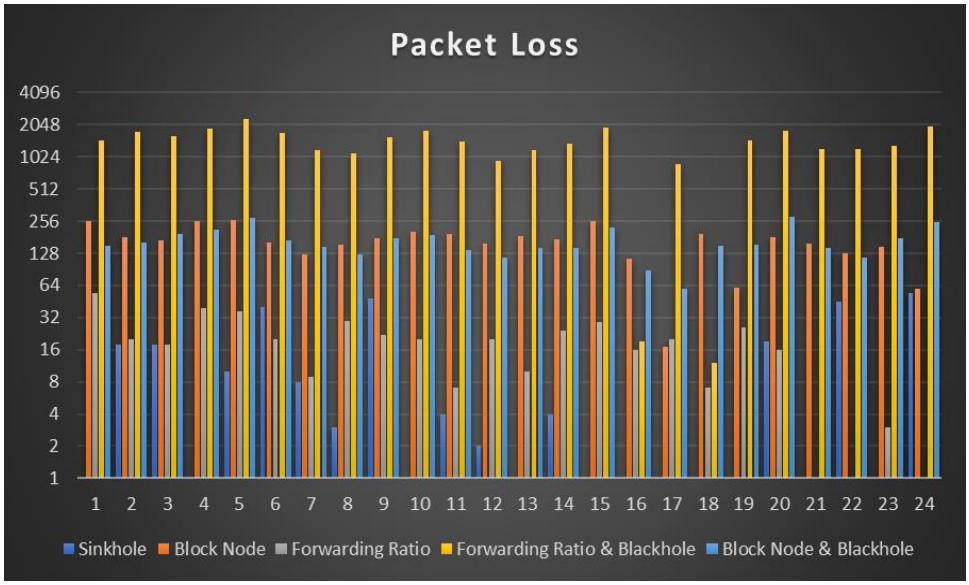


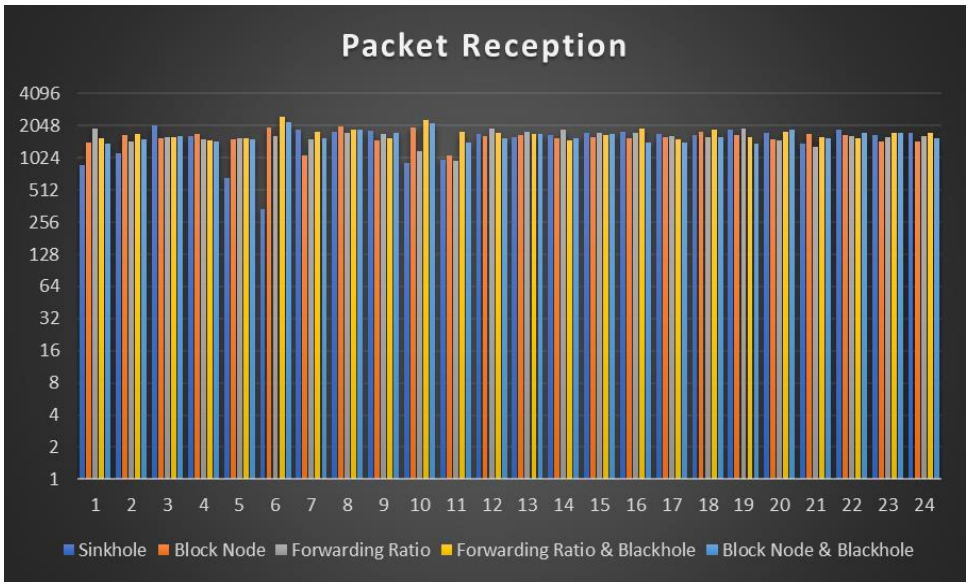
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot delayed Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	0	88	181	132	0	4	1774	165	172	219
	2	0	210	61	87	2	83	1296	31	183	154
	3	0	52	61	135	0	3	720	16	60	0
	4	51	411	124	1	8	71	15	74	31	7
	5	0	19	181	52	0	4	1033	80	60	6
	6	25	16	121	93	12	8	1303	157	205	163
	7	0	67	61	56	4	100	722	1	60	4
	8	0	306	18	56	11	135	856	82	15	132
	9	1	34	94	196	9	57	724	1	119	260
	10	0	5	102	7	6	93	1359	78	128	36
	11	15	37	84	22	4	36	12	71	68	43
	12	0	190	151	211	17	95	1128	126	84	220
	13	0	161	70	85	10	145	999	154	112	286
	14	0	15	60	10	2	30	780	24	72	24
	15	0	195	182	66	22	60	1176	191	179	144
	16	2	7	60	29	12	189	740	44	62	7
	17	0	229	138	235	3	35	814	205	198	306
	18	0	3	61	4	0	15	11	145	86	64
	19	9	112	190	211	0	180	1349	3	183	337
	20	0	68	60	11	251	48	1043	24	181	171
	21	0	535	61	135	6	9	1031	206	173	298
	22	3	295	66	5	0	38	727	4	61	43
	23	0	501	171	182	15	24	1273	49	130	20
	24	29	48	60	20	0	21	1444	387	174	34



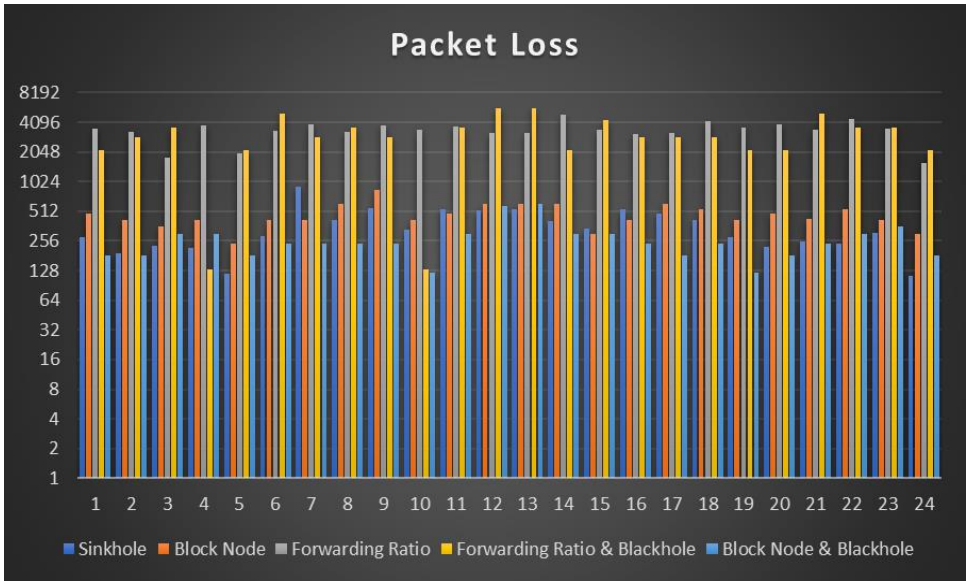


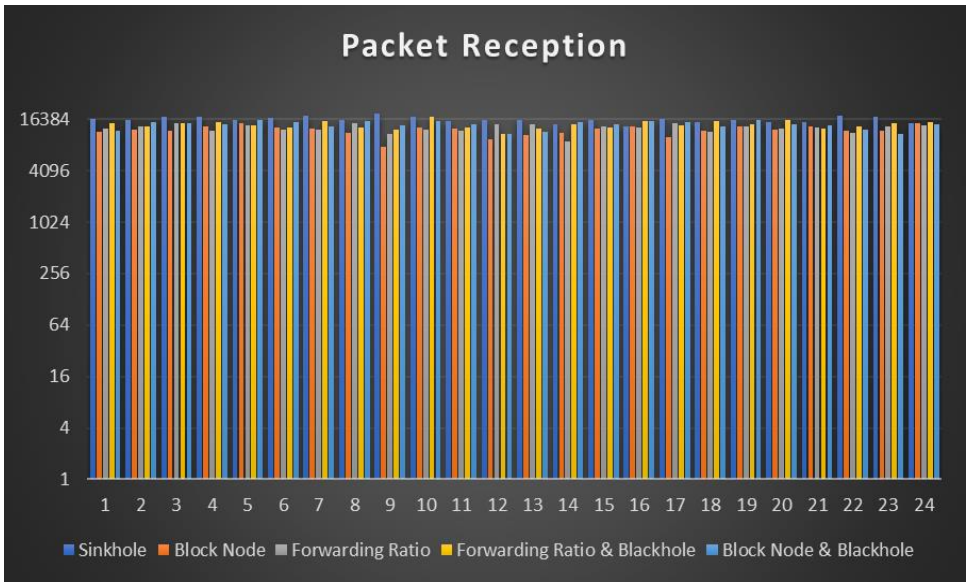
		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot delayed Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	0	880	254	1408	54	1934	1456	1571	149	1388
	2	18	1134	182	1660	20	1458	1761	1717	163	1542
	3	18	2081	167	1574	18	1603	1593	1594	196	1620
	4	0	1644	256	1732	39	1517	1890	1485	211	1473
	5	10	666	261	1528	37	1557	2336	1574	276	1525
	6	40	341	163	1966	20	1618	1700	2489	168	2199
	7	8	1892	125	1081	9	1527	1175	1805	147	1566
	8	3	1799	154	1999	30	1760	1092	1889	126	1880
	9	48	1841	176	1474	22	1700	1564	1572	176	1736
	10	0	920	204	1976	20	1193	1807	2307	190	2169
	11	4	988	194	1078	7	949	1411	1812	137	1412
	12	2	1711	158	1635	20	1944	935	1771	116	1554
	13	0	1614	185	1689	10	1774	1186	1729	143	1698
	14	4	1689	172	1570	24	1883	1359	1505	142	1552
	15	0	1733	255	1603	29	1772	1918	1686	225	1707
	16	0	1782	113	1567	16	1749	19	1930	89	1427
	17	0	1704	17	1611	20	1622	872	1515	60	1433
	18	0	1661	194	1805	7	1603	12	1897	150	1587
	19	0	1875	61	1685	26	1923	1465	1599	155	1375
	20	19	1769	180	1521	16	1479	1811	1805	283	1881
	21	0	1395	159	1704	0	1306	1198	1596	142	1578
	22	45	1899	127	1669	0	1641	1216	1574	117	1744
	23	0	1665	147	1456	3	1596	1311	1766	177	1772
	24	54	1769	60	1455	0	1637	1972	1744	249	1578





		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot delayed RDC Mid	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	282	16460	482	11670	3505	12684	2155	14691	180	11851
	2	190	15881	421	12322	3294	13557	2867	13480	181	15045
	3	229	17313	361	11916	1799	14853	3583	14613	301	14753
	4	216	17705	421	13663	3753	11893	132	14932	302	14433
	5	118	15962	241	14675	1981	13707	2155	13934	180	16017
	6	287	17121	421	13222	3327	12395	5014	13291	240	15268
	7	902	18057	421	12628	3887	12549	2868	15696	241	13358
	8	418	16199	601	11395	3258	14643	3594	13227	241	15391
	9	547	18937	841	7804	3814	11047	2873	12479	241	13801
	10	333	17308	421	12980	3418	12395	130	17340	121	15812
	11	541	15769	481	12817	3745	12125	3590	13048	301	14209
	12	526	15889	601	9488	3148	14390	5635	11029	571	11072
	13	532	16119	601	10657	3222	14154	5632	12821	602	11510
	14	405	14487	601	11306	4840	9125	2155	14136	302	15070
	15	344	16148	302	12650	3398	13495	4303	13235	302	14117
	16	540	13364	421	13616	3139	12927	2869	15673	241	15608
	17	483	16360	602	10029	3157	14839	2878	13962	180	15000
	18	420	15254	542	11934	4175	11787	2870	15684	241	13666
	19	281	16011	421	13618	3649	13440	2156	14369	121	16139
	20	222	15019	481	12422	3940	12862	2156	16063	181	14256
	21	255	15213	423	13511	3465	13214	5017	12566	241	14055
	22	239	17935	541	11991	4366	11275	3588	13531	301	12435
	23	310	17305	422	12115	3479	13378	3584	14780	361	11048
	24	114	14718	301	14852	1590	13749	2152	15191	181	14276





		Sinkhole		BN		FR		FR & BH		BN & BH	
Rerouting & Reboot delayed RDC Top	Run	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink	Lost	Sink
	1	524	14642	1180	4240	6671	11666	3594	13123	362	13302
	2	477	12061	843	7699	5017	12393	10175	7447	901	7838
	3	508	11404	901	7714	6557	7649	9949	7660	841	7778
	4	120	13755	840	8395	5947	9029	7165	10630	602	11326
	5	936	12570	1201	4305	6014	11029	10605	5561	963	5571
	6	1310	10478	1020	5717	5152	11775	11060	6274	961	7144
	7	723	14313	1142	4808	9433	4900	8529	7695	843	7157
	8	715	14833	842	7900	6995	7632	10048	8648	841	8533
	9	276	15293	841	8464	7622	7737	9326	9159	780	8989
	10	988	13916	961	6437	5268	12092	9994	7638	722	7272
	11	990	15127	1141	4917	10062	5055	9356	7699	783	8599
	12	819	13779	961	7107	8088	6881	8582	7640	901	7723
	13	478	13724	1020	6228	7575	5497	9191	8803	721	8889
	14	417	15154	842	8380	7030	9186	8599	9666	722	9293
	15	604	12917	781	7571	7900	7536	5732	9532	722	8711
	16	728	15678	902	7529	6131	7090	9089	8489	841	8486
	17	857	14797	1021	6409	8887	6403	9299	9181	661	10076
	18	350	12865	902	7891	7627	8475	8590	8966	782	8808
	19	469	15169	843	8507	7257	8492	9302	9292	721	10024
	20	382	13833	601	9790	6572	9725	7139	10630	542	9797
	21	114	15834	841	8547	7587	8505	7170	8485	542	10857
	22	657	13847	841	7826	5802	9905	7648	9819	721	9828
	23	576	11538	841	8599	7005	8676	7788	10662	712	9944
	24	114	14801	781	9242	6482	9258	6517	9658	601	11473