Intelligent Route Discovery Towards Rushing Attacks in Ad Hoc Wireless Networks

Udayakumar Allimuthu (udayakumar.allimuthu@gmail.com)
Anna University Chennai https://orcid.org/0000-0001-5376-0327
K Mahalakshmi
KIT: Kalaignar Karunanidhi Institute of Technology

Research Article

Keywords: Attacker Detection, Data Security, Mobile Node Transmission, Mobile Node Lifetime, Route Finding, Routing Security, Rushing Attack, Time Confine

Posted Date: March 9th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-171257/v1

Version of Record: A version of this preprint was published at Journal of Ambient Intelligence and Humanized Computing on April 9th, 2021. See the published version at https://doi.org/10.1007/s12652-021-03195-9.

Intelligent Route Discovery Towards Rushing Attacks in Ad Hoc Wireless Networks

Udayakumar Allimuthu,

Department of Information and Communication Engineering, Anna University, Chennai, Tamil Nadu, India

udayakumar.allimuthu@gmail.com

K. Mahalakshmi, Professor, Department of CSE, KIT-Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India

prof.dr.mlk@gmail.com

Email address of the corresponding author: *udayakumar.allimuthu@gmail.com*

Abstract. MANET (Mobile Ad-hoc Networks) are distributed or delegated away from a central server, authoritative location of wireless networks that communicate without pre-existing structure. Ad-hoc networks are compromising the many types of attacks and routing. In MANET, the routing plays a vital role in terms of packets interaction and data transmission. Due to decentralized control, the MANET data transmission becomes insecure because of dispersed routing on the mobile ad-hoc nodes. Since the efficient route on MANET only controls the packets and does not simplify the route between the source to the destination, the maintenance of route interaction becomes a crucial process. Maintain effective data transactions over the MANET network, and it is essential to improve the route and locate the attacker. Nevertheless, MANET allows for route interaction against security threads. In this research article, four processing schemes are suggested to preserve the security measures against routing protocols. Especially in node communication, the rushing attacker has a significant impact on packet-based data transmission in MANET. Also, for this research, an Attacker detection automation of the Bees Colony Optimization (ADABCP) method is used, as a result of which the desired result is brought about in the effective attacker detection on the routing process. Moreover, the proposed Hybrid Random Late Detection (HRLD) routing protocol manages the MANET routing and overcomes the MANET congestion communication. The Swift Implicit Response Round Trip Time (SIRT) mechanism is generated by the Route Finding Manipulation (RFM) to enhance the performance. This RFM scheme helps to find the optimal routing in a secured manner. The proposed (SIRT-ADABCP-HRLD) approach was compared to the existing ESCT, ZRDM-LFPM, and ENM-LAC approaches, found to have improved by routing and data transmission. Compared to the conventional method, the method mentioned above achieves a better ratio for the end-to-end delay, communication overhead, packet delivery ratio, network lifetime, and energy consumption.

Keywords: Attacker Detection, Data Security, Mobile Node Transmission, Mobile Node Lifetime, Route Finding, Routing Security, Rushing Attack, Time Confine.

1 Introduction

In an ad-hoc network, routing plays a vital role in data packet interaction and data transmission. It is always easy to manage the data transmission over the ad hoc network because of distributed control on the ad hoc network nodes. Since the efficient route on an ad-hoc network only controls the packets and does not simplify the route between the source to the destination, the maintenance of route interaction becomes a crucial process. To maintain routing over the ad-hoc network, it is essential to improve the route and security concerns. Nevertheless, an ad-hoc network allows for route interaction against security threads. Based on the above consideration, a mobile ad-hoc network has an incredible number of mobile nodes. It makes the secured mobile route for data transference, data security, and time delay. The research perspectives are created and provided to the user for communication between the mobile nodes with no trouble. Here, the infrastructure-less network mainly depends on the transfer rate, security, and time. These domains have their operational style that must have applied on the infrastructure-less network, in which the process will be suspended (delay) for entire data transmission [1] [2]. The efficient infrastructure-less network selection has to be done systematically with attacker detection, route finding, time confine, node ranking criteria, interaction history, dead node reduction, and alive node boost-up. These processes meet an efficient transmission on the infrastructure-less network. Attacker Detection Automation (ADA) is employed to classify suitable attackers against other nodes. ADA is used to define the automatic reduction of the attackers who also accommodate the "Swift Implicit Response Round Trip Time" mechanism [3] to evaluate the attacker-less network infrastructure [3]. Possibly data delivery time interval for the mobile node is increased by using Hybrid Random Late Detection (HRLD). This HRLD scheme ensures secure route-finding and data transmission using "Use Best Approximation" which helps observe the routing problem. The route-finding approach is used to retrieve the confidential route between the mobile nodes. This confidential route is useful to find an optimal solution for dead node reduction by using interaction history in a well-organized manner. The working of dead node reduction depends on the time interval assignment. i.e., the time interval that has been assigned to each node in reply to the sender node. This happened on the mobile node key assignment. Within this time interval, the transmitted node directs the reply messages to the transmit node for proving node confirmation. In this way, end-to-end delay is reduced for one-way communication. Finally, the node ranking is taken from the "Past Interaction History" for every transmission. It is used to rank the nodes to select the adequate short time process. The Attacker Detection Automation of Bees Colony Optimization (ADABCP) is run in parallel to update the dead node and active links [4] [5]. The cyclic processes of node ranking express the continuous monitoring system of infrastructure-less network, which produces the enhanced alternative for existing strategies. In conclusion, our proposed research makes the attackers efficient route interaction between the nodes using route finding, time confine, node ranking criteria, interaction history, and dead node reduction. In the result part, the proposed techniques compared with the existing methods like Evolutionary Self-Cooperative Trust (ESCT) scheme [12], Zone-based Route Discovery Mechanism - a Link Failure Prediction Mechanism (ZRDM-LFPM) [9], and Evolving Network Model based on Local-Area Choice (ENM-LAC) approaches [18] [6]. Finally, it found that the proposed SIRT-ADABCP-HRLD process provides the efficient transmission in-terms of end-to-end delay, communication overhead, packet delivery ratio, network lifetime, and energy consumption [7] [8] [9]. Research aspects implemented with the help of network simulator 2. The rest of the research article is organized as follows.

Section 1 discusses the introduction to the research article. Section 2 reviews existing literature work for MANET and existing route selection strategies. Section 3 presents the proposed routing protocols communication for rushing attacker detection. Finally, Section 4 describes the various result-oriented parameters such as end-to-end delay, communication overhead, packet delivery ratio, network lifetime, and energy consumption. At last, Section 5 concludes the article.

2 Related Works

Efficient route interaction and data transference are provided in MANET. It is a collection of mobile node interactions. Route interaction and data transmission over the MANET network are at risk as the attackers have broadened ubiquitously. Thus, route interaction efficiency is crucial. This research work significant role lies in route interaction and data transference across the network against the rushing attacks. MANET (rushing attacks) is the art of securing data by hybrid random late detection protocol and swift implicit response. Nodes interaction can be categorized as attacker detection automation, hybrid random late detection, the best approximation, and past interaction history. These are all the techniques necessary for making the nodes interact efficiently. This survey clarifies a broad review of MANET route interaction condition for efficient routing, especially against rushing attacks, time delay, attacker detection, route finding, time confine, node ranking criteria, and interaction history. It considers the newest routing-based methodologies that present in the route interaction based on MANET. The fundamental commitments of this paper are accompanied by the following table 1 survey.

Table 1. Fundamental commitments of a various research survey

Author (Year)	Li Zhinan et al. (2017) [10]	Hurley et al. (2017) [11]	Bai et al. (2017) [6]
Introduction or Background	Optimized Link State Routing Scheme [12]	Pre-Existing Routing [13]	Cooperative Routing in MANET [14]
Aim or Purpose or Objective	Smooth Mobility and Link Reliability based OLSR (SMLR OLSR)	The flexibility and MANET increasing popular in a wide range of use cases	Cooperative communication in MANET can improve system capacity and energy efficiency
Existing research works	Semi-Markov Smooth and Complexity Restricted mobility model (SMS CR)	Less popular in a wide range of use cases	Lack of a systematically designed cooperative routing scheme
Overcome this problem	Reliability enhanced Multi Point Relay (MPR) Selection in SMLR OLSR	Security protocols to protect routing and application data	NA
Proposed Approaches	Accurate performance analysis, and can achieve longer MPR lifetime and less control overhead	Secure routing and communication security protocols implemented to provide protection	NA
Technology/Methodology	Multi Point Relay (MPR) Selection in SMLR OLSR	Communication security protocols	Novel Constructive-Relay-based Co-oPerative Routing (CRCPR)
Data Analysis	NA	Whilst for node authentication, access control, and communication security mechanism	Energy consumption, energy harvesting, and link break probability
Results /Finding	Accurate Performance Analysis	NA	NA
Conclusion	Accurate performance analysis	Increasing popular in a wide range of use cases	Low energy consumption, high energy harvesting, and link break probability
Author (Year)	**Chen et al (2017) [13]**	**Bozorgi et al (2017) [8]**	**Taha et al (2017) [15]**
Introduction or Background	A Delay Sensitive Multicast Protocol [2]	Electric Vehicles based on Historical Driving Data [16]	Energy Efficient Multipath Routing Protocol [11]
Aim or Purpose or Objective	Utilize the limited resources of MANET efficiently	A routing algorithm that leads to the extended driving range and battery longevity of electric vehicles (EV) is proposed	Energy consumption significant limitations in MANET
Existing research works	Measuring the busy/idle ratio of the shared radio channel, estimating one-hop delay is suggested	locating the time and energy efficient routes	Reducing network lifetime, energy consumption
Overcome this problem		Desired speed profile to be tracked by the driver	Fitness Function technique

Proposed Approaches	Multicast tree, delay sensitive multicast protocol for real-time applications in multi rate	Data mining techniques	
Technology/Methodology	Delay estimation method	Data mining techniques	Ad Hoc On Demand Multipath Routing with Life Maximization, Ad Hoc On Demand Multipath Distance Vector with the Fitness Function
Data Analysis	Increase the network capacity	WarrigalProject	Energy Consumption, throughput, packet delivery ratio, end-to-end delay, network lifetime, and routing overhead ratio performance metrics, varying the node speed, packet size, and simulation time
Results /Finding	NA	Verify the Effectiveness	NA
Conclusion	NA	Verify the Effectiveness	Network Performance Metrics and Parameters

Author (Year)	**Cai et al (2018) [12]**	**Chintalapalli et al (2018) [14]**	**Kacem et al (2018) [17]**
Introduction or Background	Self-Cooperative Trust	multi-objective optimization model	determine an optimal routing of packets
Aim or Purpose or Objective	reliable routing in MANET	secure routing in MANET	find the least-cost routing of nominal traffic and survivability against node failure
Existing research works	open transmission media and the dynamic network topology.	Untrusted, malicious nodes Interaction	pre-existing infrastructure or centralized administration
Overcome this problem	To reduce the Routing Disruptions	optimal route for data forwarding	provide a strategy for sending data at any time between nodes
Proposed Approaches	evolutionary self-cooperative trust (ESCT) scheme	hybrid optimization algorithm, called M-LionWhale	fuzzy synchronized Petri net (SynFPN)
Technology/Methodology	Reputation and Credit-Based Based Approach	quality of service (QoS) parameters	ant system
Data Analysis	Sending / Receiving History Record (SHR):	fitness function	EFMMRP, EELB-Mega, LOADng, and ETX-Ant protocol
Results /Finding	Reduce the Black Hole, Gray-Hole(GH), Mixed Routing Disruption, Malicious Collective(MC), Selfish Node	packet delivery ratio (PDR), throughput, and energy	best routes in the proposed protocol
Conclusion	PDR, throughput, overhead, and end-to-end delay	energy, distance, link lifetime, delay, and trust	It is preventive and quickly adapted to the changes also detect faulty nodes

			and speedily propose new routing tables, to avoid extensive transmission delays that lead to packet losses

Author (Year)	Liu et al (2019) [18]	Khudayer et al (2020) [9]	Zhang et al (2020) [19]
Introduction or Background	Location preference	Source routing in MANET network topology	efficient use of multiple sub-paths and network traffic load
Aim or Purpose or Objective	Reduce random failures in MANET.	Reduce link breakages	optimal data transmission
Existing research works	Complex network theory.	Source routing in MANET	MSDs with multiple network interfaces
Overcome this problem	Random Edge Failure	Enhance on-Demand Source Routing Protocols	hidden Markov model (HMM)-based optimal-start multipath routing scheme
Proposed Approaches	Evolving Network Model based on Local-Area Choice (ENM-LAC)	zone-based route discovery mechanism (ZRDM) and a link failure prediction mechanism (LFPM)	QoE-driven MPTCP-based data delivery model
Technology/Methodology	Average Shortest Path Length (ASPL)	Flooding	past connection state and improve Open Shortest Path First MANET Designated Routers (MDR)
Data Analysis			data delivery model
Results /Finding	Created network structure against attacks	Efficient Route Discovery	MPTCP subpaths
Conclusion	the accuracy and general framework are studied on MANET (ASPL)	Route Discovery and Link Failure Detection against Routing Protocol	balancing and increase throughput and reliability

Table 1 shows some reviewed study collaboration methods and represents the prominent issues. Table 1 and its continuity shows a route interaction between the most active nodes in MANET. These tables feature (background, objective, existing research works, problem definition, proposed approaches, data analysis, results, and conclusion) to extract every arrangement into a particular classification and with agreeable methodologies in the proposed efficient route interaction of mobile nodes in mobile ad hoc network. After an article-by-article investigation of the schemes, efficient route integration situations still demonstrate a few difficulties are viewed as a research survey in table 1. Previous research frequently-absents efficient route interaction models that did not guarantee data transference, data security, and time delay. It is also challenging to ensure system attacker detection, route finding, time confine, and security [11] [20]. The proposed system introduces all the above requirements that turn mobile nodes efficient route interaction in multipurpose conditions. The proposed part of the research plans exhibited in the past has potential difficulties. The most noteworthy are counted in the reference section as given in table 1. Cai et al. (2018), Kacem et al. (2018), and Zhang et al. (2020) [12] [17] [19] discussed the mobile node transmission and high dead node issues. Even though MANET means measuring such problems, the proposed system can expose the problems and establish regularity and routing. Hurley et al. (2017), Li Zhinan et al. (2017), Bai et al. (2017), and Taha et al. (2017) have [6] [10] [11] [15] discussed the security, the trust issues in their proposed frameworks and stated that they require additional disclose in regularity based routing security, further work on the MANET. These further contribution actions are promoting the existing routing security. Bozorgi et al. (2017), Chen et al. (2017), Chintalapalli et al. (2018), and Khudayer et al. (2020) [8] [9] [13] [14] have discussed the transferring time issues. The systems with numerous mobile nodes passing data between nearby route nodes require a more efficient route. The proposed interaction history finds the factor which adds multi-routing history to the framework. Liu et al. (2019) proposed [18] source routing in MANET network topology, which also discusses the mobile nodes discovery issue. Their proposed frameworks commonly expect source hubs disclosure and the end goal to determine the best node to coordinate and accomplish an ideal routing. It may be the appropriate idea for solving the mobile nodes discovery issue in MANET; in any case, it can be the toughest one within sight of inactive mobile nodes issue. Li Zhinan et al. (2017), Chen et al. (2017), Taha et al. (2017), and Zhang et al. (2020) node multitasking issue [11] [10] [21]. Mobile nodes can have a specific IP address as well as routing information. In this manner, data transformation goals must be expected to meet the needs to adjust and standardize node correspondence to accomplish an ideal data transfer. Kacem et al. (2018), Liu et al. (2019), and Khudayer et al. (2020) discussed [8] [13] [14] the node failure. In their perspective, adaptation to internal failure separation of a mobile node causes reduction of the lifetime of nodes, which corresponds to node failure. The saved interaction history of the node interaction signals helps avoid further interaction on the inactive failure node with specified request/response periods. Subsequently, it is essential to recognize the node, recover the earlier transaction, and retransmit from the initial nodes to the destination mobile nodes.

This comprehensive way has given a detailed review and the best investigation of mobile nodes efficient route interaction in MANET. It also worked out broad research on route interaction and significant data transformation. However, table 1 gives a detailed relevant work review of all the outstanding route interaction models accessible in MANET. Even the same process displays yet with various domains like WSN communication and so on. It concentrates on the multiple issues in the efficient route interaction.

3 Proposed routing protocols communication for rushing attacker detection

Figure 1 demonstrates the process of the rushing attack establishment communication channel. In this circumstance, MN1 –sender, MN17 –receiver, t – the distance between MN1 and MN17. (MN8) and (MN9) is the rushing attack route and the actual route of the routing protocols communication, index sender to receiver [7] [22] [23]. It is referred to the MN1 –sender, index MN8 to the receiver MN8, R1 is the general rushing route, R1MN1→ MN2→ MN5→ MN10→ MN9 is the total amount of nodes directivity between MN1–sender, MN17 –receiver, without (R1, MN1) and (R1, MN17) is 5. It is referred to as the MN1 –sender, index to the receiver MN9, R2 is the general rushing route, R2MN1→MN4→MN9, and R3 is the available rushing route, R3MN1→ MN4→ MN8 is the total amount of nodes directivity between MN1 –sender, MN17 –receiver, without (R2, MN1) is three and (R3, MN17) is 3. The distance from MN1–sender or MN17–receiver to the center of the area routing protocols communication is concerned with the distance from the attackers to the sender or receiver (MN8) and (MN9) [4] [2] [24] [25].

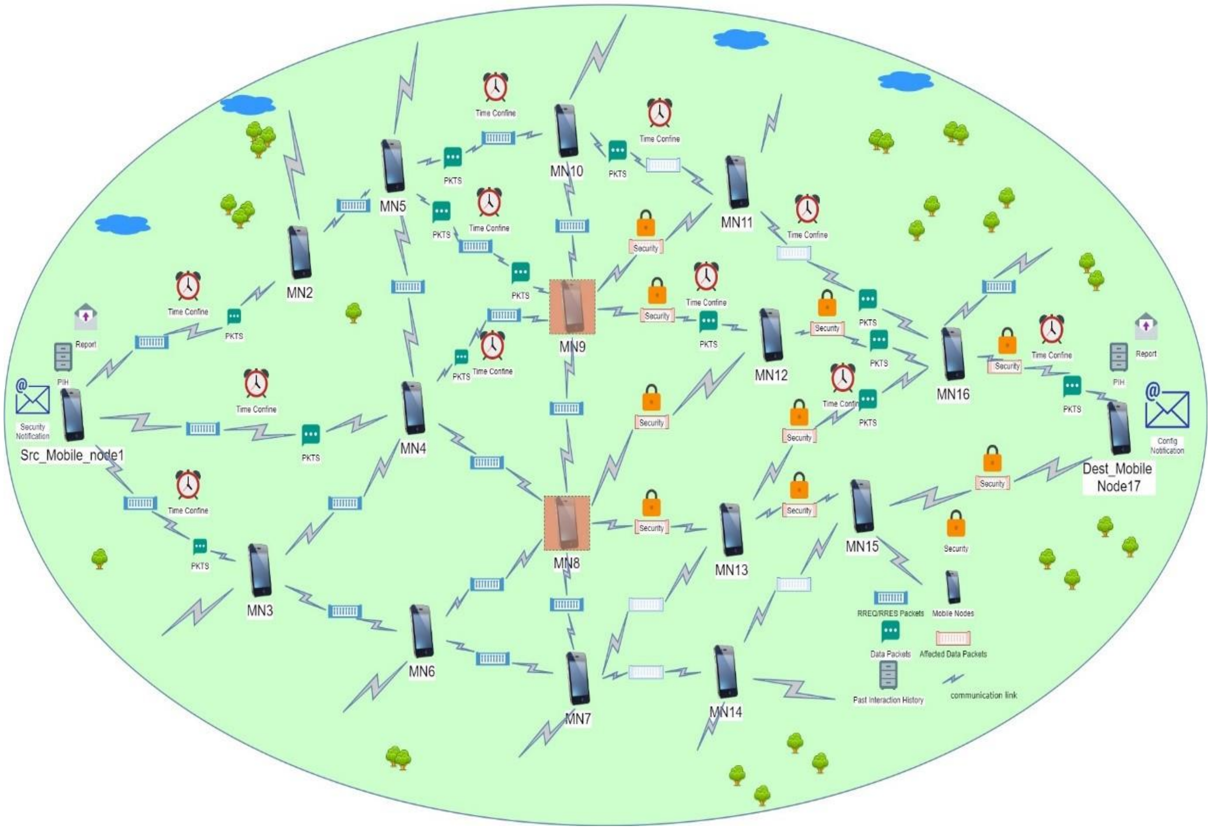


Figure 1. Simulation of MANET Routing protocols communication and rushing attack scenario for 17 nodes with the accommodative procedure

3.1. Attacker Detection Automation of Bees Colony Optimization (ADABCP) method

In this section, the proposed attacker detection automation of Bees Colony Optimization (ADABCP) uses a routing framework based on Bees Colony Optimisation that offers improved network traffic routing in MANET scenario to improve the energy efficiency in terms of three factors [3] [16] such as

1. Routing operation: To perform the movement of nodes within the boundary in MANET
2. Detection automation application: To optimize route on attacker detection
3. Control parameters: To improve the energy efficiency of attacker detection automation

This attacker detection automation of Bees Colony Optimization (ADABCP) deals with the mobile ad hoc-network attacker finding technique, where mobile nodes are randomly distributed in a large field of the environment [31] [32] [33] as shown in figure 3 [69].

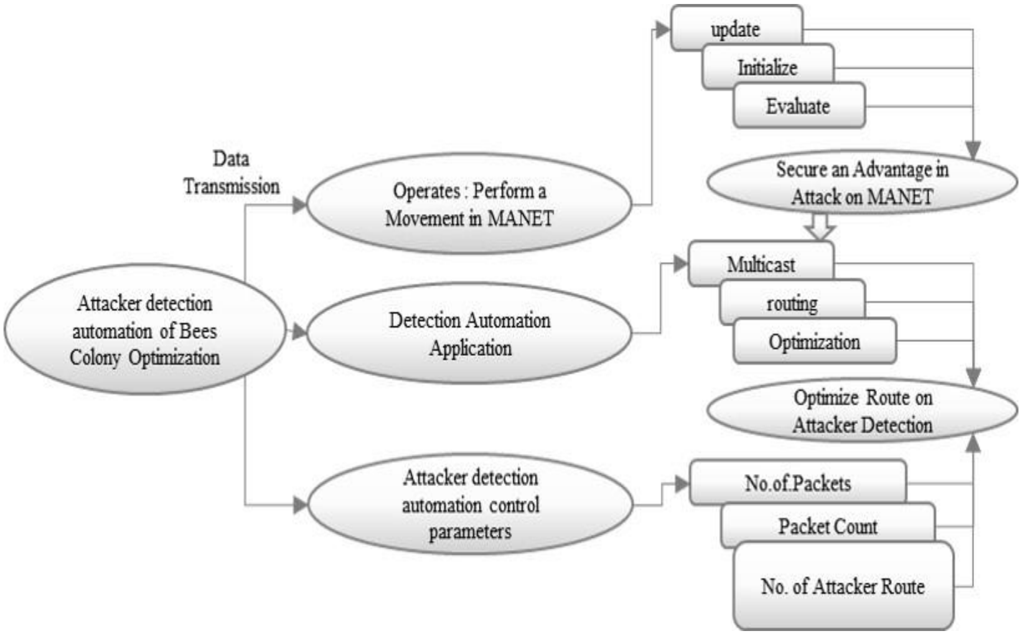

update
Initialize
Evaluate
Data Transmission
Operates : Perform a Movement in MANET
Secure an Advantage in Attack on MANET
Multicast
routing
Optimization
Attacker detection automation of Bees Colony Optimization
Detection Automation Application
Optimize Route on Attacker Detection
Attacker detection automation control parameters
No.of.Packets
Packet Count
No. of Attacker Route

Figure 2. Activities of attacker detection automation of Bees Colony Optimization (ADABCP) on participated mobile nodes based routing algorithms for route optimization in mobile ad hoc networks.

Figure 2 discusses the Attacker Detection Automation of the Bees Colony Optimization (ADABCP) method employed in MANET to accomplish the appropriate refinement on the routing issues. Compared to the "intrusion detection automaton", "hybrid random early detection", "node ranking method", the proposed ADABCP method has been the most secure and has optimal paths in MANET routing. This research considers the number of presented live moveable nodes-based agile algorithms in a routing operation, namely "Use Best Approximation" and the "Swift Implicit Response Round Trip Time" mechanism is suggested. This "Use Best Approximation" predicts the efficient route in an optimized manner. "Swift Implicit Response Round Trip Time" also supports managing global optimization [34]. The combination of the "Use Best Approximation" and "Swift Implicit Response Round Trip Time" mechanism produces the Modified AODV and Hybrid Random Late Detection (HRLD) for route finding, time confine against the attacks like (Rushing attacks, Sybil attacks). In this research, the rushing attacks are taken because they allow denial-of-service, especially since these attacks make duplicate copies of the original mechanism and spread attack activities to the nearby nodes route by accessing route and also gain access to original sending data from source to destination [35] [36].

The three factors are followed in the ADABCP method. First, the routing operation performs the node movement within the boundary in MANET [37]. Hence, head nodes are chosen in the transmission environment. This process is also called node initialization [38]. Secondly, the detection automation application is also used for optimizing routes on attacker detection. Whenever the head nodes of the selected transmission environment form a time limit, i.e., each node has been generated for individual packet transmission around the nearby nodes, the Node id is determined. The initial nodes incremental values assign this node-id determination to the final node of a transmission environment. From this consideration, the nodes start the packet transaction around the nearby nodes. In this condition, if the node is sharing the information based on inter-connectivity, the routing path is built by sharing nodes, which is used to merge all nodes coordinate systems. All nodes are placed randomly in a large transmission environment field in this era, and RREQ/RREP messages are broadcasted. In these circumstances, each node will then find its node grade, node id, and distances of the neighboring node. A source node with the lowest ID between its adjacent nodes becomes a transmission environment initiator node, and the timer starts [16] [39].

Finally, control parameters are effectively applied to the detection automation to improve the energy efficiency on the head node of the transmission environment [40] [41] [42]. However, the node stops the timer and becomes a member of the transmission environment if it receives a cluster head declaration from other nodes before expiry. The head-node transmission environment floods the head-node declaration messages to the hops. There are two cases found in this packet RREQ/RREP messages broadcasting. Firstly, it is found that any node from the transmission MANET environment head nodes are a member of MANET. Secondly, every node between hops from the head node of the class becomes a candidate for a new head node of the MANET surroundings. Some boundary nodes in a temporary transmission environment are given a declaration message from the head of a neighboring transmission environment with a time to live of high value. These nodes are called attacker nodes with one or more numbers. This is called the rushing attacker node [5] [25] [26]. Later in the coordination process of system integration in the transmission environment, these nodes are employed. One of these candidate nodes is randomly selected by the transmission environment head node. It then provides the head node to the neighboring transmission environment with information about the chosen attacker node. For the data from the packet transaction of a node-id with increment, a value checks the sender route. It also checks the neighboring node path with their environment [39]. From this consideration, each node shares two nearby nodes that are overlapping through this process with each of its MANET surroundings. This step is that the relative coordinate systems between two successive mobile nodes are combined in two overlapping nodes. Using the "Received Signal Strength Indicator" based on distance information and the IDs of neighboring nodes, each head node supported by its members of an own overlapping node will complete the routing. By combining relative coordination systems between nodes, the ADABCP algorithm achieves a single relative coordinate system. Each node belongs to at least two routes and is assigned relative addresses from all of the routes head-nodes. This allows the aggregate node to have a relative address for each nearby node to the current node. It is used for the integration of neighboring coordinate systems [33] [43]. Figure 3. shows the routing protocols communication for rushing attack, which concerns the routing communication with route projection for instance of "Attacker detection automation", “modified AODV” and “Hybrid Random Late Detection (HRLD)”, “Swift Implicit Response Round Trip Time”, “Use Best Approximation” and “Past Interaction History” [15] [24] [26] [67].

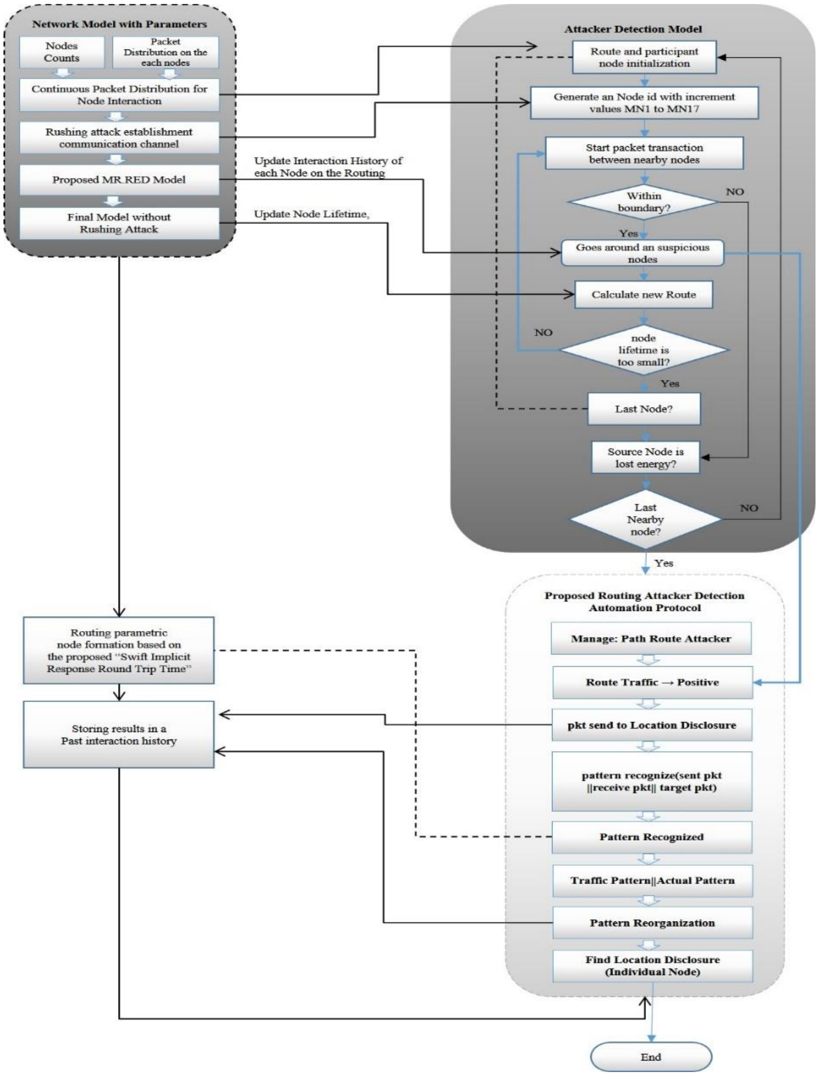

Network Model with Parameters
Nodes Counts
Packet Distribution on the each nodes
Continuous Packet Distribution for Node Interaction
Rushing attack establishment communication channel
Proposed MR RED Model
Final Model without Rushing Attack
Update Interaction History of each Node on the Routing
Update Node Lifetime,
Attacker Detection Model
Route and participant node initialization
Generate an Node id with increment values MN1 to MN17
Start packet transaction between nearby nodes
Within boundary?
NO
Yes
Goes around an suspicious nodes
Calculate new Route
NO
node lifetime is too small?
Yes
Last Node?
Source Node is lost energy?
Last Nearby node?
NO
Yes
Proposed Routing Attacker Detection Automation Protocol
Manage: Path Route Attacker
Route Traffic → Positive
pkt send to Location Disclosure
pattern recognize(sent pkt ||receive pkt|| target pkt)
Pattern Recognized
Traffic Pattern||Actual Pattern
Pattern Reorganization
Find Location Disclosure (Individual Node)
Routing parametric node formation based on the proposed “Swift Implicit Response Round Trip Time”
Storing results in a Past interaction history
End

Figure 3. Flow diagram of the proposed attacker detection automation algorithm

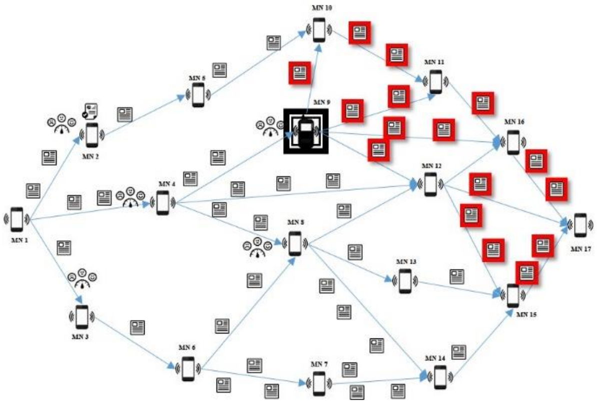


Figure 4. Example interconnected system clarifies the rushing attack after successive route request/route reply. The block highlighted nodes describes the rushing attack scenario on attacker detection automation of bees colony optimization protocol.

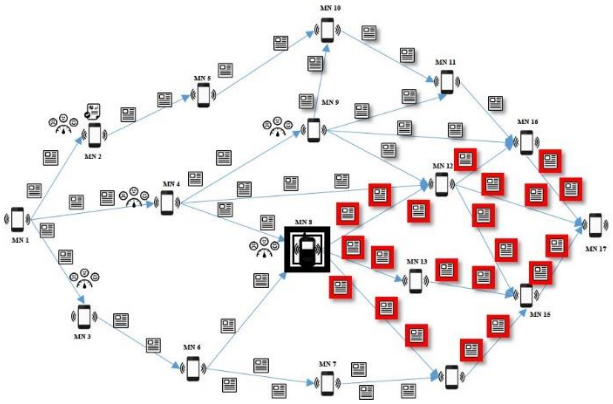


Figure 5. The above figure clarifies by giving an example of another rushing attack on the same network. The block highlighted nodes describes the rushing attack scenario on attacker detection automation of bees colony optimization protocol. The verification confirmation used to detect the rushing attack on this scenario based on the attacker detection automation of bees colony optimization protocol

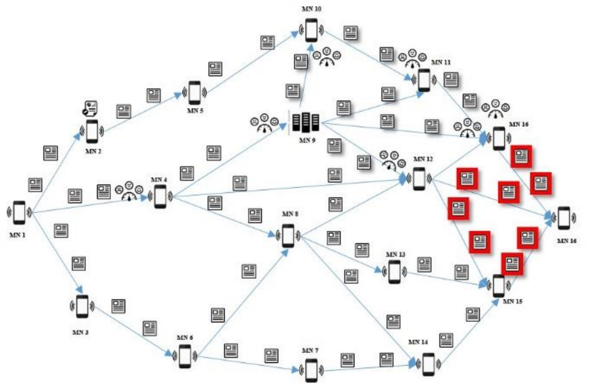


Figure 6. Detecting and removing malicious nodes with the multicast routing protocol with the neighbor node selection at the presence of rushing node at near source

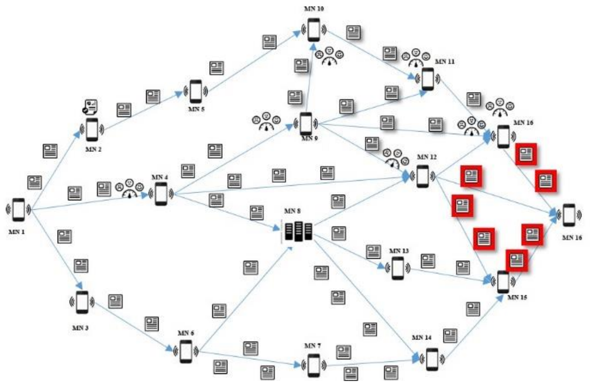


Figure 7. rushing attack prevention for MANET using random route selection to make attacker detection automation more efficient. A set of malicious nodes is rushing anywhere within the network.

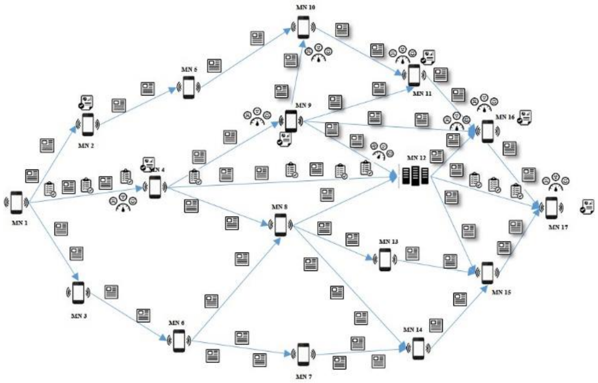


Figure 8. Our combined mechanisms to secure route discovery protocol against the rushing attack. The topology of an Optimum route selection in MANET after invoking early route detection with final multicast tree

Figure 4 to Figure 8 describes the rushing attack behavior during the route selection process of the SIRT-ADABCP-HRLD protocol. The source and destination nodes are represented as MN1 and MN17, respectively. The blue arrow represents the path of the RREQ packet. RREQ contains information to calculate the shortest path values. The (red-highlighted) packets represent the RREP, and the number represents the link attack probability. Figure 4 and figure 5 show that the characteristics and process flow described are based on the attacker detection automation algorithm. The nodes consideration on a proposed network model sets the network model following the nodes count and packet distribution on each node [22]; meanwhile, the average rate (nodes) at which packets are arriving to get served are based on the packet distribution range parameters of the transmitter and receiver arrays. The standard time interval of every packet that is arriving at the destination is fixed based on the request/response round trip time/delay.

In the proposed mechanism, the request/response round trip time/delay is demanded by a packet to travel from an origin to a finishing terminus [27]. This might be calculated by combining the time demanded by a packet to travel from the finishing terminus to a source (i.e., acknowledgment). This is also called the propagation times between the two alive nodes.

The Node Propagation Times (NPT) on the MANET packet transmission is calculated based on the following equation.

$$Nodes\ Propagation\ Time = \sum_{t=\mathrm{MN1(sender)}}^{\mathrm{MN17(receiver)}} \left[\frac{1}{(\mathcal{M}_t - \mathcal{L})}\right]_{forward} + \left[\frac{1}{(\mathcal{M}_t - \mathcal{L})}\right]_{Reverse} \tag{1}$$

From the above equation 1, the NPT calculation is the number of data requests (packets) per second transmitted concerning the distance (t) of each node on the MANET boundary. Perhaps the forwards are described based on the MN1 –sender, MN17 –receiver forwards transmission. At any legitimate packet, communication between nodes (preferably by our concern on the forward route R1MN1→ MN2→ MN5→ MN10→ MN9, R2MN1→ MN4 → MN9, and R3MN1→ MN4→ MN8) are considered as the forwards transmission. Meanwhile, the reverse might be the acknowledgment for individual transmission. (preferably by our concern on the reverse route R1MN9→ MN10→ MN5→ MN2→ MN1, R2MN9→ MN4 → MN1, and R3MN8→ MN4→ MN1). The average rate at which packets are sent and arrived is to be calculated. From this consideration, the node detection model and its parameters are generalized, and tunneling will allow simulation of the node propagation process with different time duration of the attacker node under different route conditions. The actual route function determines the probability of previously sending and receiving history direction. The proposed routing protocol is the weighted sum of the node resending and receiving functions works based on the routing protocol and their steps [28] [29] [30] [68].

3.1.1. Algorithm for Attacker Detection Automation of Bees Colony Optimization (ADABCP)

To solve route optimization issues on the MANET against the rushing attacks, Attacker detection automation of Bees Colony Optimization (ADABCP) is proposed.

The ADABCP has two stages of route organization and route reorganization [36] [44] [45]. A partial solution with individual exploration and collective experience is generated in the pattern reorganization used in the pattern reorganization [44] [46]. During the step pattern reorganization, the probability information is used to decide if the current solution should still be explored in the next step or the newly selected area is to be started. The new one is determined with probabilistic techniques like the selection of the tunneling route [33].

The route factors are a significant part of route detection, which helps discover attackers in the path, as discussed in table 2 for R1≡ MN1→ MN9. Meanwhile, the route factors are a significant part of route detection to realize and discover attackers in the path, as discussed in table 3 for R2≡ MN1→ MN9. The route detection recognizes and finds attackers in the path, as discussed in table 4 for R3≡ MN1→ MN8. Route factors are remitted between the source and destination in the path on the current route. It helps to achieve the Solution against the attacker concerning the previous experience on the route (i.e., Past Interaction History). This network arrangement must suit the packet delivery within the route capability exploration.

Route equivalence is a way for the route to prevent early detection on the route. It helps in the random late detection on the route. This might be appreciating the equivalent route comparison and past interaction history to participate in the nodes on the preferable routes. In this research, three preferable routes are available, and they are

- The first preferable route R1≡ MN1→ MN2→ MN5→ MN10→ MN9,
- The second preferable route R2≡ MN1→ MN4 → MN9 and
- The third preferable route R3≡ MN1→ MN4→ MN8

In this era, the process state accumulates the route confirmations special attention by adding route parameters to the source and destination nodes when it is available without attackers on the current path. Meanwhile, the past interaction history of routing in MANET is useful in redirecting the valid route with control parameters by "Past Interaction History". This transmission refers to the history packets, which are only two-node transmission routes and provide a terminal connection in the session in the MANET environment.

From this consideration, to optimize the route state problem, this research employs route organization and route reorganization. Route organization is defined by a large data stream, and it receives values for various mobile node parameters. Each subset of the parameters can be viewed in this space as a location. Where total characteristics exist on the forwarding transmission between nodes, then types of the subset will be available on forward transmission between nodes, which differ in each subsets length and other parameters [47]. The optimal position is the shortest length subset and the lowest difference in correlation between the initial and sub-set parameters. A swarm of bees is then placed in this scenario, which flies to the best place. They aim to pass and change their position over time, communicate with one another, and look for the best location at a global level, i.e., "Location Route Organization Node". Iteratively, the convergence of the process results in optimal routing [16] [46].

Table 2. Route organization and route reorganization of R1≡ MN1→ MN9

Preferable Route	**Active Node**		**Route Factors**	**Route State**	**Process State**	**Route Equivalence**	**Developed Next State**
R1≡ MN1→ MN2→ MN5→ MN10→ MN9	Node MN1→ MN2	Solution	Partial		Half of the routing process	Comparison result: never changes location	Route refinement result: packets deliver through the first Route
		Experience	collective		Past Interaction History		
		Exploration	Individual route		Uniqueness: automation	Organization: Route with no attacker	
	MN2→ MN5	Solution	Compare the packets with MN1→ MN2		Successive process MN2→ MN5	Comparison result: current node location matching with the previous node history instead of the current location.	Route Refinement Result: Redirect from MN1→ MN2 and add match case with current location.
		Experience	Collective: route stage from MN1→ MN2→ MN5		Past interaction History		
		Exploration	Individual route		Uniqueness: Update Automation	Organization: route with attacker indication not much bogus	
	MN5→ MN10	Solution	Partial		Process near to bogus	Comparison result: route collect the data from the MN2→ MN5	Route refinement result: Getting packets from MN2→ MN5 and add match case with current location MN10
		Experience	Collective: MN10 node Ids		Past interaction History		
		Exploration	Next Individual route		Uniqueness: attacker detection	Organization: refining the attacker with automation	
	MN10→ MN9	Solution	Partial		A process on attacker node	Comparison result: Reach nearby Destination Nodes on the route (R1)	Route refinement result: R1 found the route for R1≡ MN1→ MN2→ MN5→ MN10→ MN9
		Experience	collective		PIH: “Past Interaction History” in this transmission refers to the history packets data		
		Exploration	Individual route		Uniqueness: R1 route detection	Organization: route arranged for MN1→ MN2→ MN5→ MN10→ MN9	

Table 3. Route organization and route reorganization of R2≡ MN1→ MN9

Preferable Route	Active Node	Route Factors	Route State	Process State	Route Equivalence	Developed Next State
R2≡ MN1→ MN4 → MN9	Node MN1→ MN4	Solution	Partial	Successive process MN1→ MN4	Comparison result: never changes the location of the second route	Route refinement result: packets deliver through the Second Route
		Experience	Collective: MN4 node Ids	PIH		
		Exploration	Individual route	Uniqueness: route detection	Organization: Route with no attacker	
	MN4→ MN9	Solution	Partial	Process on attacker node	Comparison result: current node location to be matching with the previous node MN1→ MN4 instead of the current location MN4	Route Refinement Result: Redirect from MN1→ MN4 and add match case with current location MN4
		Experience	Collective: MN9 node Ids	PIH		
		Exploration	Individual route	Unique: detection automation techniques	Organization: route with attacker indication much bogus	

Table 4. Route organization and route reorganization of R3≡ MN1→ MN8

Preferable Route	Active Node	Route Factors	Route State	Process State	Route Equivalence	Developed Next State
R3≡ MN1→ MN4→ MN8	Node MN1→ MN4	Solution	Partial	Successive process MN1→ MN4	Comparison result: route collect the data from the MN1→ MN4	Route refinement result: packets deliver through the third Route
		Experience	Collective: MN4 node Ids	PIH		
		Exploration	Individual route	Uniqueness: attacker detection	Organization: refining the attacker with automation	
	MN4→ MN8	Solution	Partial	Process on attacker node	Comparison result: Reach nearby Destination Nodes on the route (R2)	Route refinement result: Getting packets from MN1→ MN4 and add match case with current location MN8
		Experience	Collective: MN9 node Ids	PIH		
		Exploration	Individual route	Unique: detection automation techniques	Organization: route with attacker indication	

Meanwhile, it represents the total characteristics that exist on reverse transmission (i.e., acknowledgment) between nodes, then describes the subset types that will be available on reverse transmission between nodes, which differ in the length of each subset and other parameters. The optimal position is the comparative length subset and the lowest difference in correlation between the initial and sub-set parameters. A swarm of bees is then placed in this scenario, which flies to the best place. They aim to fly and verify their position over time, communicate with one another, and look for the best location at a global level, i.e., "Location Route Reorganization Node". The following algorithm can do this optimal routing.

Algorithm for Attacker Detection Automation of Bees Colony Optimization (ADABCP)

```
StartNode ← Mobile_node1
DestNode← StartNode(Mobile_Node1)
NodeNetworkKey← null
  while (start node ! == (Mobile_node 1))
ParticipateNode ← null
for(StartNode in NeighborNode)
if(not NodeNetwork(ParticipateNode , NeighbourNode))
NodeNetworkList ← ParticipateNode + NeighbourNode
          end
   end
DestNode ← FindDestNost(ParticipateNodeList)
                Mobile_Node1 ← DestNode(Key)
  for (NodeList←StartNode||NodeList←(InitialKey+RandomKey(NodeList)||
                                   FindDestNost← ParticipateNodeList(Mobile_Node1))
                if(NodeRoute(NodeList) > (StartNode||DestNode))
                NodeRoute← MinPath(StartNode, DestNode)
   End
                Step 1: Generate the size of nodes NS by Section 3.1
                Step 2: current evaluation times of the participating node, PEs = NS
                Step 3: While PEs ≤ MaxPEs // the maximum number of participating node evaluation
                do employed bees phase
                Step 4: for first scenario node = initial to size of nodes NS do
                Step 5: Generate a new route (Eulers formula is performed in Attacker detection
                automation) according to (Route Finding Manipulation (RFM));
                Step 6: Update new route based on Attacker detection automation allowing to (RFM);
                Step 7: if , set not been updated route = 0,
                                  PEs = PEs + 1;
                        else updated route i = updated route i + 1;
                end
                Step 8: do onlooker bees phase
                Step 9: for second scenario node = 1 to NS do
                Step 10: Choose a source node from the current employed bees phase
                Step 11: do step 6 to step 7
                Step 12: do Scout Bees phase
                Step 13: for final scenario node = 1 to NS do
                Step 14: if PEs > second scenario node,
                Step 15: replace NS with a new random node
                Step 16: if PEs > Max PEs,
                Step 17: output (MinPath)
                end
MinPath(Node) ← Route_Factor(NodeNetworkList)
   Route_Factor ← ThresholdValue (StartNode!=CA, DestNode|| NeighbourNode)
                for(Route_Factor ←StartNode!=CA &&StartNode;MaxPath(NodeList) ←
   DestNode||NeighbourNode; NodeList(DestNode +1),
   NodeList(NeighbourNode +1)
   MinPath(ListNode) ← Minpath(Route_Factor);
         while(Route_Factor(NodeList) > Network Size)
```

```
NodeRoute (ThresholdValue(StartNode!=CA, DestNode||NeighbourNode))
   MinPath←( ThresholdValue (StartNode||DestNeighbourNode))
MinRoutePath ← MinPath
      End    endend
  return (MinPath)
```

Pseudo code for proposed routing protocol:(rushing attack)

```
 Manage: Path Route Attacker
                Avail in Route
                Route Reorganization →Positive
Gives
Malicious Node : Positive
   do :
                pkt(≪Route Reorganization ||pkt send to location disclosure||traffic pattern||actual pattern≫) as
network node,
                            result value is Route Reorganization
   else:
                Route Organization (sent pkt 1||receive pkt1|| target paket1)
end :node recognize
do :            The same as another network
                Result value is Route organization verified by attacker node and infected
   malicious node
                While :Route organization (sent pkt 2||receive pkt 2|| target pkt2)
                End with (N Packets,t time )
Node: select → attacker→positive,
                Do: Route Reorganization
   Through node
                Calculate
                            Route Reorganization: attacker→Nill;
Find: Loss of packet (pattern lost)
   If: attack occurs
    (Route omitted) ==1;
   Else: find_location disclosure (individual node)
   Endf:
Manage:Path route attacker
                Avail in route
                            Route traffic→positive
                            Else
                            Route traffic→clear
Else: Path Route Attacker_node→response_time
```

The above algorithm presents a route organization and route reorganization based routing protocol for finding the rushing attack [25] [48] [49] [50]. After finding the MANET rushing attack, the path selection might be concluded based on the Swift Implicit Response Round Trip Time mechanism-based secure path selection [51]. After avoiding the rushing attacks, this scheme was applied to obtain an efficient communication route. This method checks whether the communicating node is active or inactive. If it is inactive, then such nodes cause the rushing attacks; hence attackers occur in the routing path [36] [52].

3.2. Swift Implicit Response Round Trip Time (SIRT) mechanism

This route organization and route reorganization based routing protocol is the imperfect packet broadcasting among the nodes in the transmitting environment [9] [42]. Because the attacker node suddenly switches over its functioning by decreasing the packet delivery ratio. In the proposed research, the transformation by Swift Implicit Response Round Trip Time (SIRT) mechanism is identified and rectified, and removed from the affected communication path. Using the SIRT mechanism scheme, the nodes allow the secure node to have a higher transmission rate.

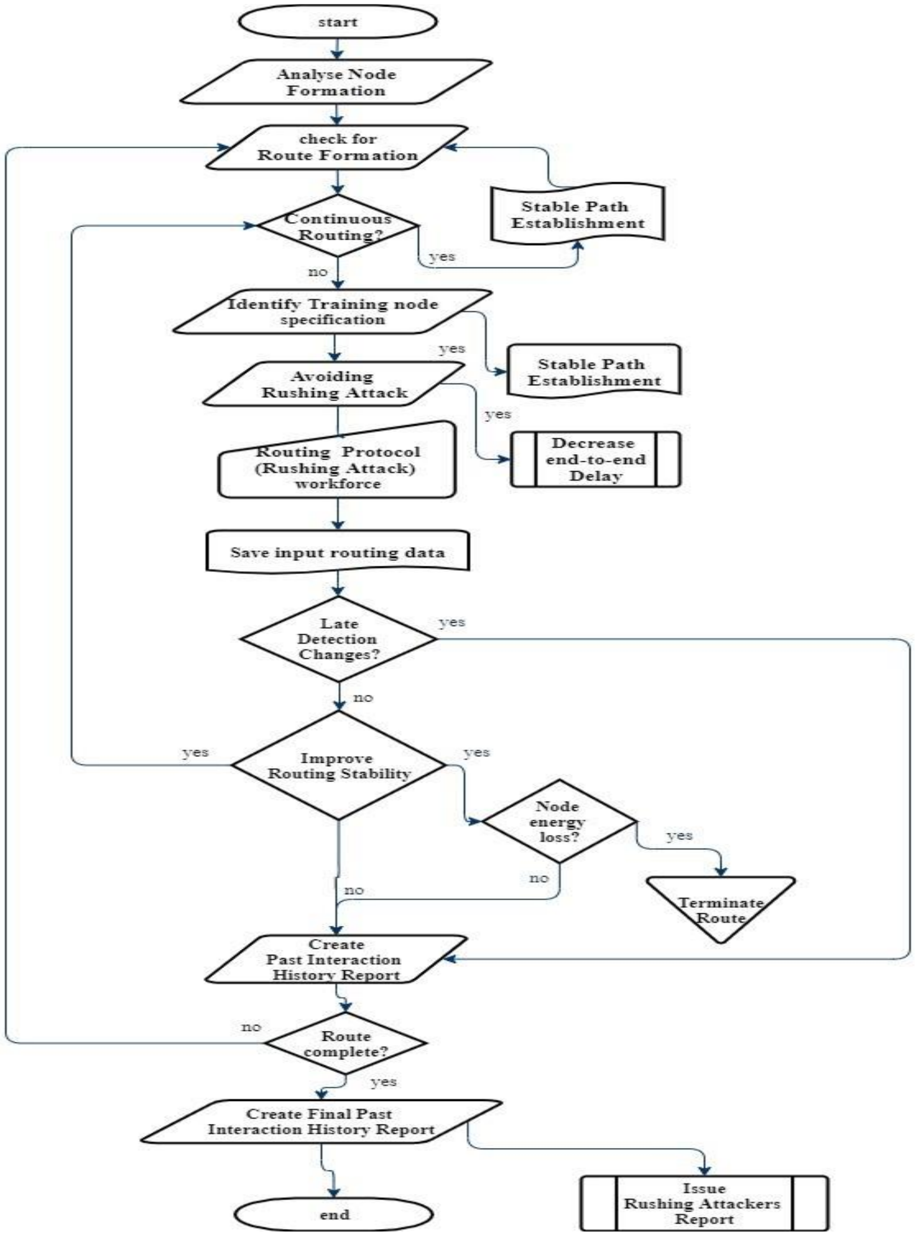

start
Analyse Node Formation
check for Route Formation
Stable Path Establishment
Continuous Routing?
yes
no
Identify Training node specification
yes
Stable Path Establishment
Avoiding Rushing Attack
yes
Decrease end-to-end Delay
Routing Protocol (Rushing Attack) workforce
Save input routing data
Late Detection Changes?
yes
no
yes
Improve Routing Stability
yes
Node energy loss?
yes
no
no
Terminate Route
Create Past Interaction History Report
no
Route complete?
yes
Create Final Past Interaction History Report
Issue Rushing Attackers Report
end

Figure 9. Flowchart of proposed MANET convergence scenario in the Swift Implicit Response Round Trip Time

Figure 9 shows the block diagram of the proposed "Swift Implicit Response Round Trip Time (SIRT) mechanism-based secure path selection scheme to choose the higher transmission rate for communication. This will be expressed by using the stable path establishment and continuous routing in the MANET network.

3.2.1. SIRT Mechanism

Swift Implicit Response Round Trip Time (SIRT) mechanism-based secure path selection scheme identifies attacker-free path with the unusual nodes delivery time. The algorithm for Attacker detection automation of Bees Colony Optimization (ADABCP) is used to monitor the node data stream status of every node in the routing path [33] [37]. This helps to increase the packet delivery ratio for the SIRT mechanism. To reduce the misbehavior in the attacker node transmission, every node must reduce the abnormal path detection with the nodes normal behavior. This helps to update the unstable route among communicating nodes through the routing path. SIRT Mechanism also provides constant security for packet transmission. This enhances packet delivery ratio, network lifetime, reduces routing overhead and packet latency. However, the proposed MANET convergence scenario in the Swift Implicit Response Round Trip Time has the following Timing Composition for Round Trip Time calculation.

A. Timing Composition of Round Trip Time Model

This section is used to calculate the round trip time of Participating Route Nodes (PNR). The context with the source node, the way in which the source node is evaluated for its response time, response time is also assessed by the time taken for their data exchange (including RREQ time /RREP time) interval based on the node response, i.e., time taken in each transaction. Similarly, the way destination node, i.e., receiver nodes, has a communication efficiency response time evaluation; the communication efficiency response time evaluations of a trusted node and attacker node are also evaluated for their network node size. Hence to calculate the communication efficiency response time assignment of source and destination:

For maximum communication response time efficiency of a trusted node,

$$A_e(n) = \left(\log \frac{1}{FT_{(Src,Revr)} - T_{min}}\right) * N_s \tag{2}$$

$A_e(n)$ is attacker response time efficiency of a node, T_{min} is minimum data communication rate, $FT_{(Src,Revr)}$ The fixed time interval for source and receiver nodes, $S_n$network node size.

For minimum communication response time efficiency of attacker node,

$$C_e(n) = \left(D_{max} - FT_{(Src,Revr)}\right)^{N_s} \tag{3}$$

$C_e(n)$ is communication response time efficiency of a node, D_{max} is maximum data communication rate, $FT_{(Src,Revr)}$ the fixed time interval for source and receiver nodes, N_s network node size.

$$FT_{(Src,Revr)} = \sum_{x=1}^{k} \left[\frac{PRN_{(Src,Revr)}}{K}\right] \tag{4}$$

$FT_{(Src,Revr)}$ is Fixed time interval between source and destination, k is the total number of nodes in the network, PRN is the Participating Route Nodes(PNR) between source and destination.

In such a case, the mobile nodes in a MANET do not update their position frequently. If the process needs to establish the connection node on a secure path, the route must be changed its path flow energetically to avoid the damage nodes (attacker) in the exact route. The routing is logically restored by the relay node, which is accountable for the attackers destruction. This rushing attacker destroys the process in which it affords closer to the target node in the routing path by using the "Use Best Approximation" process. Use best approximation that utilizes the Static route with continuous routing on the MANET [39].

3.2.2. Use Best Approximation

Whenever the route transmission is denied, the receiver node gets the packets from the sender repeatedly. To avoid that communication, the proposed static route with continuous routing is employed. These continuous routing packet delivery communications try to send a massive quantity of control packets to the destination. Due to the enormous packet on the static path, the traffic density is also increased. To avoid traffic occurrence on the network, the minimum packet latency is allowed for data transmission [53]. This minimum packet latency transmission ensures the unwanted excess data packet broadcasting in the MANET environment. This process supports reducing the data corruption and rushing attacks and also makes more packet latency.

The maximum secure route of the mobile nodes makes the easiest communication. If the $Stable_r$ is stable route, $Conti_r$ is continuous routing.$then\ O_n * R_n$ is route organization rate at reverse acknowledgment direction. Meanwhile $Stable_f$ is the stable route, $Conti_f$ is continuous routing at forwarding direction.

$$Conti_r = \sum_{n=NM1}^{MN17} \left[threshold_{count} |Stable_r| - \left[\max_{t=(node-1)} (threshold_{count}(O_n * R_n)) \right] \right] \tag{5}$$

$$Conti_f = \sum_{n=MN17}^{MN1} \left[threshold_{count} \left|Stable_f\right| - \left[\max_{t=(node-1)} (threshold_{count}(O_n * R_n)) \right] \right] \tag{6}$$

The above equations 5 and 6 indicate this route communication for continuous routing on the forward and the reverse (i.e., acknowledgment) directions. This proposed scheme monitors the constant routing path chosen concerning the time interval (t) throughout finding the path within the period of the projected path. Such a process is used to measure the distance between nodes in the routing path. The proposed $Conti_r$ removes the wrong data packets in a network. Therefore, based on threshold count, an alternative path is used to transfer the data between the nodes with stable value. This process flow avoids the attacker data packets for broadcasting on a stable path. While the average data transfer rate value of a node is minimized for each node fixed value, it reduces the proposed re-route damage and increases the communication [54]. The reserve among the various nodes is improved based on node position by equation 7.

$$E_n = residual_{energy} - \max_{t=(Stable_{node})} \left[consumed_{energy} \right] \tag{7}$$

The proposed "Use Best Approximation" scheme is used to detect the attacker route with the exact maximum damage route. In-between this damage route, all nodes are identified as the intermediate nodes with minimum TTL value in the MANET network. This intermediate node is recognized as the rushing attackers nodes within the node frequency coverage range [44] [55]. This marching scheme is addressed as the SIRT mechanism.

The details regarding the malicious attacker node are broadcasted within the network or even the destination node. To avoid these malicious activities, this article proposes the Static route with continuous routing. It also compares every nodes characteristics in a network to measure the abnormal behavior; if it is high, then the node becomes malicious; otherwise, it is considered an accomplished node. The destination node contains the details of the link establishment for each destination node. Network knowledge of each link with the present quality level helps distinguish malicious nodes and each routing node in the network environment [16]. In this era, some nodes get removed from the routing path based on packet transmission speed and routing speed-accuracy rate, and the quality of service paths provides help to any failure node. The destination node contains complete details to start a pattern recognized to the link with low packet latency without the malicious nodes [9] [20] [41]. The target node organizes this information through dual procedure packet sharing with the remaining nodes through the routing path intermediate nodes. It guarantees more probability and minimum traffic, and those details of the network state are contained each to restore previous routes and start initially by excluding the rushing attackers nodes. The malicious nodes can support the restriction of data to the routing path, which is a more stable one than the remaining paths, and it minimizes the packet transmission traffic, and hence the output shows improvement in the network lifespan.

This research aims to aid data transmission against rushing flagging protocol at the Hybrid Random Late Detection (HRLD) to reduce the rushing attack effectiveness and increase the data delivery time interval [56]. This scheme ensures data transmission on a secure path against the rushing flagging protocol. These HRLD models are developed for effective data transmission without any attacks [25] [26] [36].

3.3. Hybrid Random Late Detection (HRLD)

This HRLD scheme ensures secure data transmission using "Use Best Approximation", which helps route problem observation. This proposed process meets an efficient transmission in the infrastructure-less network. Moreover, attacker detection automation is used to locate the appropriate attackers. The proposed swift implicit response overcomes the congestion communication on MANET routing. The initial matching made with the other nodes is used to reduce an attacker with the help of the "SIRT" mechanism.

The confined route is useful in finding an optimal solution for dead node reduction and active links node boost-up by using interaction history in a well-organized manner [5] [9] [57]. The working of dead node reduction and active link nodes boost-up depends on the time interval assignment. In this manner, the time interval will be assigned to each node for responding to the sender node by using a key assignment. Within this designated time interval, the transmitted node will send the reply messages to the transmitting node for proving node confirmation. This confirmation helps to reduce the end-to-end delay for one-way communication. To decrease performance degradation, efficient routing is maintained by route interaction (shown in table 2, table 3, and table 4). This routing scheme helps to find the optimal routing securely and intelligently. Finally, node ranking is taken from the past interaction history to every transmission. In addition to that, the Attacker detection automation is run parallel to update the dead nodes and active links [43]. These updates are applied to past interaction history. The cyclic processes of node ranking express the continuous monitoring system of infrastructure-less network, which produces the enhanced alternative for existing strategies. On this continuing cyclic process, the usual routing path on the mobile ad hoc networks is not a confirmed path for the entire timing of completion of data transmission [53] [56].

However, to maintain the data transmission for successful communication, normally MANET introduces automatic route rearrangement in unexpected mobile nodes; For this data transmission ability without conveyed easy roaming around the environment, past interaction history, attacker intrusion, etc., there are two general requirements [56].

Firstly, legally developed algorithms are needed to construct successful data transmission on mobile ad hoc networks. This research designed the node flexibility, mobility, and nodes energy validity based on MANET data transmission [31] [15]. The proposed system accomplishes the route observation in mobile ad hoc networks. The proposed system working is based on the late detection procedural aspect for physically constructed mobility networks, intellectually designed hardware sensitivity, and legally developed data forwarding algorithms.

3.3.1. Mechanism against the late detection

The routing protocol of mobile nodes algorithmically mentions late detection. Commonly in the critical situation, mobile nodes share the critical messages over the network by the data-transfer application by using the end-to-end communication [28] [30] [32]. From this consideration, this research takes the survey based on the beneficial two side communication such as node to node communication and node to controller communication. These two communications have their challenges in providing reliable and secure data transfer between the node to node communication or node to controller communication.

This research article gives the solution to the data transfer application concerning the routing protocol of mobile nodes. The novel protocol design called Hybrid Random Late Detection (HRLD) routing protocol is one of the proposed works to speed up the data transmission; this protocol must share the trusted data to the confident end user [20] [42] [58]. This data transfer mechanism keeps the reliable and security measures of the whole participating MANET environment system [24] [42] [49].

3.3.2. Hybrid Random Late Detection (HRLD) routing protocol

This research defines the Hybrid Random Late Detection (HRLD) routing protocol by the following two assumptions. An HRLD routing protocol is mainly proposed for path optimization on the MANET [33] [34].

i. Past Interaction History with Transmission data

The Hybrid Random Late Detection (HRLD) routing protocol uses the Past Interaction History (PIH) for updating the packet delivery on node interaction [23] [50] [29]. Past interaction history (PIH) has (Table 5) quality factors such as source node location, receiver node location, time taken to transmit packets, minimum route path, and trust values. This PIH is exposed below table 6 by the terms like network id, node pattern, trust value, node lifetime, efficiency, and bandwidth [58].

Table 5. Past interaction history for trust values

Possible_ Route	Network ID	Host ID	Mobile_Network_Recognition			Bytes per Symbol information (BpS)	Route Perceptual_structure	Trust_Value			
			Network_Src_address	Network_Dest_address	Network_Mask			Sender_node	Time taken for avg execution	Receiver _ Node	Time taken for avg execution
MN1→ MN2	192.168.0.X	192.168.0.1↔ 192.168.0.2	192.168.0.1	192.168.0.2	255.255.255.248	54	trusted	1	10.35	1	9.86
MN2→ MN5	192.168.0.X	192.168.0.2↔ 192.168.0.5	192.168.0.2	192.168.0.2↔ 192.168.0.5	255.255.255.248	68	trusted	1	10.35	1	8.65
MN5→ MN10	192.168.0.X	192.168.0.5↔ 192.168.0.10	192.168.0.5	192.168.0.5↔ 192.168.0.12	255.255.255.248	50	trusted	1	10.35	1	9.33
MN10→ MN9	192.168.0.X	192.168.0.9↔ 192.168.0.10	192.168.0.9	192.168.0.9↔ 192.168.0.12	255.255.255.248	90	trusted	-1	10.35	0	4.65
MN1→ MN4	192.168.0.X	192.168.0.1↔ 192.168.0.4	192.168.0.1	192.168.0.1↔ 192.168.0.6	255.255.255.252	64	trusted	1	10.35	1	9.33
MN4 → MN9	192.168.0.X	192.168.0.4↔ 192.168.0.9	192.168.0.4	192.168.0.4↔ 192.168.0.11	255.255.255.252	58	trusted	1	10.35	1	9.85
MN1→ MN4	192.168.0.X	192.168.0.1↔ 192.168.0.4	192.168.0.1	192.168.0.1↔ 192.168.0.6	255.255.255.252	94	Untrusted	0	10.35	1	7.66
MN4→ MN8	192.168.0.X	192.168.0.4↔ 192.168.0.8	192.168.0.4	192.168.0.4↔ 192.168.0.10	255.255.255.252	55	trusted	1	10.35	1	9.89

Table 6. Past interaction history for final route destination transmission data history

Possible_Route	*Network ID*	*Host ID*	*Packet Life time(ms)*		*AvgNetwork Life time(ms)*	*Efficiency*	**Energy consumption rate**	*Node_final_FTI_attain*	*final route_distination*
			Sender_node to Receiver_ Node	*Receiver_ Node to Sender_node*					
MN1→ MN2	192.168.0.X	192.168.0.1↔192.168.0.2	2.4970	2.4137	30.2467	Higher	49.6443	79.8915	Minimum
MN2→ MN5	192.168.0.X	192.168.0.2↔192.168.0.5	2.1176	2.2829	33.3627	Average	41.6648	75.0276	Minimum
MN5→ MN10	192.168.0.X	192.168.0.5↔192.168.0.10	2.5744	2.4440	30.0486	Higher	49.4479	79.4965	Minimum
MN10→ MN9	192.168.0.X	192.168.0.9↔192.168.0.10	-0.333	2.0331	153.224	Minimum	6.00413	159.228	Maximum
MN1→ MN4	192.168.0.X	192.168.0.1↔192.168.0.4	2.2344	2.3222	32.1736	Average	44.7261	76.8997	Minimum
MN4 → MN9	192.168.0.X	192.168.0.4↔192.168.0.9	2.3931	2.3761	30.8660	Higher	48.1734	79.0395	Minimum
MN1→ MN4	192.168.0.X	192.168.0.1↔192.168.0.4	0.7663	2.1222	49.1705	Lower	24.1885	73.3590	Minimum
MN4→ MN8	192.168.0.X	192.168.0.4↔192.168.0.8	2.4722	2.4045	30.3781	Higher	49.3661	79.7443	Minimum

The network lifetime is determined by the ratio of confirmed acknowledgment to the whole number of possible node transmissions on reaching the prescribed Trust Values (TV). In this research, the time is fixed on the first packet transmission. At the end of the session, the consolidated time interval is calculated. This time length is compared to the individual packet transmission and acknowledgment time interval. At each time, the interval time is noted and recorded to the past interaction history. In this instant, the time consumption for the current packet is calculated concerning the amount of energy spent on the REQ/REP process [8] [15] [41]. This process is expressed as the following process,

The Network Lifetime (NLT) of Packet (Pkt) at nth node is carried out by following equation 8,

$$\mathrm{NLT}(\mathrm{S} \leftrightarrow \mathrm{D}) = \frac{\mathrm{Energy}_{\mathrm{1st\ pkt\ tran(t)}} - (\mathrm{Energy}_{\mathrm{nth\ pkt\ tran(t)}})}{\mathrm{Energy}_{\mathrm{total\ pkt\ tran(t)}} - (\mathrm{Energy}_{\mathrm{nth\ pkt\ tran(t)}})} \tag{8}$$

Meanwhile, the Bytes per Symbol information(BpS) is calculated based on the data transfer rates. The two parameters that access the BpS are connection strength and packet speeds. If the participating mobile node quantity is increased, the packet delivery speed also is dramatically increased. In the MANET transmission, the Bytes per Symbol information(BpS) calculation is in symbols per second (i.e., Data rate in BpS × 204) / (188 × BpS). To convince this byte per Symbol information(BpS), this research can be used in the Hybrid Random Late Detection (HRLD) routing protocol [59], which is constituted based on the past interaction history with route interaction from network id 0.0.0.1. to an end-user node [30] [32].

While a packets transmission between the origin of the Hybrid Random Late Detection (HRLD) routing protocol and end-user occurs, the proactive protocol gets activated for speeding up the packet delivery by using inspected nodes and its route at the same time. This proactive protocol manages the immediate packet delivery to nearby nodes without any rush and improves the end-to-end delay time called random late detection. To carry the packet without rush, broadcasting packets using random exact minimal path rectification proficiency is utilized. In MANET, the nearby nodes will change their location due to the node movements aspect. At that time, the routes availability and destination node are switched in the random detection zone.

This same procedure is extended to another group to enhance routing protocol on each successive zone [42]. These techniques help to find transmission acceleration of the network irrespective of whether the node transmits the data or not. The transmission speed is found based on the following node transmission accelerate (shown in table.7). Node transmission range patterns are formed by increasing the packet delivery ratio of the individual node and reduce packet delay on selected routes from the past interaction history [55] [60]. Once a nodes route is established without any intrusion, the destination node path will be stored in the node transmission that accelerates the table using the proactive protocol. This sequential transmission acceleration and address are always used to deliver the packet for the next sequential node [43].

Table 7. Node transmission accelerate table

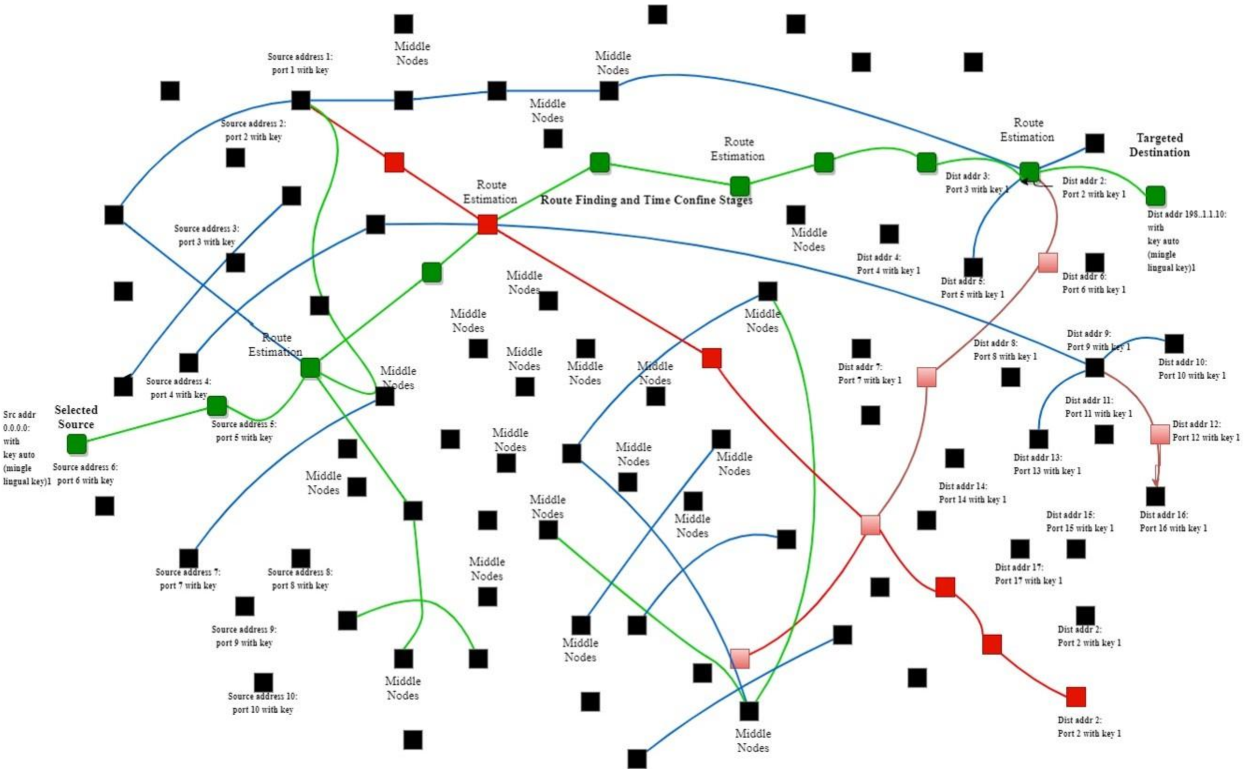
Network Id		Next Hop	Current Node To Gateway	Cost	No of Nodes presented	No.of. Route on The Gateway
Network Destination	**Net Mask**	**Gateway**	**Interface**	**Metric**		
0.0.0.1	0.0.0.10	192.130.10.10	192.130.10.0	n	1 to N(n-1)*n	R1
125.0.0.0	232.0.0.10	197.1.1.10	197.120.10.10	n	1 to N(n-1)*n	R2
..	..	..	..	..	..	..
..	..	..	..	..	..	..
198.162.0.1	255.255.255.255	198.162.0.100	198.162.0.142	n	1 to N(n-1)*n	Rr

The intrusion with respect to the packet transmission is observed using the node transmission acceleration table switching technique. Here, the packet sent over to the neighbor group or the nearby controller would be based on the key assignment, past interaction. [5] [39]. After forming the node transmission accelerate table, the MANET ratio range rate would be activated based on data transmission, networking, and protocols. The data transmission protocols are derived from the following algorithms and used to activate the MANET ratio range.

The proposed data transmission acceleration protocols are also used to perform efficient data transmission against the routing protocol [42] [32]. This protocol has found the nth destination address concerning the MANET completion. The input ratio range is assured based on the MANET environments current scenario for the bandwidth modulation.

ii. Route Finding and Time Confine

This route finding and time confine are taking the communication between the sender and the receiver for finding the exact route between the source and destination by the get route (). The two aspects are considered for forming sender-receiver path manipulation [61]. Firstly, the mobile node is checked based on the node lifetime and node energy. These mobile node platforms have a continuous check on the route based on the switch inputs over broadcasting the packet signal to the nearby nodes shown in Figure 10.



Middle Nodes
Source address 1: port 1 with key
Middle Nodes
Middle Nodes
Source address 2: port 2 with key
Route Estimation
Route Finding and Time Confine Stages
Route Estimation
Route Estimation
Targeted Destination
Dist addr 3: Port 3 with key 1
Dist addr 2: Port 2 with key 1
Dist addr 198..1.1.10: with key auto (mingle lingual key)1
Source address 3: port 3 with key
Middle Nodes
Dist addr 4: Port 4 with key 1
Dist addr 5: Port 5 with key 1
Dist addr 6: Port 6 with key 1
Middle Nodes
Middle Nodes
Middle Nodes
Route Estimation
Middle Nodes
Middle Nodes
Middle Nodes
Middle Nodes
Dist addr 7: Port 7 with key 1
Dist addr 8: Port 8 with key 1
Dist addr 9: Port 9 with key 1
Dist addr 10: Port 10 with key 1
Source address 4: port 4 with key
Src addr 0.0.0.0: with key auto (mingle lingual key)1
Selected Source
Source address 5: port 5 with key
Source address 6: port 6 with key
Middle Nodes
Middle Nodes
Middle Nodes
Middle Nodes
Dist addr 11: Port 11 with key 1
Dist addr 12: Port 12 with key 1
Dist addr 13: Port 13 with key 1
Dist addr 14: Port 14 with key 1
Middle Nodes
Middle Nodes
Dist addr 15: Port 15 with key 1
Dist addr 16: Port 16 with key 1
Source address 7: port 7 with key
Source address 8: port 8 with key
Middle Nodes
Dist addr 17: Port 17 with key 1
Source address 9: port 9 with key
Middle Nodes
Dist addr 2: Port 2 with key 1
Source address 10: port 10 with key
Middle Nodes
Middle Nodes
Dist addr 2: Port 2 with key 1

Figure 10. Conceptual framework and proposed rushing attacker route structure, functionalities and processing model packet data transmission with route finding and time confine

For a particular stage, the active node takes minimal time to get the acknowledgment. In this period, the active mobile node becomes a lesser route for nearby nodes, and this is illustrated in the following switch case inputs. To follow these route estimation criteria, the route finding and time confine are established.

iii. Sender-Receiver Address Status

This sender-receiver destination address status has taken the communication over the radio range, and the data rate of SDN for finding the exact route between the sender and receiver by using the command include find (). The next possible nearby node is summarized concerning the throughput of each ratio range and each transactions data rate. The two conditions are considered for forming the destination of particular data transmission.

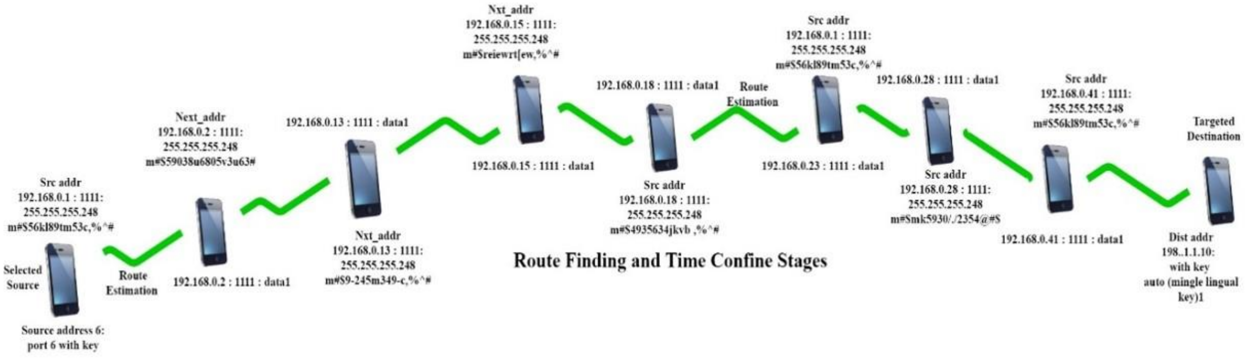


Figure 11. Sender-receiver destination addresses status

The mobile node is checked based on the ratio range and data rate. These mobile platforms have a continuous check on the ratio range against the throughput over the packet signal broadcasting to the nearby nodes. The active node throughput comparison returns to the final possible designation node with minimal time for getting acknowledgment. To follow the criteria of the command include find() destination, the receiver path has been manipulated with the help of route estimation on MANET Platforms as shown in figure 11. On the other hand, node transmission acceleration is returned to the secured and shortest path based on the source and receiver node trust value.

3.3.3. Route Finding Manipulation (RFM)

Does routing or data communication assisting improve MANET communication with the environment, or is MANET making the route determination into offering "RFM?". This research is committed to this demand with "Hybrid Random Late Detection (HRLD)". Route Finding Manipulation (RFM) is elementary support for the sender and receiver and also the middle node for data communication [62]. Route finding manipulation supports precisely the best route between the sender and receiver and considers data communication significance. It is formed as in the below table 8.

Table 8. Utility matrix of Route Finding Manipulation (RFM) with route nodes stages

Mobile Node MN_p	Node 1	Node 2	Node 4	Node 5	Node 8	….	Node MN_D-1	Node MN_D
Node 1	Node1				…	….	…	
Node 2	❶	Node2			…	….	…	
Node 4		❷	Node4			❸	❹	
Node 5				Node5		❺	…	
…	…	…	…	…		❻	❼	
….	….	….	….	….	….		❽	…
Node MN_S-1	…	…	…	…	…		❾	Node MN_D-1 ●MN_S-1
Node MN_S	…	…	…	…	…	…	…	Node MN_S●MN_D

Above table 8 considers the node name with the participating mobile nodes.

- It uses the sender/receiver nodes for an individual transaction
- Sender/receiver nodes help to find the nearby nodes for improving route efficiency

Depending on the above constraints, route finding manipulation grants the MANET internal representation as Sender, receiver, and intruder.

The following case study was applied to the route manipulation matrix; the individual condition that meets its queries concerning the route-finding manipulation is directed in Table 9.

Table 9. Source, receiver and intruder determination

Source, Receiver and Intruder Determination	MANET Internal Representation	Is uses the Sender/Receiver for individual transaction	Is Sender/Receiver help to find the nearby nodes for improve route efficiency
Case 1: Source Determination	***Sender***	Yes	Yes
	Receiver	No	Yes
	Intruder	No	No
Case 2: Receiver Determination	***Sender***	No	No
	Receiver	Yes	Yes
	Intruder	Yes	No
Case 3: Intruder Determination	***Sender***	No	No
	Receiver	Yes	No
	Intruder	No	Yes

- Is the sender used for the individual transaction: Yes
- Is sender/receiver helpful to find the nearby nodes for improving route efficiency: Yes

From this Case 1: The Sender generally knows that the sender/receiver for individual transactions uses the nearby nodes successful finding for improving route efficiency. But in the case of the receiver, the receiver knows about the sender key values alone. This helps to fine-tune the route efficiency. Likewise, the intruder will offer route proficiency for the route availability [63].

- Is the receiver used for the individual transaction: Yes
- Is sender/receiver helpful to find the nearby nodes for improving route efficiency: Yes

From this case 2: The receiver usually knows that the nearby nodes for individual transactions use the destination nodes successful finding for improving route efficiency. But in the sender's case, the receiver does not know about the source sender, but it knows about the sender's key values. This helps to fine-tune the route efficiency concerning the receiver. Likewise, the intruder will offer route proficiency concerning route availability [63]. The intruder is available in the sender/receiver nearby nodes determination on the data communication process. To overcome this intruder on the destination determination, MANET will need to improve the security enhancement in the key distribution [2] [11]. This conclusion is enhanced in the coming circumstances. In a particular route, to enhance the initial packet distribution ($\mathrm{MN_p}$) from the source to nearby nodes, Eulers formula can be used to make the manipulation on the destination determination. The participation nodes ($\mathrm{MN_S}$) are considered as the till end nodes ($\mathrm{MN_D}$) concerning the throughput ($\hat{\mathrm{r}}$). The individual nearby nodes ($\mathrm{MN_{Near}}$) are determined by the following Eulers formula by equation 9 to 14,

$$MN_{p_{total}} = e^{-\hat{r}\gamma} \sum_{MN_S=MN_S-1}^{MN_D} e^{-\hat{r}2\pi \frac{MN_{Near_{MN_S}}}{\chi}} \tag{9}$$

From the first refinement, Eulers formula can be applied to the two nearby nodes such as (node 1 – node 2). This is described in the following illustration. Here the initial node throughput ($\hat{\mathrm{r}}$) becomes null. i.e., (0) and is applied in equation 9. For individual node determination,

$$\mathrm{MN_{p_{total}}} = \sum_{\mathrm{MN_S-1}}^{\mathrm{MN_D}} \mathrm{e}^{-\hat{\mathrm{r}}2\pi \frac{\mathrm{MN_{Near_{MN_S}}}}{\chi}} \tag{10}$$

In this stage, Eulers formula is applied to the whole network; hence the corresponding route node is calculated concerning the packet distribution ($\mathrm{MN_p}$)

$$\mathrm{MN_p} = \mathrm{e}^{-\hat{\mathrm{r}}2\pi \frac{\mathrm{MN_{Near_{MN_S}}}}{\chi}} \tag{11}$$

The enhancement bandwidth (χ) and node speed ($\dot{s}$) consolidate the final distribution packet with respect to the data rate (δ). This illustration produces the individual disclosure of the correct nearby nodes on each participant (MN_p).

$$MN_p = e^{-\hat{r}2\pi\frac{\dot{s}T}{\chi}} \tag{12}$$

The above individual discloses the correct nearby nodes on each participant (MN_p) and it is extended till the final node to check their availability based on the secret authenticated key, and this distribution is clustered in the following statement.

$$MN_p = e^{-\hat{r}2\pi fT} \tag{13}$$

Finally, the Route Finding manipulation is formed based on equation 13 for each node, which tabulated with respect to the Route Finding Manipulation

$$MN_p = e^{-\hat{r}\delta T} \tag{14}$$

- Is the intruder used for the individual transaction? Yes
- Is proposed protocol helpful to locate the attacker nodes for cut down route efficiency? Yes

From this case 3: In intruder determination, the sender could not know about the intruder. Meanwhile, the receiver also could not know about the nearby nodes as an intruder for individual transactions uses the delimiting of the nearby nodes for improving route efficiency on both sender and receiver nodes. In the case of an intruder, the receiver knows about the senders key values. This helps to decrease the route efficiency. The intruder does not know about the path history, which helps prevent the authentication of the key. Hence, the intruder has become null, and the route will offer route proficiency for the route availability [63].

3.3.4. Hybrid Random Late Detection (HRLD) routing algorithm

```
Input: Ratio Range, Data Rate, Bandwidth Modulation, Mobile Platform, throughput, switch inputs,
MANET completion (C)
Output: Efficient Data Transmission
C = getRoute (Sender node communication, Receiver node communication)
Process: by default: Mobile Platform ← Null connection
MANET Environment || operating system (starting position(C))
route (r) = [Null connection] ↔ switch inputs (Open)
While (Mobile Platform active node <switch inputs (route (r)))
For Route Estimation in route (r) do
Route_Estimation.deductSourceNode(MANET completion (C))
throughput= []
While (possible_Near_Node! = End position(C))
If (Sender node communication == ProValve(throughput))
throughput = ratio of favourable cases(C)
Else
Ratio Range = getPossiblity(Bandwidth Modulation)
    Or else
Data Rate = get Bandwidth Modulation (Ratio Range (C))
End
Include find:next_possible_Near_Node = throughput (Ratio Range|| Data Rate)
If (next_possible_Near_Node∀throughput = [])
nextNode = Call Include find ()
Else
possible_Near_Node = End position(C)
If (Receiver node communication≠ ProValve(throughput))
throughput = Acknowledgement probability(getRoute)
Else
find:next_possible_Near_Node ≠ throughput (Ratio Range|| Data Rate)
If (next_possible_Near_Node∩throughput = [])
nextNode = destination node ()
nextNode.append(destination node ())
```

```
End End
Route.append((destination node ()))
End
nextNode ++
End
return efficient data transmission
```

The above algorithm discusses the sender-receiver destination addresses using MANET routing protocols concerning the path nodes. The mobile nodes in a MANET do not update their positions frequently [4] [24] [15]. If the process needs to establish the connection node on a secure path, the route must change its path flow energetically to avoid the damage of nodes (rushing attacker) in the exact route. The routing is logically restored by the relay node, which is accountable for the attackers history. This rushing attack destroys the process that affords closer to the target node in the routing path. Whenever the route packet transmission is denied, the receiver node gets the packets from the sender repeatedly. To avoid that communication, the proposed Hybrid Random Late Detection (HRLD) routing algorithm is employed. These continuous routing packet delivery communications try to send an enormous quantity of control packets to the destination. Due to the massive packet on the static path, the traffic rush also is increased. To avoid the rush occurrence on the network, the minimum packet latency is allowed for data transmission. This minimum packet latency transmission ensures the unwanted excess data packet broadcasting in the MANET environment. This process supports reducing the data corruption and rushing attack and also makes more packet latency [25] [26] [64].

The maximum secure route of the mobile nodes ensures the easiest communication if the $\mathrm{S_r}$ is a stable route, $\mathrm{C_r}$ is rushing routing.$\mathrm{T_n} * \mathrm{E_n}$ participating node ($\mathrm{MN_p}$) route and rate (equation 15).

$$\mathrm{C_r} = \sum_{\mathrm{MN_S}=\mathrm{MN_1}}^{\mathrm{MN_D}} \left[\mathrm{threshold_{count}}|\mathrm{S_r}| - \left[\max_{\mathrm{t=(node-1)}}(\mathrm{threshold_{count}}(\mathrm{T_n} * \mathrm{E_n}))\right]\right] \tag{15}$$

The above formula indicates this route communication for continuous routing. This proposed scheme monitors the constant routing path chosen concerning the time interval (t) throughout the path-finding within the period of the projected path. Such a process is used to measure the distance between nodes in the routing path. The proposed $\mathrm{C_r}$ is to remove the wrong data packets in the network. Therefore, based on threshold count, an alternative path is used to transfer the data between the nodes with a stable value. This process flow avoids the attacker's data packets from broadcasting on a stable path. While the nodes average data transfer rate value is minimized to each node fixed value, it reduces the proposed re-route damage and increases communication. For this reason, the reserve among the various nodes is improved based on node position

$$\mathrm{E_n} = \mathrm{residual_{energy}} - \max_{\mathrm{t=(Stable_{node})}}\left[\mathrm{consumed_{energy}}\right] \tag{16}$$

The proposed scheme is used to detect the attacker route with the exact maximum damage route (equation 16). In-between this damage route, all nodes are identified as the intermediate node with a minimum TTL value in the MANET network. This intermediate node is recognized as the malicious attackers nodes within the node frequency coverage range. The details regarding the malicious attackers node are broadcast within the network or even the destination node. To avoid these malicious activities, this article proposes the Static route with continuous routing. It also compares each node characteristics in the network to measure the abnormal behavior, and if it is high, it is malicious. Otherwise, it is an efficient node. The destination node contains the details of the link establishment for each destination node. Network knowledge of each link with the present quality level helps distinguish malicious nodes and each routing node in the network environment [16]. In this era, some nodes are removed from the routing path based on packet transmission speed and routing speed-accuracy rate, and the quality of service paths helps reduce failure nodes. The destination node contains complete details to start a pattern recognized with the link with low packet latency without the malicious nodes. The target node organizes this information through dual procedure packet sharing with the remaining nodes through the routing path intermediate nodes. With the minimum traffic, it is guaranteed that those details of the network state are contained to restore previous routes and start initially by exclusive of the rushing attacker nodes. The malicious nodes can support the restriction of data to the routing path, which is a more stable one compared with the remaining paths, and it minimizes the packet transmission traffic so that the output shows improvement in the network lifespan [9] [43].

4. Performance Analysis and Result Discussion

In the computer simulation, specified execution factors that define a system and determine their performances are shown in the X graph in ns2.34 [65]. The performance is measured through throughput, packet delivery ratio, end-to-end delay, communication overhead, network lifetime, and energy consumption. The Routing Protocols Communication for Rushing Attacker Detection and routing are modeled with the Network Simulator tool (NS2.34). In attacker detection automation simulation, 250 sensor nodes spread and processed with 0.5x102 ms simulation time with traffic source time steps to 2400ms. In that complete configuration, the nodes are distributed randomly. In this random manner, the nodes are propagated over the radio range with radio propagation model X (mm) at 0.025ms by 150m - 200m, Y (mm) at 0.025ms by 200m - 250m and propagation of Z (mm) at 0.025ms by 150m - 250m. It has a different transmitting range that varies from 150 to 250 meters. Routing protocol provides a constant speed of packet transmission in the network to limit the traffic rate. Table 10 shows the approximation simulation setup. i.e.,

Table 10. Simulation Parameters

Parameters	Denounce	Ranges/ Values
No. of Nodes	Active nodes	35
	Participated nodes	250
Channel	Channel/Wireless Channel	Channel/Wireless Channel
Area Size	X Position	0
	Width X (Half Way)	3
	Y Position	2.5
	Width Y (half Way)	3
Antenna	Antenna/OmniAntenna	Antenna/OmniAntenna
MAC type	802.11g	Mac/802_11
Radio Range with Radio propagation model	Propagation: RR X (mm) @0.025ms	150 m-200 m
	Propagation: RR Y (mm) @0.025ms	200 m-250 m
	Propagation: RR Z (mm) @0.025ms	150 m-250 m
Simulation Time	0.5x102 milliseconds	0.5x102ms
Traffic Source	Set Time Steps to 2400ms	2400ms
Packet Size	24pkts/msminimum packet inHRLD	2400pkts/data, max packet inHRLD
network interface type	Phy/WirelessPhy	WirelessPhysical layer
Interface Queue	DropTail (for RREQ)	PriQueue (RREP)
Mobility Model	Random	SIRT-ADABCP-HRLD
Protocol	HRLDRouting Protocol	

The comparison was conducted in terms of attackers, execution time, mobility count, network size, node speed, packet size and pause time.

i. **End to End Delay:** Figures 12 to 16 and Table 11 demonstrate end-to-end delay, calculated by the quantity of time taken for packet transmission from sender to receiver. The past interaction history table stores all node connectivity. In Proposed “Optimal Aggregation of Attacker detection automation of

Bees Colony Optimization" method [4], packet latency is cut down and compared to existent method ESCT - Cai et al. (2018), ENM-LAC - Liu et al. (2019), and ZRDM-LFPM - Khudayer et al. (2020).

$$\text{End to End Delay} = \text{End Time} - \text{Start Time} * 100$$

Table 11. Performance result analysis of end-to-end delay

Mobility nodes count	End to End Delay (ms)				Average End to End Delay (%)
Delay versus Mobility	**ESCT - Cai et al. (2018),**	**ENM-LAC-Liu et al. (2019)**	**ZRDM-LFPM - Khudayer et al. (2020)**	**SIRT – ADABCP-HRLD**	**Inference for Existing system with Proposed System**
20.0000	26.75	19.25	15.75	8.25	59.9190% decrease
30.0000	27.25	20.50	16.25	8.75	58.9844% decrease
40.0000	27.75	21.50	16.50	9.00	58.9354% decrease
50.0000	28.75	21.75	17.75	10.75	52.7473% decrease
60.0000	29.75	22.25	18.75	11.00	53.3569% decrease
70.0000	30.25	22.75	19.00	11.75	51.0417% decrease
80.0000	31.00	23.25	19.25	12.00	51.0204% decrease
90.0000	31.50	24.75	20.00	12.75	49.8361% decrease
100.000	32.00	25.00	21.00	13.00	50.0000% decrease

This mechanism considers mobility variation by indicating the lower mobility over the network with the higher nodes, which examine against the accuracy, quality, and node lifetime. This graph Contributes to reducing the End to End Delay by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. This improves the efficiency of assigning sources in the routing process. Here there are 100 samplings to discover the amount of packet to be delivered, and this research implemented Hybrid Random Late Detection (HRLD) approach in the MANET environment and evaluated it by some well-known attacker [Kleineberg et al., (2017)].

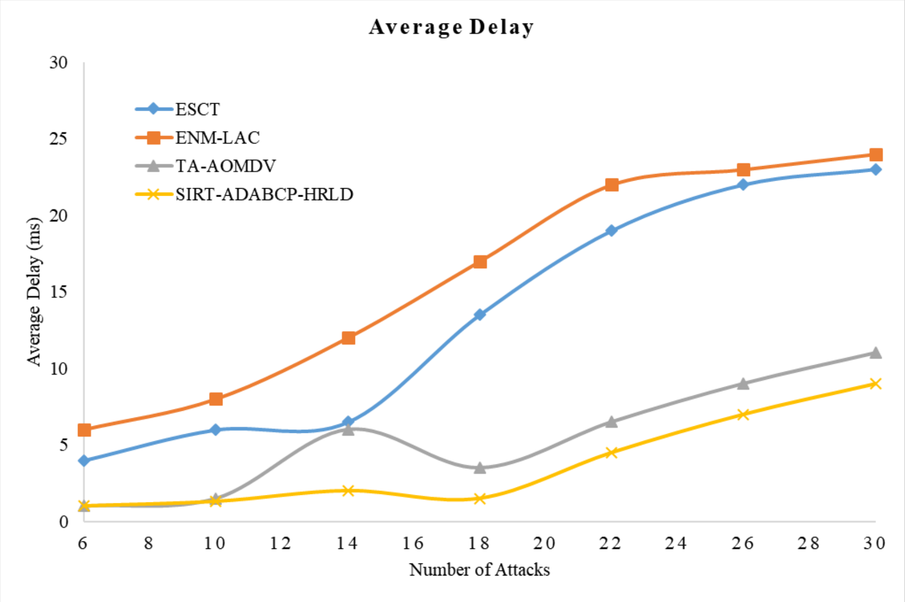


Figure 12. Graph for an end-to-end delay Vs. number of attackers

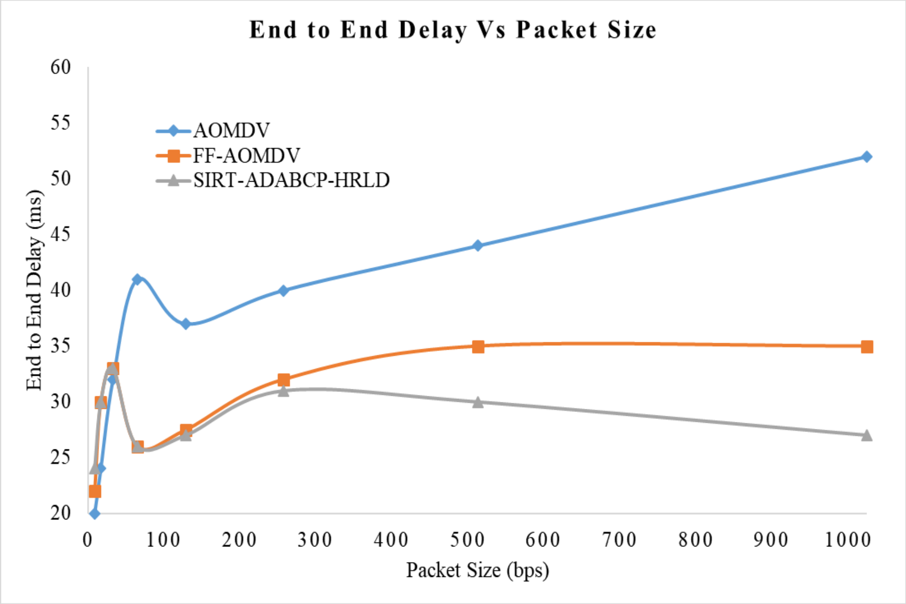


Figure 13. Graph for End to End Delay Vs. Packet Size

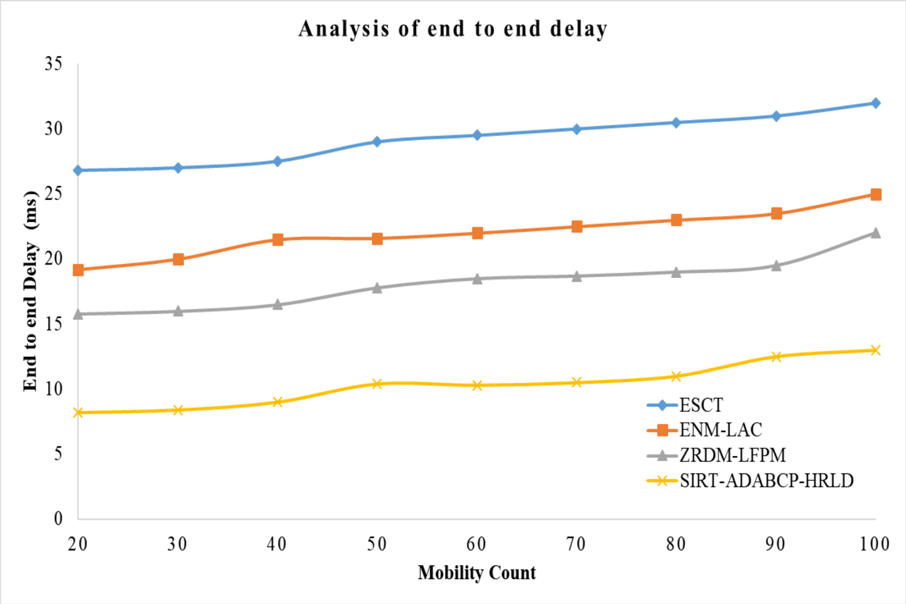


Figure 14. Graph for an end-to-end delay Vs. mobility count

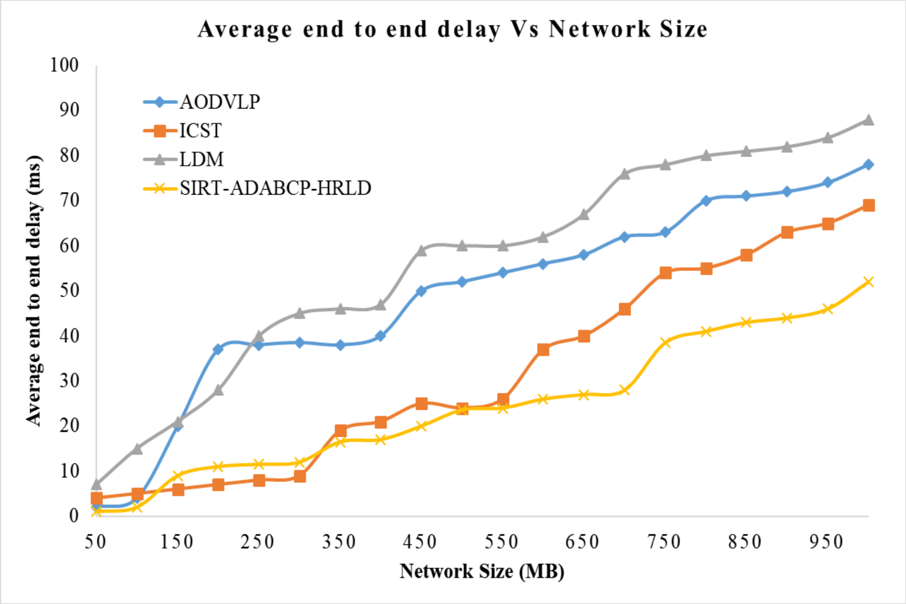


Figure 15. Graph for an end-to-end delay Vs. network size

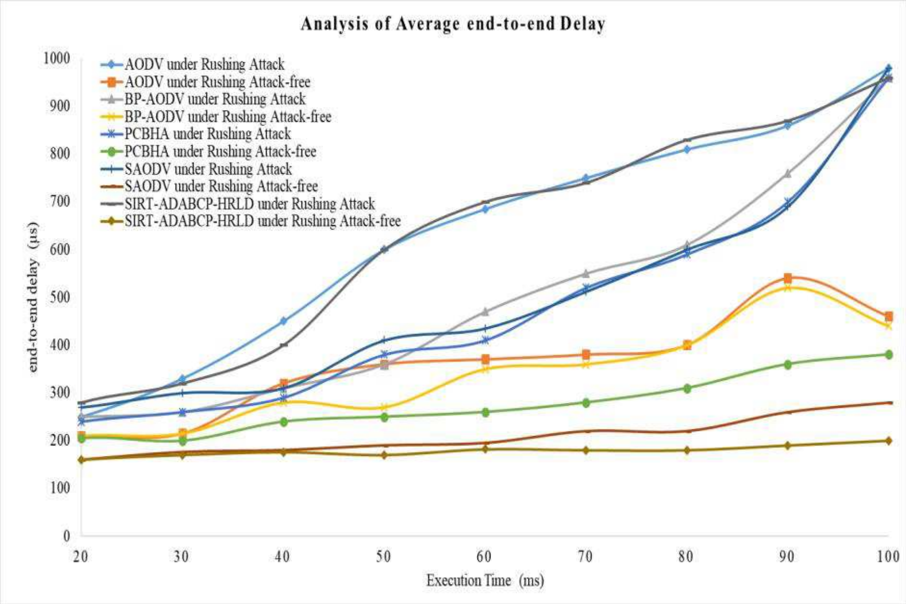


Figure 16. Consolidated performance result analysis of end-to-end delay

The Figure 12 to 16 contributes to reducing the end-to-end delay by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. This mechanism considers mobility variation by indicating the lower mobility over the network with the higher nodes, which examines against the accuracy, quality, and node lifetime. This graph contributes to reducing the end-to-end delay by presenting the SIRT framework. This efficiently improves the assigned source in the routing process. There are 100 samplings to discover the amount of packet to be delivered, and this research has implemented Hybrid Random Late Detection (HRLD) approach in the MANET environment and evaluated it by some well-known attacker [57]. Figure 12 demonstrates the simulation result of end-to-end delay (ms)inference for existing ESCT - Cai et al. (2018), ENM-LAC - Liu et al. (2019), and ZRDM-LFPM - Khudayer et al. (2020) system with proposed SIRT-ADABCP-HRLD system. The proposed SIRT-ADABCP-HRLD system shows the end-to-end delay (ms) of the existing system compared to the proposed method due to intrusion-free contributions. Figure 13 shows the simulation result of the end-to-end delay (ms) for the proposed SIRT-ADABCP-HRLD system and existing schemes like ESCT - Cai et al. (2018), ENM-LAC - Liu et al. (2019), and ZRDM-LFPM - Khudayer et al. (2020). It shows the end-to-end delay (ms) of the proposed SIRT-ADABCP-HRLD compared to the existing system, which finds a low position in end-to-end delay (ms) high attacker-less result. Figure 15 demonstrates the performance evaluation results of SIRT-ADABCP-HRLD with existing methods in terms of low end-to-end delay (ms) of 49.8361% compared with the existing methods.

ii. **Communication Overhead:** Figures 17 to 20, when communicating overhead is minimized in any source forward packet to an intermediate node, the proposed SIRT-ADABCP-HRLD System provides a secure and attacker-free route path. In the proposed method, communication overhead is minimized when compared to existing ESCT, ENM-LAC, and ZRDM-LFPM methods

$$\boldsymbol{Communication\ overhead = (Number\ of\ Packet\ Losses/Received) * 100}$$

Table 12. Performance result analysis of Communication Overhead

Nodes Mobility Count	**Communication Overhead (pkts/ms)**				**Average Communication overhead (%)**
Overhead versus Mobility	**ESCT - Cai et al. (2018),**	**ENM-LAC - Liu et al. (2019)**	**ZRDM-LFPM - Khudayer et al. (2020)**	**SIRT – ADABCP-HRLD**	**Inference for Existing system with Proposed System**
10.0000	85.23	71.60	67.56	33.46	55.2654% decrease
20.0000	77.65	66.46	60.89	25.63	62.4927% decrease
30.0000	71.39	61.95	54.34	21.19	66.1285% decrease
40.0000	68.99	56.96	48.94	20.91	64.1317% decrease
50.0000	65.39	51.28	43.64	19.93	62.7035% decrease
60.0000	61.66	40.93	31.15	15.22	65.8591% decrease
70.0000	56.09	27.94	20.97	11.35	67.5714% decrease
80.0000	52.96	22.35	13.94	8.68	70.8235% decrease
90.0000	47.99	21.46	11.38	6.88	74.4649% decrease
100.000	43.46	20.12	10.96	4.61	81.4462% decrease

Table 12 contributes to reducing the Communication Overhead (pkts/ms) by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. This Swift Implicit Response Round Trip Time is to consider Pause Time, indicating the higher pass time over the network with the exact route on the MANET environment, which examines against the overhead and node lifetime. The above graph is used to reduce the Communication Overhead by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. This improves the efficiency of assigning sources in the routing process. Here 100 samplings are used to discover the amount of packet to be delivered. This research implemented Hybrid Random Late Detection (HRLD) approach in the MANET environment and evaluated it by some well-known attackers. Table 12 establishes the result of Communication Overhead Inference for Existing ESCT, ENM-LAC, and ZRDM-LFPM system with Proposed SIRT–ADABCP-HRLD System. The Proposed SIRT–ADABCP-HRLD system shows the communication overhead of the existing system that has obtained a high rate compared to the proposed system due to the efficient route between nodes.

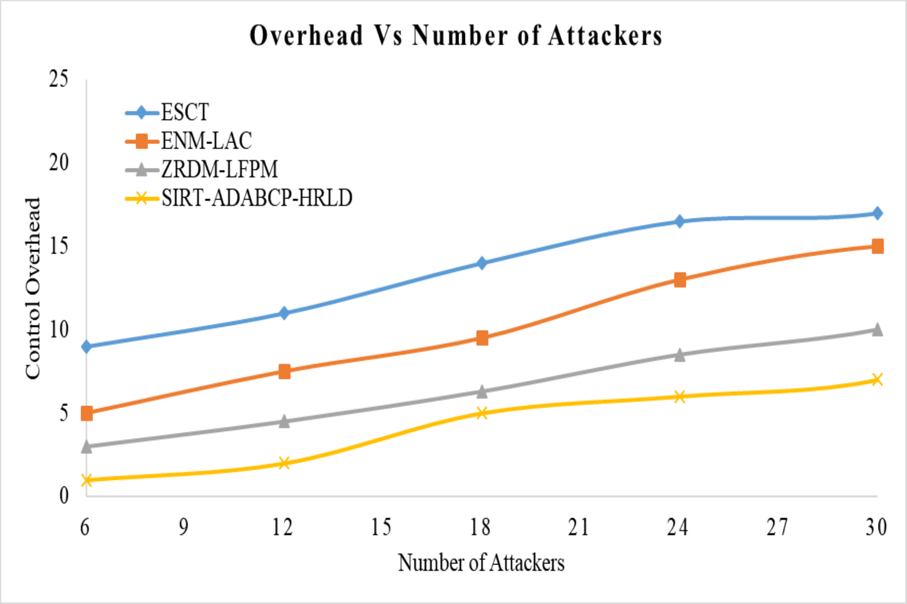


Figure 17. Graph for communication overhead Vs. number of attackers

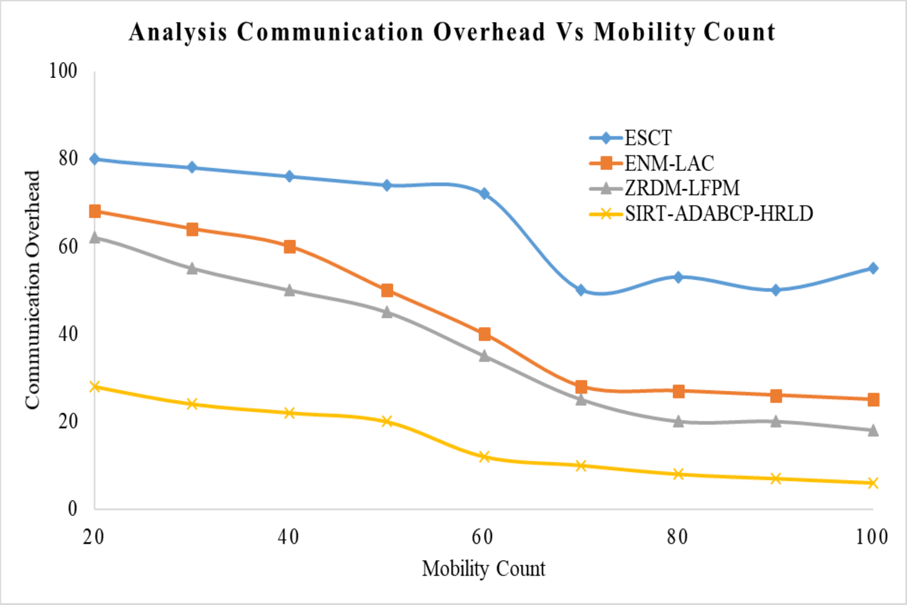


Figure 18. Graph for communication overhead Vs. mobility count

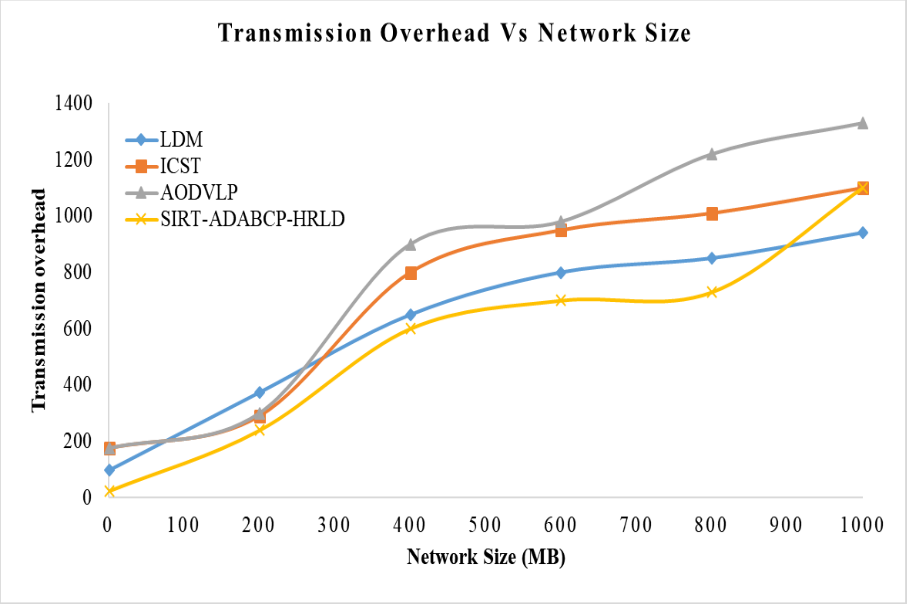


Figure 19. Graph for transmission overhead Vs. network size

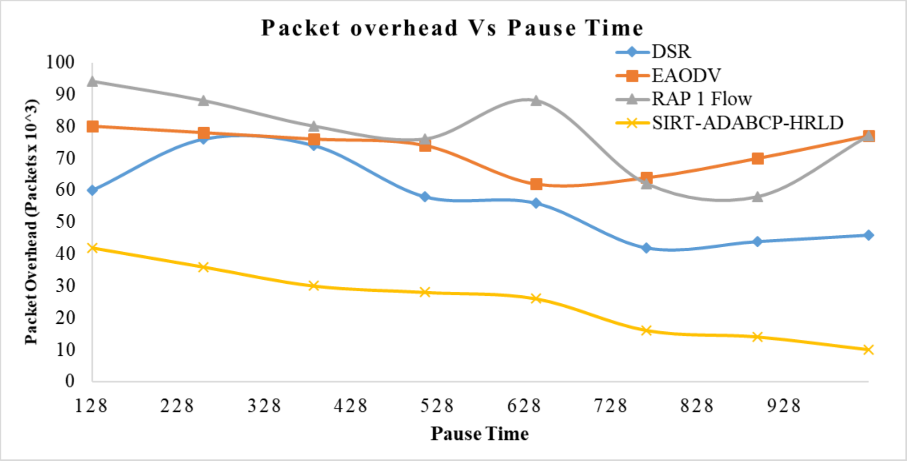


Figure 20. Graph for communication overhead Vs. network lifetime

Figure 17 contributes to reducing the communication overhead (pkts/ms) by presenting the Swift Implicit Response Round Trip Time (SIRT) framework.

This SIRT considers pause time, indicating the higher pass time over the network with the MANET environment exact route, which examines against the overhead and node lifetime. The above graph is used to reduce the communication overhead by presenting the SIRT framework. This efficiently improves the assigning source in the routing process. Here 100 samplings are used to discover the amount of packet to be delivered. This research implemented Hybrid Random Late Detection (HRLD) approach in the MANET environment and evaluated it by some well-known attackers. Figure 18 establishes the result of communication overhead inference for existing ESCT, ENM-LAC, and ZRDM-LFPM systems with the proposed SIRT-ADABCP-HRLD System. The proposed SIRT-ADABCP-HRLD system shows the existing system communication overhead that has obtained a high rate compared to the proposed method due to the efficient route between nodes.

Figure 19 shows the simulation result of communication overhead for the proposed SIRT-ADABCP-HRLD system and existing schemes. It shows the communication overhead of the proposed SIRT-ADABCP-HRLD, which has obtained low communication overhead compared to others due to high attacker fewer results. Figure 20 demonstrates the performance evaluation results of SIRT-ADABCP-HRLD with existing methods in terms of low communication overhead of 81.4462% decrease compared with the existing methods.

iii. **Packet Delivery Ratio (PDR):** Figure 21 demonstrates that the packet delivery ratio is assessed by the quantity of packet received to a packet sent count primarily distinguished from other node region rates. Node speed is a constant in MANET; the simulation rate is fixed at 150ms. The proposed method packet delivery ratio is enhanced compared to the existing ESCT, ENM-LAC, and ZRDM-LFPM methods.

$$\boldsymbol{Packet\ Delivery\ Ratio = (Number\ of\ packet\ received/generated\ packets) * 100}$$

Table 13. Performance Result Analysis of Packet Delivery Ratio (PDR)

Nodes Mobility Count	Packet Delivery Ratio (pkts/ms)				Average Communication overhead (%)
PDR versus Mobility	**ESCT - Cai et al. (2018),**	**ENM-LAC - Liu et al. (2019)**	**ZRDM-LFPM - Khudayer et al. (2020)**	**SIRT – ADABCP-HRLD**	**Inference for Existing system with Proposed System**
10.0000	28.05	42.05	46.06	55.07	42.2262% increase
15.0000	28.50	43.09	46.50	55.75	41.6293% increase
20.0000	29.08	44.03	47.08	56.06	39.9284% increase
25.0000	30.05	44.50	48.03	56.50	38.277% increase
39.0000	31.04	45.07	49.04	57.09	36.8518% increase
35.0000	31.75	45.75	49.50	58.01	37.0315% increase
40.0000	32.07	46.02	50.01	59.08	38.3607% increase
45.0000	32.50	46.50	50.50	59.50	37.8378% increase
50.0000	33.06	47.01	51.06	60.02	37.3141% increase

Table 13 contributes to increasing the Packet Delivery Ratio (pkts/ms) by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. Table 13 establishes the result of Packet Delivery Ratio Inference for Existing ESCT, ENM-LAC, and ZRDM-LFPM system with proposed SIRT–ADABCP-HRLD System.

Performance comparison of packet delivery ratio: The Proposed SIRT–ADABCP-HRLD System shows the existing system packet delivery ratio obtained a high rate compared to the proposed system due to the efficient packet delivery source and destination nodes.

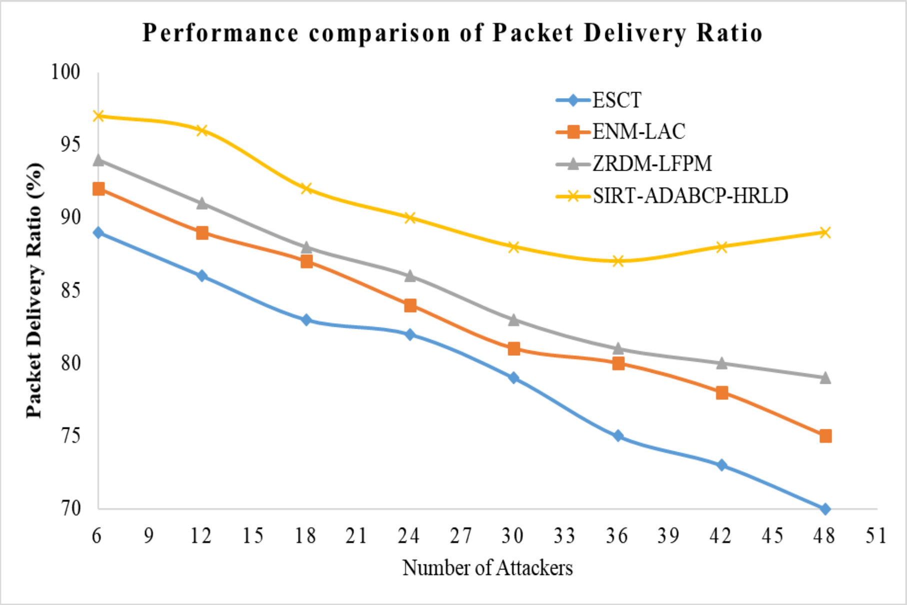


Figure 21. Graph for packet delivery ratio Vs. number of attackers

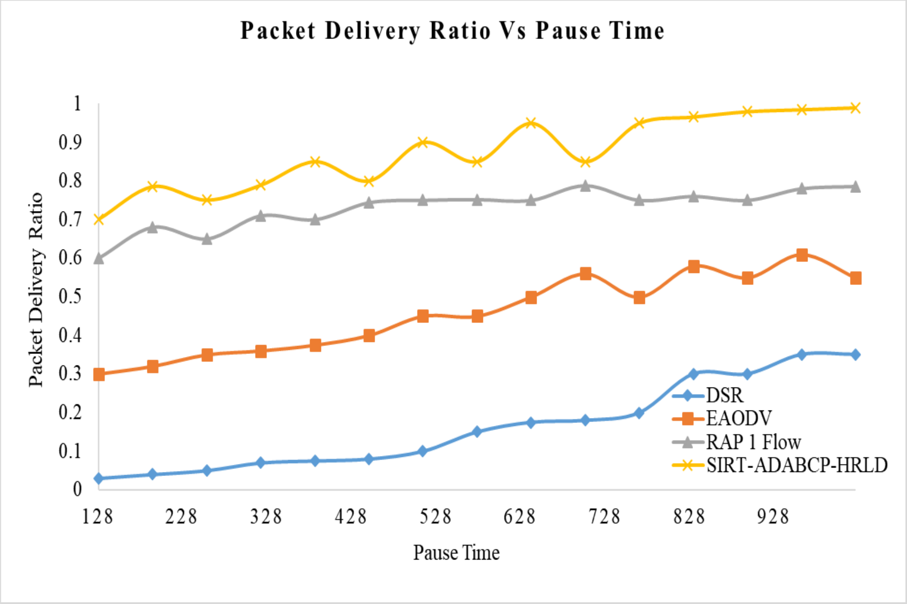


Figure 22. Graph for Packet Delivery Ratio Vs. Network Lifetime

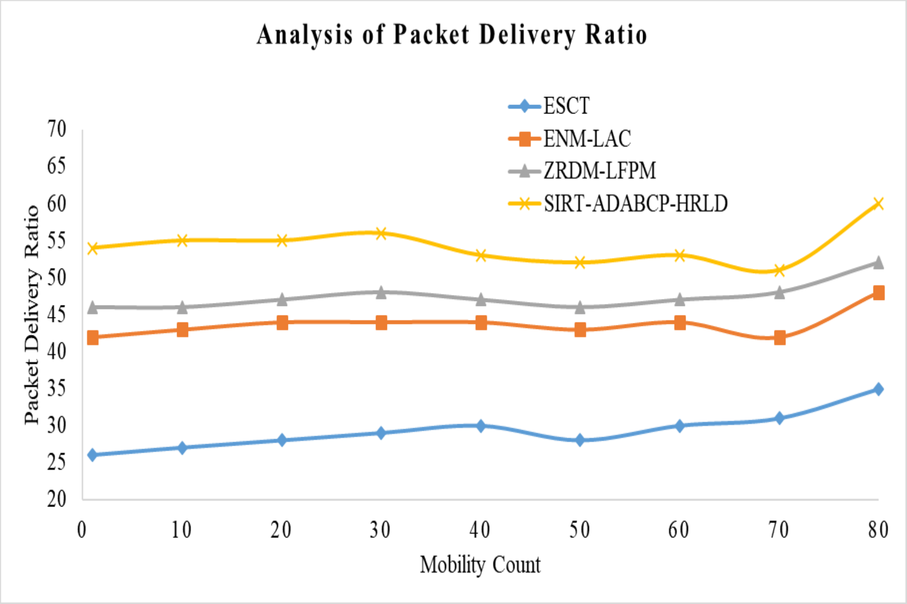


Figure 23. Graph for packet delivery ratio Vs. mobility count

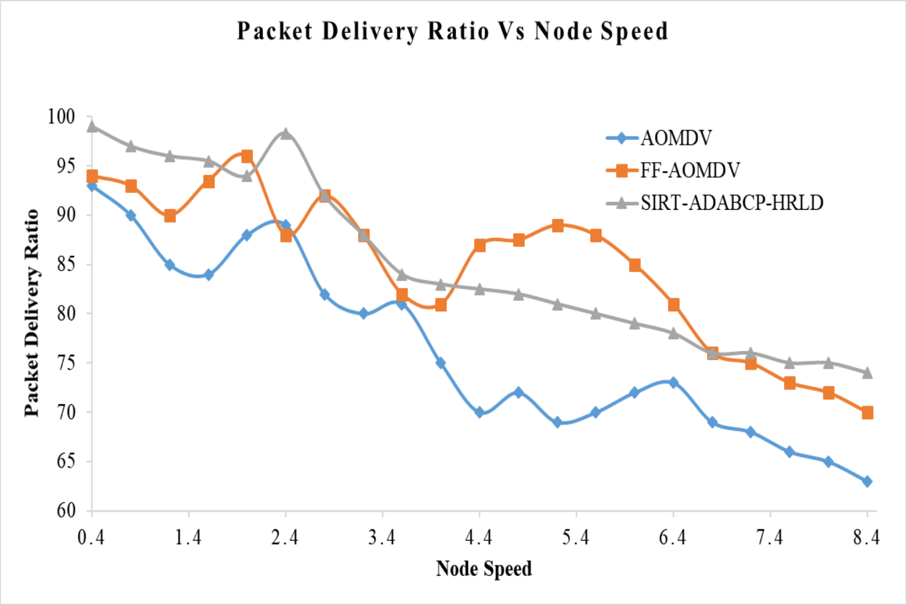


Figure 24. Graph for Packet Delivery Ratio Vs. Node Speed

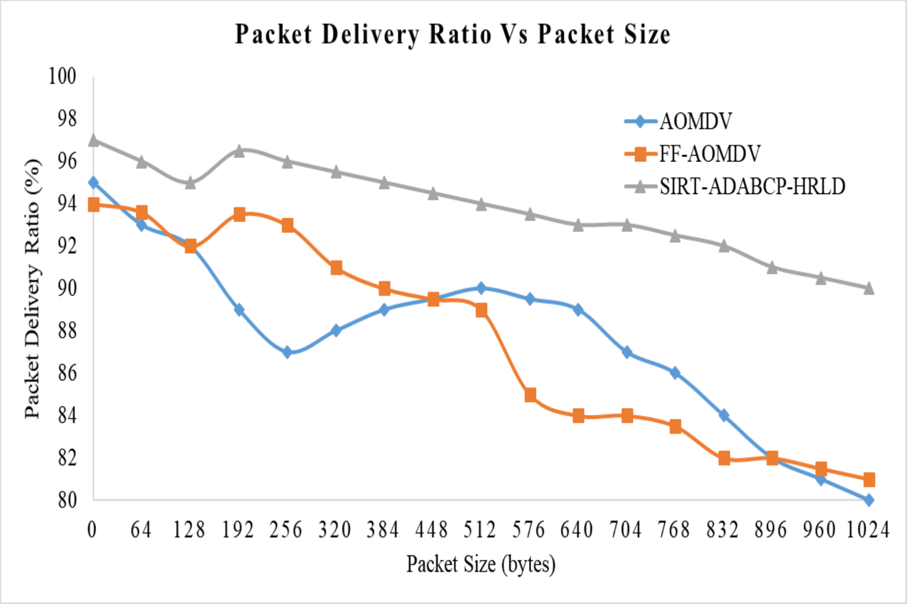


Figure 25. Graph for packet delivery ratio Vs. packet size

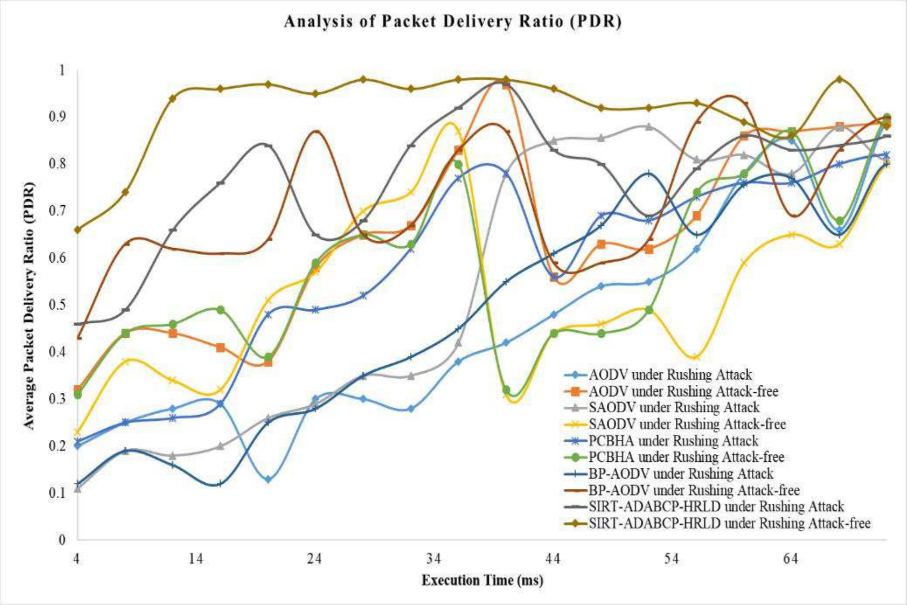


Figure 26. Performance result analysis of Packet Delivery Ratio (PDR)

Figure 22 contributes to increasing the packet delivery ratio (pkts/ms) by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. This SIRT considers the number of nodes indicating the higher delivery ratio over the network with the MANET environment exact route, which is examined against the packet delivery ratio and node count. The above graph is shown to reduce the packet delivery ratio by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. This efficiently improves the assigning source in the routing process. Here a test is done with the 50 samplings to find the number of packets to be delivered per minute. Figures 23 to 26 establishes the result of packet delivery ratio inference for the existing ESCT, ENM-LAC, and ZRDM-LFPM systems with the proposed SIRT-ADABCP-HRLD system. The proposed SIRT-ADABCP-HRLD system shows the existing system packet delivery ratio that has a high rate than the proposed system due to the efficient packet delivery source and destination nodes. Figure 24 shows the packet delivery ratio simulation result for the proposed SIRT-ADABCP-HRLD system and existing schemes. It shows the packet delivery ratio of the proposed SIRT-ADABCP-HRLD that has obtained a higher quantity of packets delivered to the destination than the others due to the lower attacker less result. Figure 25 demonstrates the performance evaluation results of SIRT-ADABCP-HRLD with the existing methods in terms of high Packet Delivery Ratio (PDR) of 42.2262% increase compared to the existing methods.

iv. **Network Lifetime:** This has been calculated by the processing time that is the time taken by normal nodes to become a dead node. i.e., the time taken to issue energy by any participating nodes is referred to as the Network lifetime. Figure 27 manifests the lifetime of the network that is estimated by the whole process of the proposed system network and the effort employed to do communication successfully. In the proposed method, the lifetime of the network is enhanced when compared to the existing method. For this consideration, each packet relaying node is inspected by the data packet transition. In this era, the network lifetime is balanced concerning the energy spending on routing protocols communication. This proposed Attacker Detection Automation of the Bees Colony Optimization (ADABCP) protocol is measured using the network lifetime [24] [30] [34]. All the participant nodes do not act in the routing stage at the same time. Some nodes act as sleep nodes, some as dead nodes, and most of the nodes are in the alive node.

In these three stages, the nodes have preserved the energy for increasing the node sensing capability. If one node becomes the dead node instead of this, another node will take the responsibility to transmit the packets to the destination. Rapidly, this process is happening in the data transmission to improve the network lifetime for the whole network; this postponement of energy reduction is much useful to the continuous packet delivery because of the networks un-interrupted lifetime [54]. The above introduces the proposed techniques to step-up the network lifetime by node energy and routing process. Figure 27 shows that better network lifetimes are achieved on the target node by the Hybrid Random Late Detection (HRLD). HRLD protocol is integrated with the node selection process and route optimization process to improve the network lifetime in the active routing stage. The network lifetime of the suggested protocols is expressed in figure 27

$$\boldsymbol{Network\ Lifetime = \ length\ of\ energy\ usage/overall\ energy}$$

Table 14. Performance Result Analysis of Network Lifetime

Nodes Mobility Count	**Network Lifetime (J/ms/bits/pkts)**				**Average Network Lifetime (%)**
NLT versus Mobility	**ESCT - Cai et al. (2018),**	**ENM-LAC - Liu et al. (2019)**	**ZRDM-LFPM - Khudayer et al. (2020)**	**SIRT – ADABCP-HRLD**	**Inference for Existing system with Proposed System**
10.0000	32.50	53.51	70.04	83.06	59.6796% increase
20.0000	34.08	53.72	71.503	84.08	58.3398% increase
30.0000	34.75	54.07	72.08	85.07	58.614% increase
40.0000	34.95	55.03	72.50	86.06	58.8996% increase
50.0000	35.00	56.04	73.04	86.50	58.1546% increase
60.0000	36.06	57.08	73.50	87.07	56.7511% increase
70.0000	37.08	57.50	74.06	88.06	56.6532% increase
80.0000	37.50	58.01	74.50	88.50	56.1673% increase
90.0000	38.08	59.07	74.75	88.75	54.8866% increase
100.000	38.55	59.50	75.11	89.08	54.3313% increase

In these three stages, the nodes have preserved the energy to increase the node sensing capability. If one node becomes the dead node instead of this, another node will take the responsibility to transmit the packets to the destination. Rapidly this process is happening in the data transmission to improve the network lifetime for the whole network; this postponement of energy reduction is much useful to the continuous packet delivery by the un-interrupted lifetime of the network [Ramamoorthi et al., (2019)]. Above table 14 introduces the proposed techniques to step-up network lifetime by node energy and routing process. In table 14, better network lifetimes are achieved on the Hybrid Random Late Detection (HRLD) target node. HRLD protocol is integrated with the node selection process and route optimization process to improve the network lifetime active routing stage. The network lifetime of the suggested protocols is expressed in Figure 27

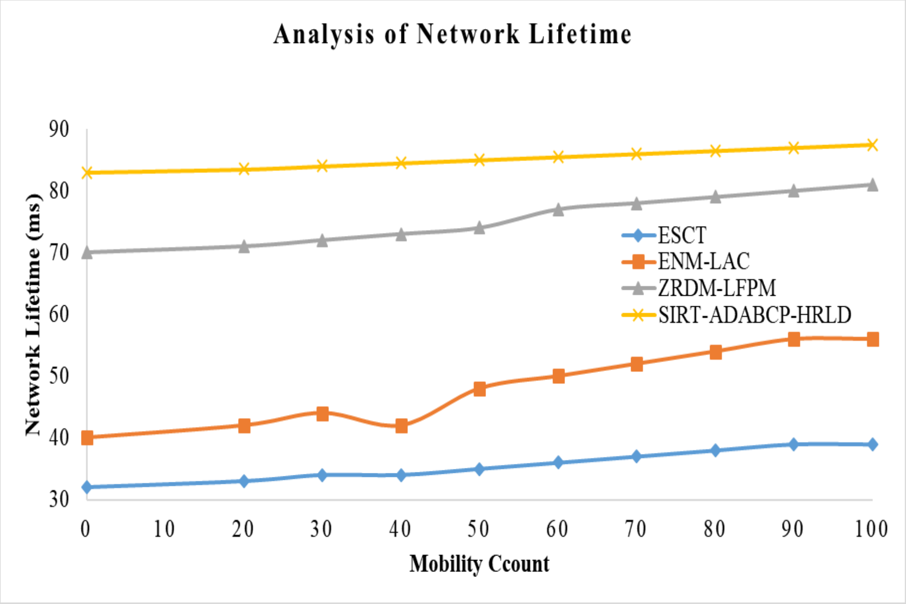


Figure 27. Graph for network lifetime Vs. mobility count

Figure 27 clarifies the values of the speed of packets delivered Vs. energy consumption per bit during a single relay (from 1 to100 node). This speed of the nodes will declare the lifetime of the network and total energy saved in one packet delivered to the destination. The packet delivery time is significantly higher for any two selected transmissions. The proposed SIRT-ADABCP-HRLD packet delivery rate is compared to ESCT, ENM-LAC, and ZRDM-LFPM. The data transmission improves the amount of packet delivered by 56.9775%, more as compared to ESCT, ENM-LAC, and ZRDM-LFPM.

v. **Energy Consumption:** Figure 28 and Table 15 establish energy consumption to evaluate the packet transmissions total energy between sender and receiver nodes. In the proposed method, the high routing delay is used for packet transmission; hence the energy consumption is minimized compared to the existing method. In mobile ad hoc networks, the participants nodes are processed in the data transfer between the nodes by confirming the source and destination availability [66]. After that, route searching, path routing, and data transfer are usually considered. This happens by spending the node energy. This energy consumption is considered for data transfer alone, but some energy values are negligible on the RREQ and RRES on the routing process.

$$\boldsymbol{Energy\ Consumption = \ Initial\ Energy - Final\ Energy}$$

In the proposed SIRT-ADABCP-HRLD, the time required for energy transmission can be calculated based on the time of data transfer, considering n nodes have participated in the proposed MANET. Based on the proposed algorithm, the routing chooses the most straightforward route between nodes, and its energy consumption is deficient compared to all existing simulations. In Figure 28, a total of 100 nodes have participated; 1000 request transactions were done. One hundred packets/nodes are requested for the transaction before the data transmission. From this consideration, firstly, energy consumption for routing with different routing parameters varies from 145 J/Sec from 190 J/Sec on the proposed system, which is 36.31% less value compared to the existing ESCT, ENM-LAC and ZRDM-LFPM. All 100 nodes are taking 1400 J/Sec to execute all transactions within the stipulated time interval.

Table 15. Performance Result Analysis of Energy Consumption

Nodes Mobility Count	Energy Consumption (J/sec)				Average Energy Consumption (%)
Energy Consumption versus Mobility	**ESCT - Cai et al. (2018),**	**ENM-LAC - Liu et al. (2019)**	**ZRDM-LFPM - Khudayer et al. (2020)**	**SIRT – ADABCP-HRLD**	**Inference for Existing system with Proposed System**
20.0000	260	243	205	145	38.55% decrease
30.0000	270	248	209	151	37.68% decrease
40.0000	278	253	211	158	36.11% decrease
50.0000	285	261	221	160	37.41% decrease
60.0000	293	268	231	162	38.63% decrease
70.0000	298	270	235	170	36.48% decrease
80.0000	305	271	241	178	34.63% decrease
90.0000	312	276	248	184	33.97% decrease
100.000	320	280	255	190	33.33% decrease

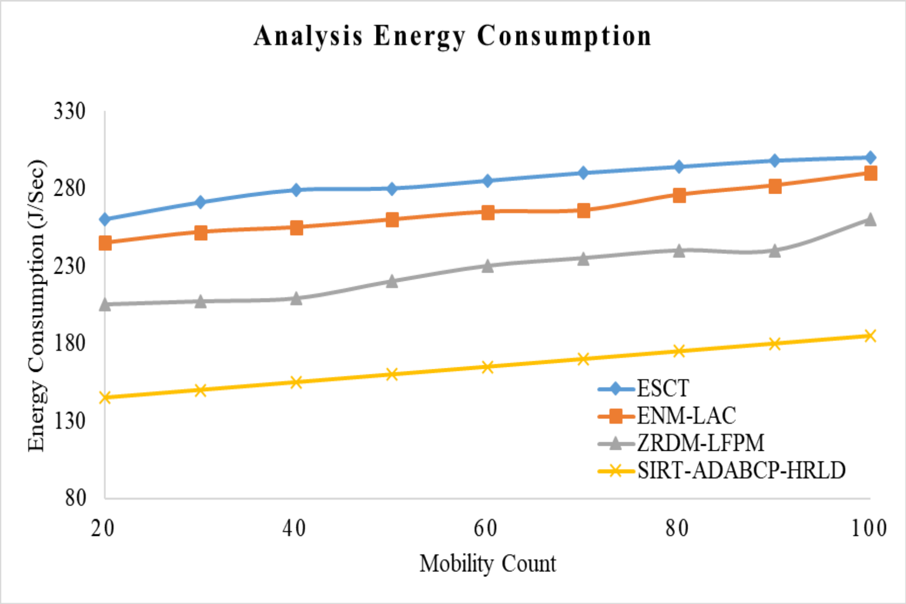


Figure 28. Graph for Energy Consumption Vs. Mobility Count

If the participant nodes are increased, the energy consumption becomes higher compared to the ZRDM-LFPM. This higher energy consumption is also reduced in the proposed SIRT-ADABCP-HRLD. SIRT-ADABCP-HRLD consumes lower energy because nodes have continuous attention with the attentiveness of the MANET participants. For this reason, even when the energy consumption rate is less, the number of nodes is increased. Finally, the proposed model without an error rate saves 38.63% times the energy than the normal existing routing process.

vi. **Throughput:** During network lifetime, throughput is determined as the number of data packets (number of bits) successfully interchanged between source and destination and, because of that, acknowledges the packet data delivery. The average number of bytes received by destination nodes per second provides the throughput of the network. The throughput is expressed in kilobits per second (Kbps).

This is also used to measure a routing protocol efficiency in receiving data packets by destination. Throughput is calculated by using

$$\mathbf{Throughput} = \frac{(\mathbf{total\ number\ of\ data\ packets\ received} * \mathbf{8})}{(\mathbf{simulation\ time})} * \mathbf{1000\ kbps}$$

This expressed above is the formula to calculate the throughput. The above equation affords the average number of bits (8 bits) obtained by destination nodes per second. Throughput refers to the average data rate during successful data delivery over a specific communication link.

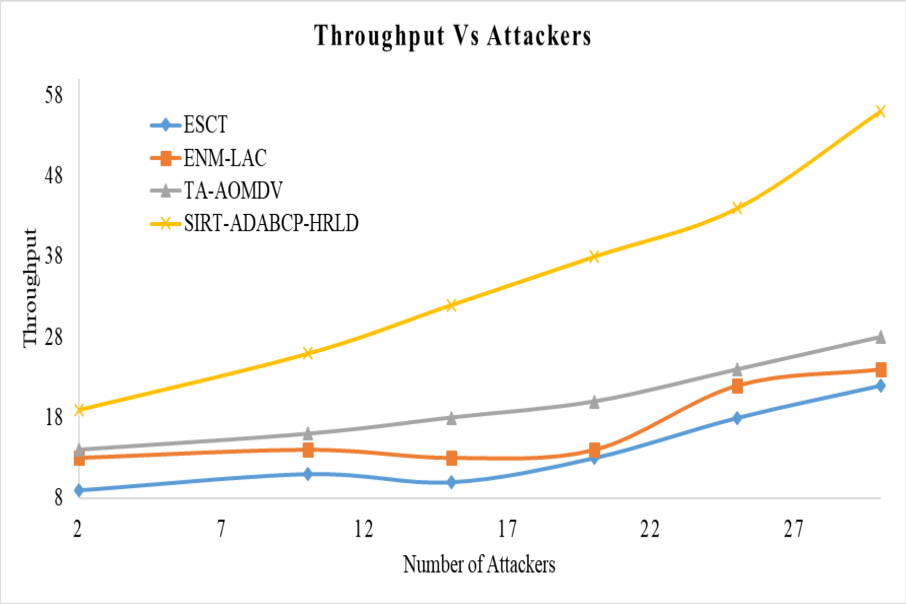


Figure 29. Graph for throughput Vs. attackers

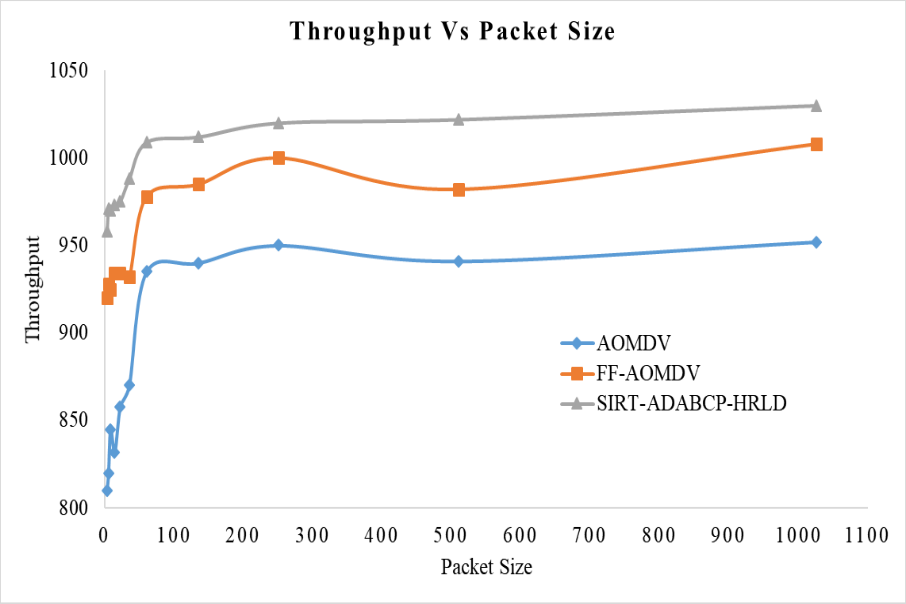


Figure 30. Graph for throughput Vs. packet size

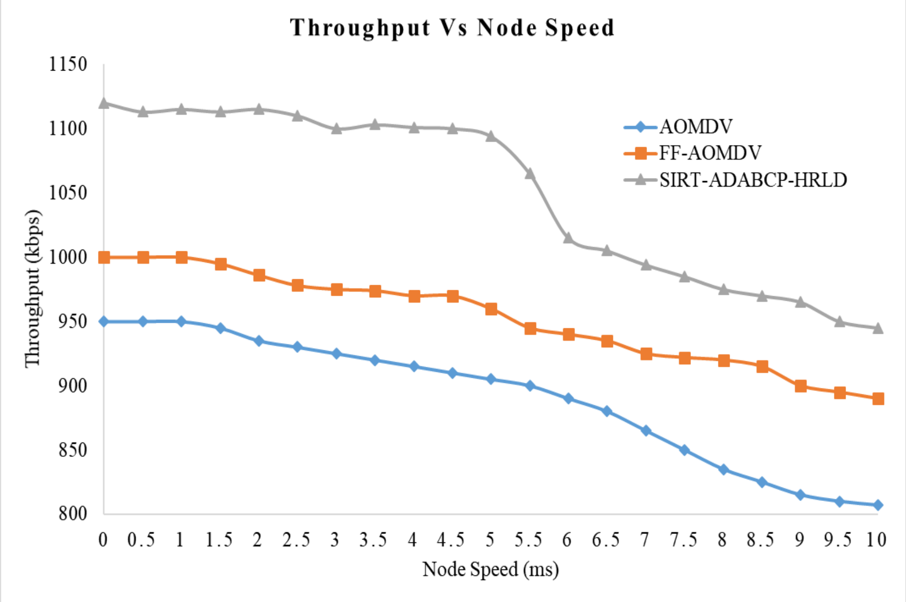


Figure 31. Graph for throughput Vs. node speed

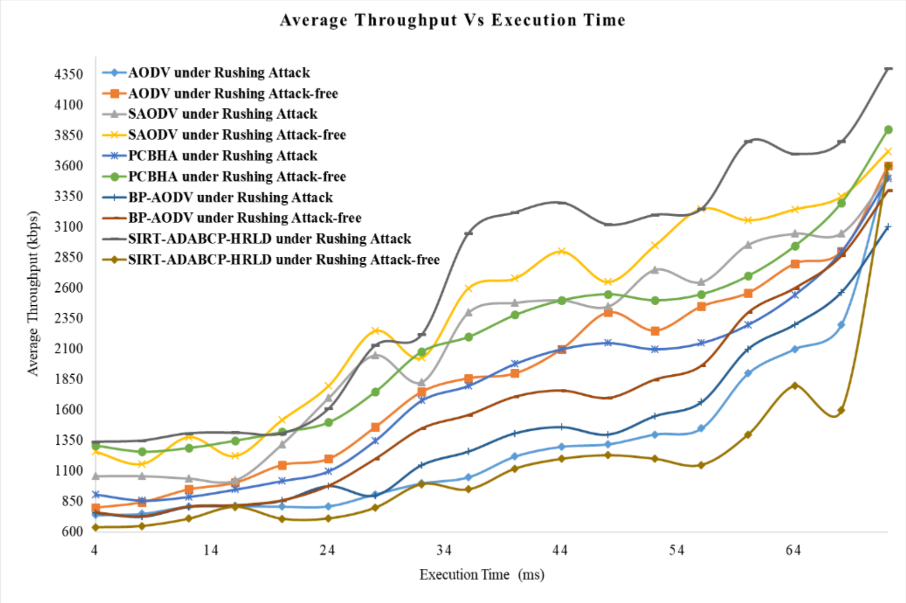


Figure 32. Performance result analysis of for throughput

Figure 29 shows throughput comparison between SIRT-ADABCP-HRLD protocol with ESCT, ENM-LAC, and TA-AOMDV at different explosion lengths of an attacker. At explosion length of attacker 0-25 gives better performance as compare to ESCT, ENM-LAC. Figure.30 shows the effect of varying attackers on the throughput for ESCT, ENM-LAC, and TA-AOMDV routing protocols. Attacker count is varied as (6, 8, 10, … 30) count. When the attacker count increases, the throughput increases also. The SIRT-ADABCP-HRLD protocol has better performance in terms of throughput than ESCT, ENM-LAC, and TA-AOMDV protocols. Above stated graph shows the impact of a different number of attacker nodes on the throughput. The attackers nodes increase in the 2-30 range, the throughput of SIRT-ADABCP-HRLD increases from 30Kbps to 66Kbps. As shown in Figure 31, as the number of attacker nodes increases, SIRT-ADABCP-HRLD has a more significant performance advantage than ESCT, ENM-LAC, and TA-AOMDV protocols. There is an improvement in throughput when using the SIRT-ADABCP-HRLD protocols mechanism when applying ADABCP with SIRT-HRLD, throughput increases at most of the explosion periods of attack. Figure 32 shows the variation of throughput for FF-AOMDV, AOMDV, and SIRT-ADABCP-HRLD. When the packet size increases as (100, 200, 300, 400, …, 1000) bytes, the throughput decreases. The SIRT-ADABCP-HRLD decreases from 1134.78 kbps to 981.26 kbps; the AOMDV also decreases from 968.kbps to 880kbps. The SIRT-ADABCP-HRLD routing protocol has better performance than both AOMDV and FF-AOMDV in terms of throughput.

Figure 30 depicts the performance of throughput of packets against the node speed. According to the throughput changes in figure 31, the performance is analyzed from two-speed ranges. As the node speed increases (0, 0.5, 1, 1.5ms), the throughput of the proposed SIRT-ADABCP-HRLD decreases from 950Kbps to 800Kbps. SIRT-ADABCP-HRLD has the best performance within this speed range, followed by AOMDV, and FF-AOMDV has the worst performance. When the node speed increases (20, 25, 30, 35, 40ms), the throughput of SIRT-ADABCP-HRLD decreases from 500.86Kbps to 100Kbps. SIRT-ADABCP-HRLD has the best performance in the range of 0-10ms speed. These ranges show the throughput changes in different data rate scenarios. Figure 29 demonstrates the throughput for the suggested SIRT-ADABCP-HRLD and existing methods. In Figure 32, the mean throughput of the MANET is 50% when there is no attack. For rushing attacks, the malicious agent is launched at 68ms and floods data packets to all its neighbors. As a result, the mean throughput is reduced to 70%. In the AODV protocol, the rushing attack node, which is activated at 30ms, starts dropping the packets. Hence, the throughput regularly drops by 95%, and the mean throughput decreases to 23% for rushing attacks. From this consideration, the throughput is high in the absence of a rushing attack.

Above, Figure 32 illustrates the results of the Throughput comparison between a proposed model with existing models. In this analysis, 500 nodes were used. The performance of throughput (kb/s) was analyzed in each node. For instance, for 100 nodes, network throughput was 1006 kb/s. This result showed that the throughput reached the maximum rate because the aggregation was performed based on distance. In line with this, the rushing attacks were also reduced. The results reveal that the four protocols produce almost the same average throughput under attack conditions during the simulation. The results of the average throughput in the figure. 32, show that the SIRT-ADABCP-HRLD protocols are protected under the rushing attack performed with malicious nodes during the routing process. These protocols can detect the malicious node and remove it from the route paths during the routing process. The performance evaluation of SIRT-ADABCP-HRLD based routing was carried out with the existing approaches based on throughput with two aspects such as attack and without attack. The existing techniques used for the comparison are AODV, SAODV, PCBHA, Bp-AODV. At the maximum time limit, SIRT-ADABCP-HRLD had a throughput of 3750kbps, while AODV, SAODV, PCBHA, Bp-AODV had below 3000kbps. In figure. 32, the comparative analysis results based on throughput are shown in all the considered protocols, which is higher than all the other techniques.

5. Conclusion and Future Enhancement

In MANET routing, the packets interaction and data transmission are efficiently discussed concerning the MANET routing. This research involves managing the packets and routes between the sources and the destination to maintain the route interaction process. The pursued effective data transaction over the MANET network always improves the route and reduces the attacker by the proposed (SIRT-ADABCP-HRLD) mechanism. However, the proposed mobile ad hoc conditions are uncompromised for route interaction against security threats. In this research article, the proposed four processing schemes are preserved with the security measures against routing protocols. Even though, ADABCP method works against attacker detection on the routing process. Furthermore, the proposed Hybrid Random Late Detection (HRLD) routing protocol manages the MANET routing. It overcomes the congestion communication on MANET, although the Swift Implicit Response Round Trip Time (SIRT) mechanism helps find optimal routing securely and intelligently. The simulation results are compared against existing ESCT, ZRDM-LFPM, and ENM-LAC approaches. As a result, the simulated illustration (SIRT-ADABCP-HRLD) is improved by routing and data transmission. Compared to the other method, SIRT-ADABCP-HRLD achieves a better ratio for the end-to-end delay, communication overhead, packet delivery ratio, network lifetime, and energy consumption. In the future, this research can be applied to the intrusion detection system and IoT-based suspect detection system on finding the susceptible object and cyber attacker over the internet black chain technology.

Conflict of Interest: Corresponding author and co-author declare that they have no conflict of interest.

Reference

[1]. Balaji, S., Julie, E. G., Robinson, Y. H., Kumar, R., & Thong, P. H. (2019). Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model. Computer Standards & Interfaces, 66, 103358.

[2]. Djedjig, N., Tandjaoui, D., Medjek, F., &Romdhani, I. (2020). Trust-aware and cooperative routing protocol for IoT security. Journal of Information Security and Applications, 52, 102467.

[3]. Hahn, F., Pappa, A., &Eisert, J. (2019). Quantum network routing and local complementation. npj Quantum Information, 5(1), 1-7.

[4]. Al-Zahrani, F. A. (2020). On Modeling Optimizations and Enhancing Routing Protocols for Wireless Multihop Networks. IEEE Access, 8, 68953-68973.

[5]. Alzamzami, O., &Mahgoub, I. (2020). Link Utility Aware Geographic Routing for Urban VANETs using Two-Hop Neighbor Information. Ad Hoc Networks, 102213.

[6]. Bai, J., Sun, Y., Phillips, C., & Cao, Y. (2017). Toward constructive relay-based cooperative routing in MANETs. IEEE Systems Journal, 12(2), 1743-1754.

[7]. Amutha, S., &Balasubramanian, K. (2018). Secured energy optimized Ad hoc on-demand distance vector routing protocol. Computers & Electrical Engineering, 72, 766-773.

[8]. Bozorgi, A. M., Farasat, M., & Mahmoud, A. (2017). A time and energy efficient routing algorithm for electric vehicles based on historical driving data. IEEE Transactions on Intelligent Vehicles, 2(4), 308-320.

[9]. Khudayer, B. H., Anbar, M., Hanshi, S. M., & Wan, T. C. (2020). Efficient Route Discovery and Link Failure Detection Mechanisms for Source Routing Protocol in Mobile Ad-Hoc Networks. IEEE Access, 8, 24019-24032.

[10]. Li, Z., & Wu, Y. (2017). Smooth mobility and link reliability-based optimized link state routing scheme for manets. IEEE Communications Letters, 21(7), 1529-1532.

[11]. Hurley-Smith, D., Wetherall, J., &Adekunle, A. (2017). SUPERMAN: security using pre-existing routing for mobile ad hoc networks. IEEE Transactions on Mobile Computing, 16(10), 2927-2940.

[12]. Cai, R. J., Li, X. J., & Chong, P. H. J. (2018). An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE Transactions on Mobile Computing, 18(1), 42-55.

[13]. Chen, Y. H., Wu, E. H. K., Lin, C. H., & Chen, G. H. (2017). Bandwidth-satisfied and coding-aware multicast protocol in MANETs. IEEE Transactions on Mobile Computing, 17(8), 1778-1790.

[14]. Chintalapalli, R. M., &Ananthula, V. R. (2018). M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network. IET Communications, 12(12), 1406-1415.

[15]. Taha, A., Alsaqour, R., Uddin, M., Abdelhaq, M., &Saba, T. (2017). Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function. IEEE access, 5, 10369-10381.

[16]. Garaaghaji, A., &Alfi, A. (2019). A Fuzzy-Hierarchical Routing Algorithm for MANET Networks Allocation Rates Problem. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 1-9.

[17]. Kacem, I., Sait, B., Mekhilef, S., &Sabeur, N. (2018). A new routing approach for mobile ad hoc systems based on fuzzy Petri nets and ant system. IEEE Access, 6, 65705-65720.

[18]. Liu, S., Zhang, D. G., Liu, X. H., Zhang, T., Gao, J. X., & Cui, Y. Y. (2019). Dynamic analysis for the average shortest path length of mobile ad hoc networks under random failure scenarios. IEEE Access, 7, 21343-21358.

[19]. Zhang, T., Zhao, S., & Cheng, B. (2020). Multipath Routing and MPTCP-Based Data Delivery Over Manets. IEEE Access, 8, 32652-32673

[20]. Islabudeen, M., & Devi, M. K. (2020). A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks. Wireless Personal Communications, 1-32.

[21]. Sahu, R., Sharma, S., & Rizvi, M. A. (2020). ZBLE: Zone Based Efficient Energy Multipath Protocol for Routing in Mobile Ad Hoc Networks. Wireless Personal Communications, 1-19.

[22]. Bamhdi, A. M. (2020). Efficient Dynamic-Power AODV Routing Protocol Based on Node Density. Computer Standards & Interfaces, 103406.

[23]. Chen, Z., Zhou, W., Wu, S., & Cheng, L. (2020). An Adaptive on-Demand Multipath Routing Protocol WithQoS Support for High-Speed MANET. IEEE Access, 8, 44760-44773.

[24]. Srivastava, A., Prakash, A., &Tripathi, R. (2020). Location based routing protocols in VANET: Issues and existing solutions. Vehicular Communications, 100231.

[25]. Al Shahrani, A. S. (2011, November). Rushing attack in mobile ad hoc networks. In 2011 Third International Conference on Intelligent Networking and Collaborative Systems (pp. 752-758). IEEE.

[26]. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003, September). Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM workshop on Wireless security (pp. 30-40).

[27]. Robinson, Y. H., Krishnan, R. S., Julie, E. G., Kumar, R., & Thong, P. H. (2019). Neighbor Knowledge-based Rebroadcast algorithm for minimizing the routing overhead in Mobile Ad-hoc Networks. Ad Hoc Networks, 93, 101896.

[28]. Kim, B. S., Ullah, S., Kim, K. H., Roh, B., Ham, J. H., & Kim, K. I. (2020). An enhanced geographical routing protocol based on multi-criteria decision making method in mobile ad-hoc networks. Ad Hoc Networks, 102157.

[29]. Ladas, A., Deepak, G. C., Pavlatos, N., &Politis, C. (2018). A selective multipath routing protocol for ubiquitous networks. Ad Hoc Networks, 77, 95-107.

[30]. Matheus, L. M., Vieira, A. B., Vieira, M. A., & Vieira, L. F. (2019). DYRP-VLC: A dynamic routing protocol for Wireless Ad-Hoc Visible Light Communication Networks. Ad Hoc Networks, 94, 101941.

[31]. Muneeswari, B., &Manikandan, M. S. K. (2019). Energy efficient clustering and secure routing using reinforcement learning for three-dimensional mobile ad hoc networks. IET Communications, 13(12), 1828-1839.

[32]. Shen, J., Wang, C., Wang, A., Liu, Q., & Xiang, Y. (2017). Moving centroid based routing protocol for incompletely predictable cyber devices in cyber-physical-social distributed systems. Future Generation Computer Systems.

[33]. Sultanuddin, S. J., & Ali Hussain, M. Token system-based efficient route optimization in mobile ad hoc network for vehicular ad hoc network in smart city. Transactions on Emerging Telecommunications Technologies, e3853.

[34]. Mukhedkar, M. M., &Kolekar, U. (2020). E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network. International Journal of Communication Systems, 33(7), e4252.

[35]. Kausar, S., Habib, M., Shabir, M. Y., Ullah, A., Xu, H., Mehmood, R., ... & Iqbal, M. S. (2020), Secure and efficient data transfer using spreading and assimilation in MANET. Software: Practice and Experience.

[36]. Ghoreishi, S. M., Razak, S. A., Isnin, I. F., &Chizari, H. (2014, August). Rushing attack against routing protocols in Mobile Ad-Hoc Networks. In 2014 International Symposium on Biometrics and Security Technologies (ISBAST) (pp. 220-224). IEEE.

[37]. Priya, J. S., Femina, M. A., & Samuel, R. A.(2020) APSO-MVS: an adaptive particle swarm optimization incorporating multiple velocity strategies for optimal leader selection in hybrid MANETs.

[38]. Allimuthu, U. (2017). BAU FAM: biometric-blacklisting anonymous users using fictitious and adroit manager. J. Adv. Res. Dyn. Control Syst.(12-Special), 722

[39]. Robinson, Y. H., Julie, E. G., Saravanan, K., Kumar, R., Abdel-Basset, M., & Thong, P. H. (2019). Link-Disjoint Multipath Routing for Network Traffic Overload Handling in Mobile Ad-hoc Networks. IEEE Access, 7, 143312-143323.

[40]. Chithaluru, P., Tiwari, R., & Kumar, K. (2019). AREOR–Adaptive ranking based energy efficient opportunistic routing scheme in Wireless Sensor Network. Computer Networks, 162, 106863.

[41]. Jabbar, W. A., Saad, W. K., & Ismail, M. (2018). MEQSA-OLSRv2: A multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT. IEEE Access, 6, 76546-76572.

[42]. Kanagasundaram, H., &Kathirvel, A. (2018). EIMO-ESOLSR: energy efficient and security-based model for OLSR routing protocol in mobile ad-hoc network. IET Communications, 13(5), 553-559.

[43]. Li, Y., & Wang, X. (2019). A novel and efficient address configuration for MANET. International Journal of Communication Systems, 32(13), e4059.

[44]. Ho, M. C., Lim, J. M. Y., Soon, K. L., & Chong, C. Y. (2019). An improved pheromone-based vehicle rerouting system to reduce traffic congestion. Applied Soft Computing, 84, 105702.

[45]. Yan, C., Yang, K. Y., & Martin, O. J. (2017). Fano-resonance-assisted metasurface for color routing. Light: Science & Applications, 6(7), e17017-e17017.

[46]. Zhang, L., Hu, L., Hu, F., Ye, Z., Li, X., & Kumar, S. (2020). Enhanced OLSR routing for airborne networks with multi-beam directional antennas. Ad Hoc Networks, 102116.

[47]. Ortiz, E., Starnini, M., & Serrano, M. Á. (2017). Navigability of temporal networks in hyperbolic space. Scientific reports, 7(1), 1-9.

[48]. El-Semary, A. M., &Diab, H. (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. IEEE Access, 7, 95185-95199.

[49]. Govindasamy, J., &Punniakody, S. (2018). A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. Journal of Electrical Systems and Information Technology, 5(3), 735-744.

[50]. Jaiswal, R. K. (2020). Position-based routing protocol using Kalman filter as a prediction module for vehicular ad hoc networks. Computers & Electrical Engineering, 83, 106599.

[51]. Pai, K. J., Chang, R. S., & Chang, J. M. (2020). A protection routing with secure mechanism in Möbius cubes. Journal of Parallel and Distributed Computing.

[52]. Thebiga, M., &SujiPramila, R. (2020). A New Mathematical and Correlation Coefficient Based Approach to Recognize and to Obstruct the Black Hole Attacks in Manets Using DSR Routing. WIRELESS PERSONAL COMMUNICATIONS.

[53]. Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Transactions on Reliability.

[54]. Ramamoorthi, J. S., &Sangaiah, A. K. (2019). SCGR: Self-configuring greedy routing for minimizing routing interrupts in vehicular communication networks. Internet of Things, 8, 100108.

[55]. Jain, M., Sharma, N., Gupta, A., Rawal, D., & Garg, P. (2020). Performance Analysis of NOMA Assisted Mobile Ad hoc Networks for Sustainable Future Radio Access. IEEE Transactions on Sustainable Computing.

[56]. Mishra, A., Saha, S., Makhija, S., Sinha, S., Raychoudhury, V., & CC, S. (2019). Empirical study of dynamics of amoebiasis transmission in mobile ad hoc networks (MANETs). International Journal of Communication Systems, e4186.

[57]. Kleineberg, K. K., &Helbing, D. (2017). Collective navigation of complex networks: Participatory greedy routing. Scientific reports, 7(1), 1-9.

[58]. Khanna, N., &Sachdeva, M. (2019). Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation. International Journal of Communication Systems, 32(12), e4012.

[59]. Kirst, C., Timme, M., &Battaglia, D. (2016). Dynamic information routing in complex networks. Nature communications, 7(1), 1-9.

[60]. Rosas, E., Garay, F., & Hidalgo, N. (2020). Context-aware self-adaptive routing for delay tolerant network in disaster scenarios. Ad Hoc Networks, 102, 102095.

[61]. Manolopoulos, I., Kontovasilis, K., Stavrakakis, I., &Thomopoulos, S. C. (2020). Methodologies for calculating decision-related event occurrence times, with applications to effective routing in diverse MANET environments. Ad Hoc Networks, 99, 102068.

[62]. Santos, B. P., Goussevskaia, O., Vieira, L. F., Vieira, M. A., &Loureiro, A. A. (2018). Mobile Matrix: Routing under mobility in IoT, IoMT, and Social IoT. Ad Hoc Networks, 78, 84-98.

[63]. Kalpana, V., &Karthik,(2020), S. Route Availability with QoE and QoS Metrics for Data Analysis of Video Stream Over a Mobile Ad Hoc Networks. Wireless Personal Communications, 1-22.

[64]. Hammi, B., Zeadally, S., Labiod, H., Khatoun, R., Begriche, Y., &Khoukhi, L. (2020). A secure multipath reactive protocol for routing in IoT and HANETs. Ad Hoc Networks, 102118.

[65]. Sánchez-García, R. J. (2020). Exploiting symmetry in network analysis. Communications Physics, 3(1), 1-15.

[66]. Hayashi, Y., & Uchiyama, N. (2018). Onion-like networks are both robust and resilient. Scientific reports, 8(1), 1-13.

[67]. Allimuthu, U, K.Mahalakshmi " Efficient Object-Route Interaction for Finding Old Unused Scrap Car in Coimbatore Municipality." J. Adv. Res. Dyn. Control Syst.(10-Special) (2018): 984-988.

[68]. Allimuthu, U, K.Mahalakshmi. "Observed Survey on Efficient Route Interaction of Mobile Nodes in MANET." J. Adv. Res. Dyn. Control Syst.(10-Special) (2018): 952-965.

[69]. T. D. S. Keerthi and P. Venkataram, "Locating the Attacker of Wormhole Attack by Using the Honeypot," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, 2012, pp. 1175-1180, doi: 10.1109/TrustCom.2012.196.

Figures

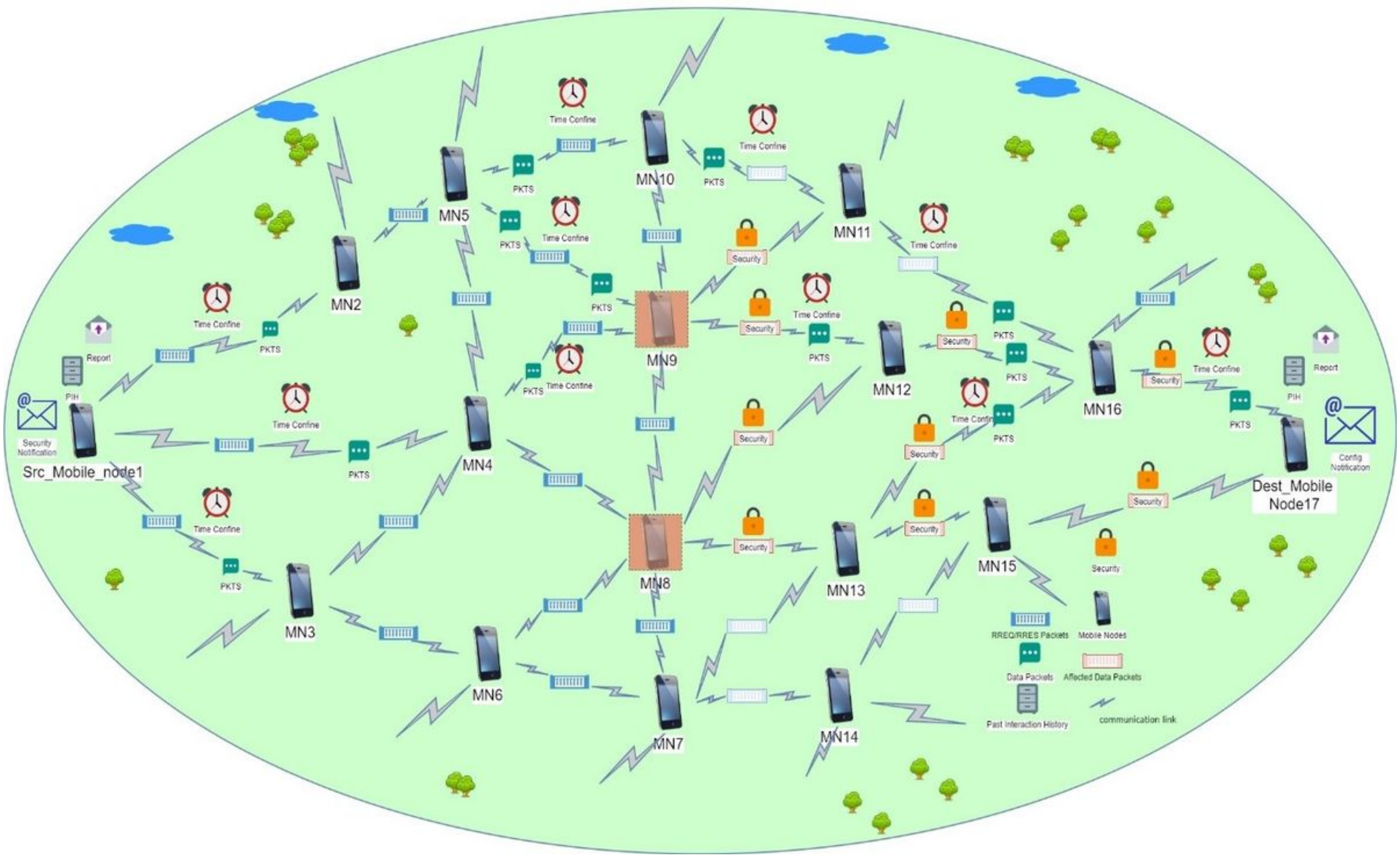


Figure 1

Simulation of MANET Routing protocols communication and rushing attack scenario for 17 nodes with the accommodative procedure

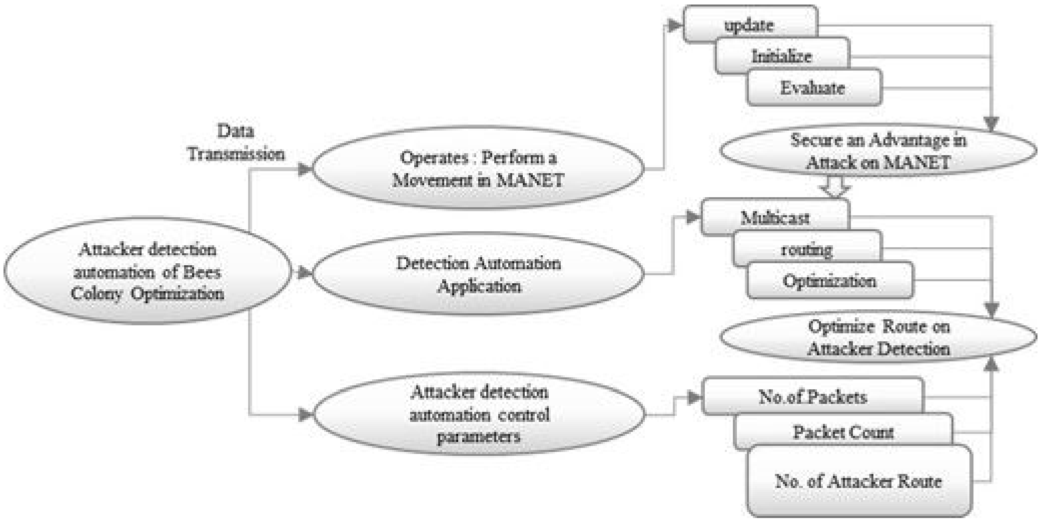

Attacker detection automation of Bees Colony Optimization
Data Transmission
Operates : Perform a Movement in MANET
Detection Automation Application
Attacker detection automation control parameters
update
Initialize
Evaluate
Secure an Advantage in Attack on MANET
Multicast
routing
Optimization
Optimize Route on Attacker Detection
No.of Packets
Packet Count
No. of Attacker Route

Figure 2

Activities of attacker detection automation of Bees Colony Optimization (ADABCP) on participated mobile nodes based routing algorithms for route optimization in mobile ad hoc networks.

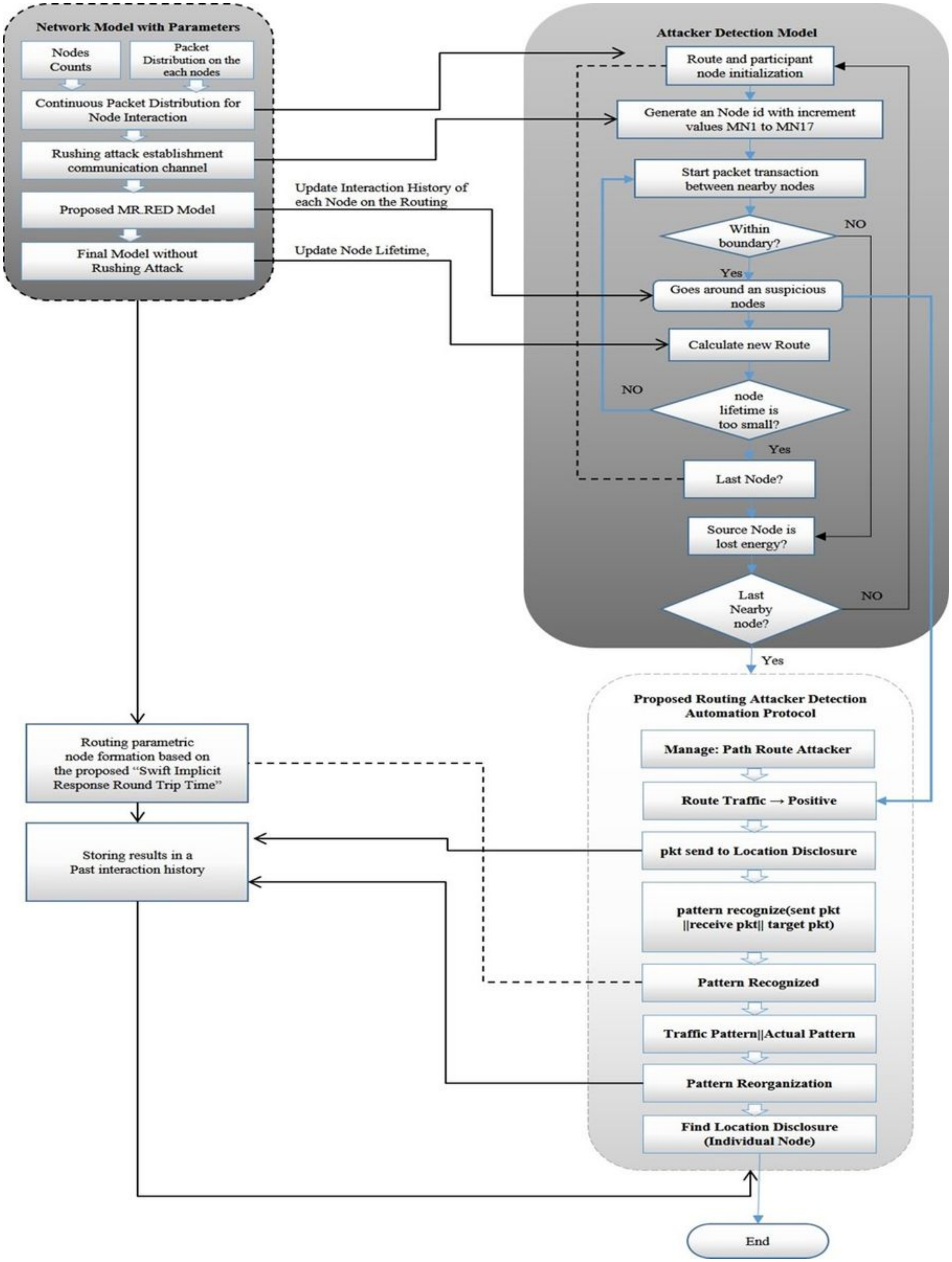

Network Model with Parameters
Nodes Counts
Packet Distribution on the each nodes
Continuous Packet Distribution for Node Interaction
Rushing attack establishment communication channel
Proposed MR.RED Model
Final Model without Rushing Attack
Update Interaction History of each Node on the Routing
Update Node Lifetime,
Attacker Detection Model
Route and participant node initialization
Generate an Node id with increment values MN1 to MN17
Start packet transaction between nearby nodes
Within boundary?
NO
Yes
Goes around an suspicious nodes
Calculate new Route
NO
node lifetime is too small?
Yes
Last Node?
Source Node is lost energy?
Last Nearby node?
NO
Yes
Proposed Routing Attacker Detection Automation Protocol
Manage: Path Route Attacker
Route Traffic → Positive
pkt send to Location Disclosure
pattern recognize(sent pkt ||receive pkt|| target pkt)
Pattern Recognized
Traffic Pattern||Actual Pattern
Pattern Reorganization
Find Location Disclosure (Individual Node)
Routing parametric node formation based on the proposed "Swift Implicit Response Round Trip Time"
Storing results in a Past interaction history
End

Figure 3

Flow diagram of the proposed attacker detection automation algorithm

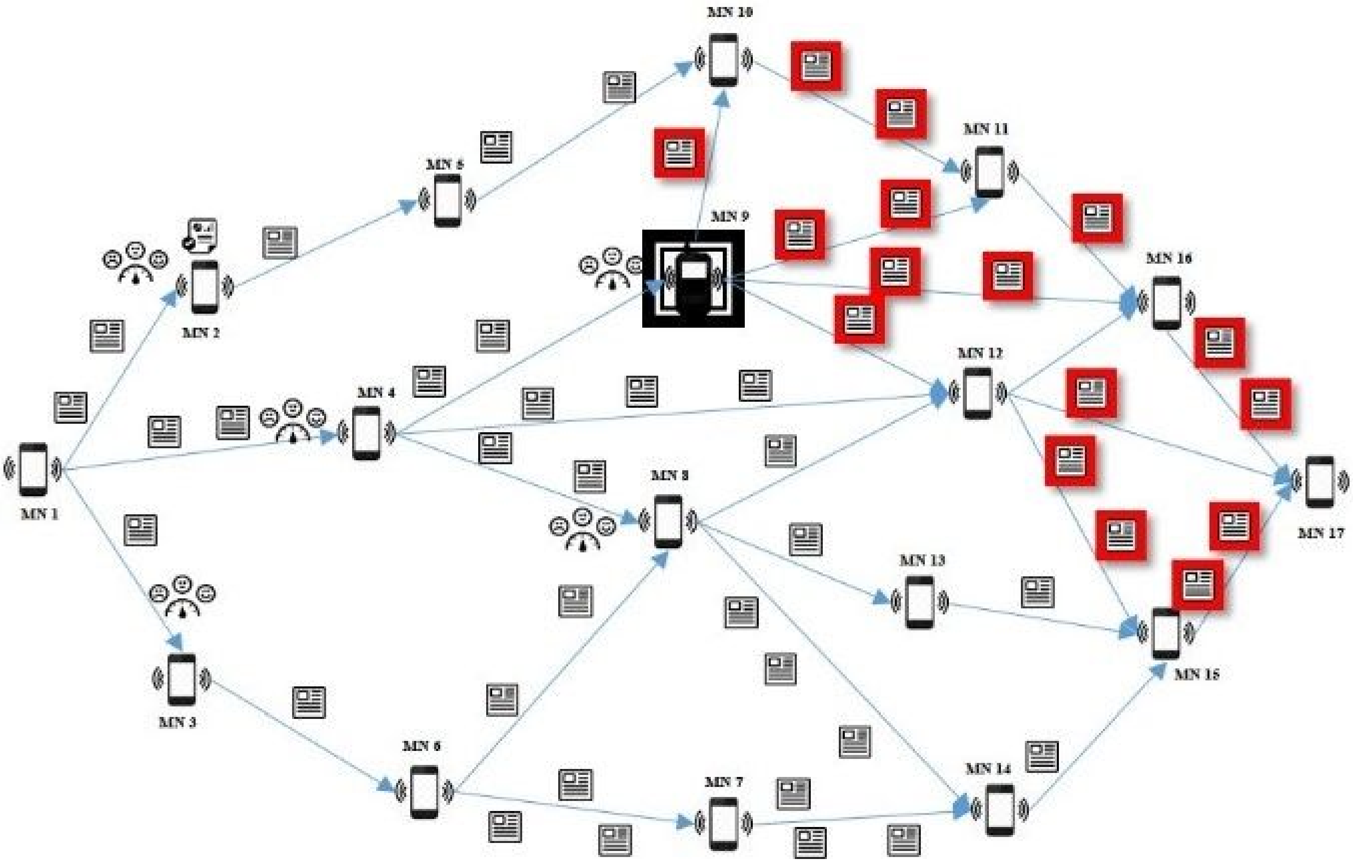


Figure 4

Example interconnected system clarifies the rushing attack after successive route request/route reply. The block highlighted nodes describes the rushing attack scenario on attacker detection automation of bees colony optimization protocol.

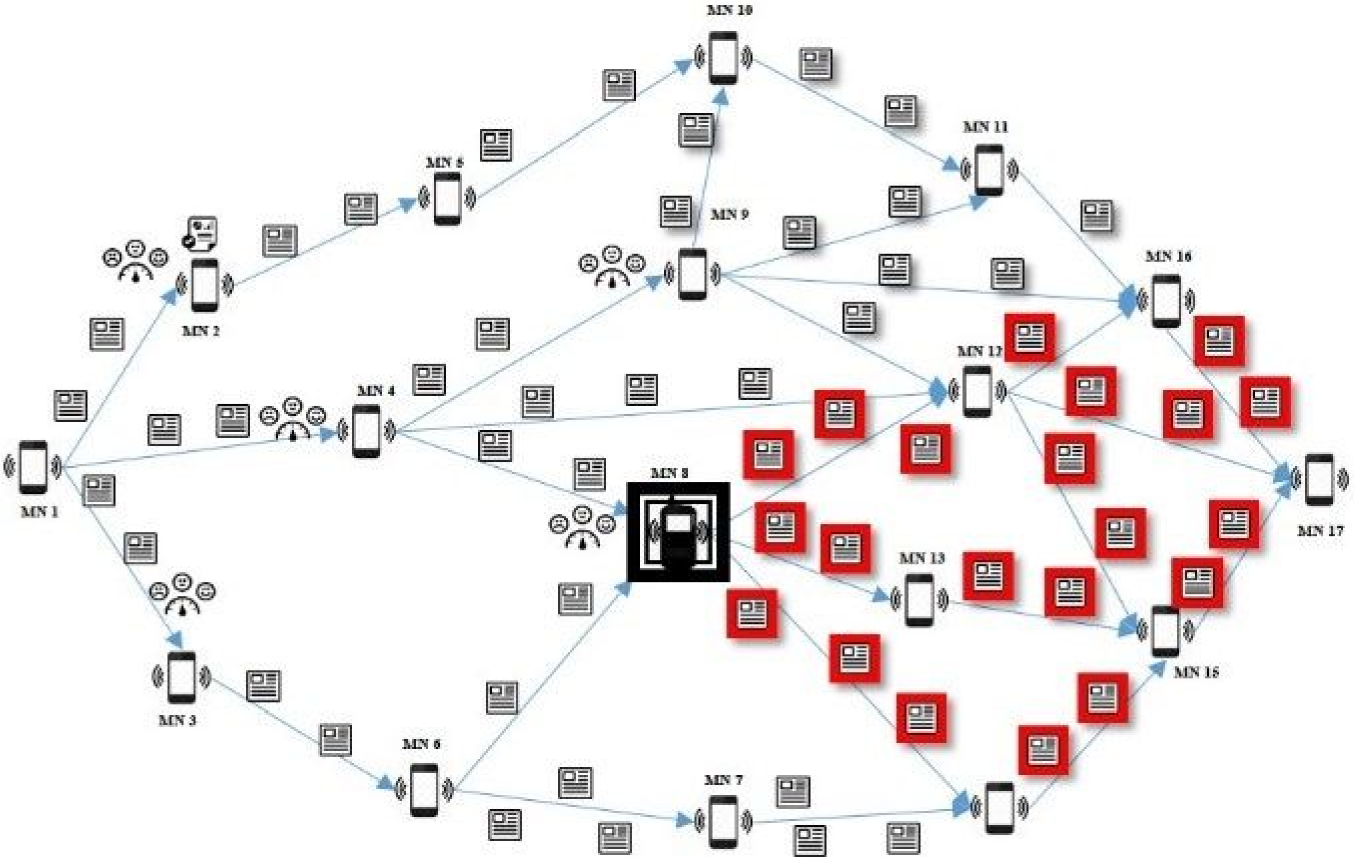


Figure 5

The above figure clarifies by giving an example of another rushing attack on the same network. The block highlighted nodes describes the rushing attack scenario on attacker detection automation of bees colony optimization protocol. The verification confirmation used to detect the rushing attack on this scenario based on the attacker detection automation of bees colony optimization protocol

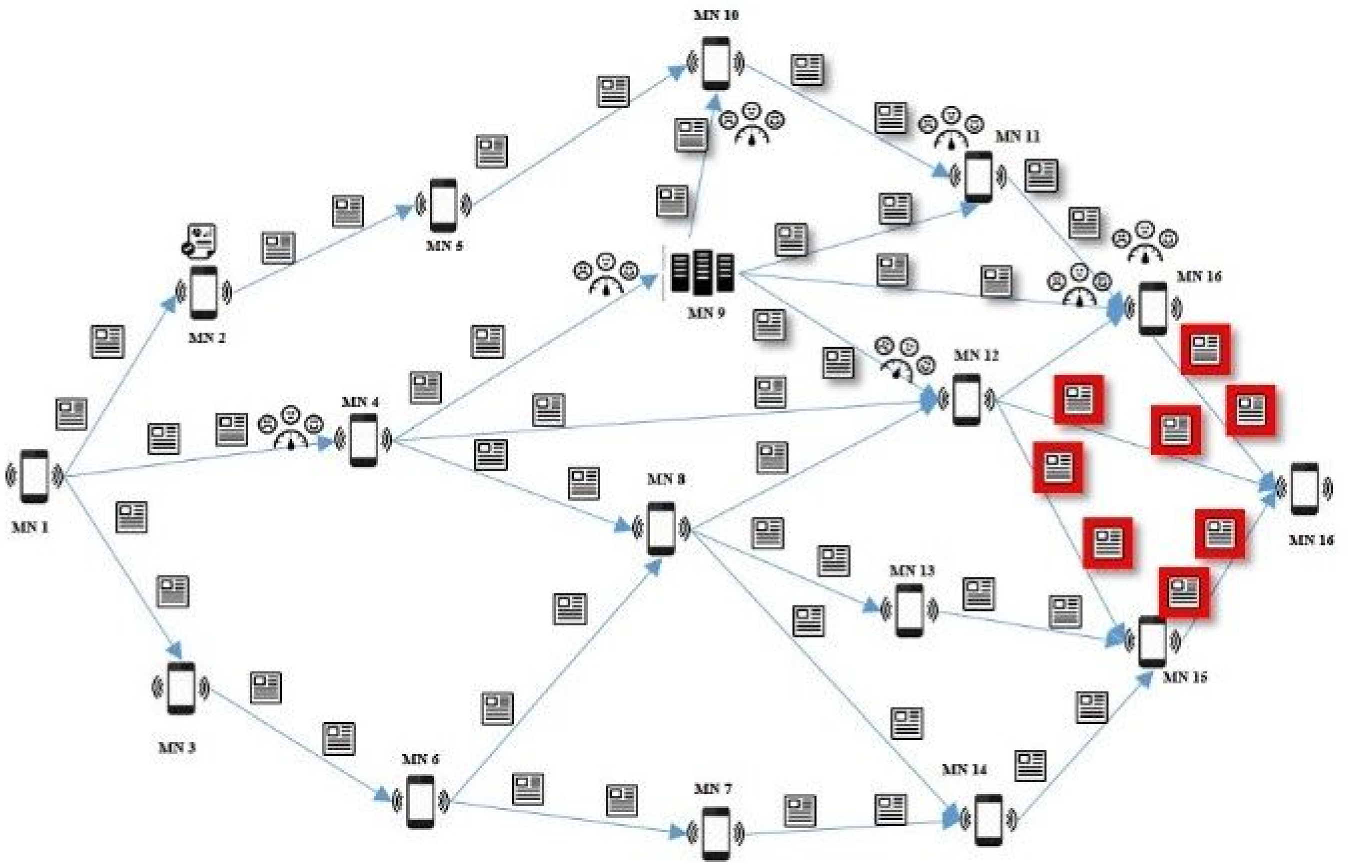


Figure 6

Detecting and removing malicious nodes with the multicast routing protocol with the neighbor node selection at the presence of rushing node at near source

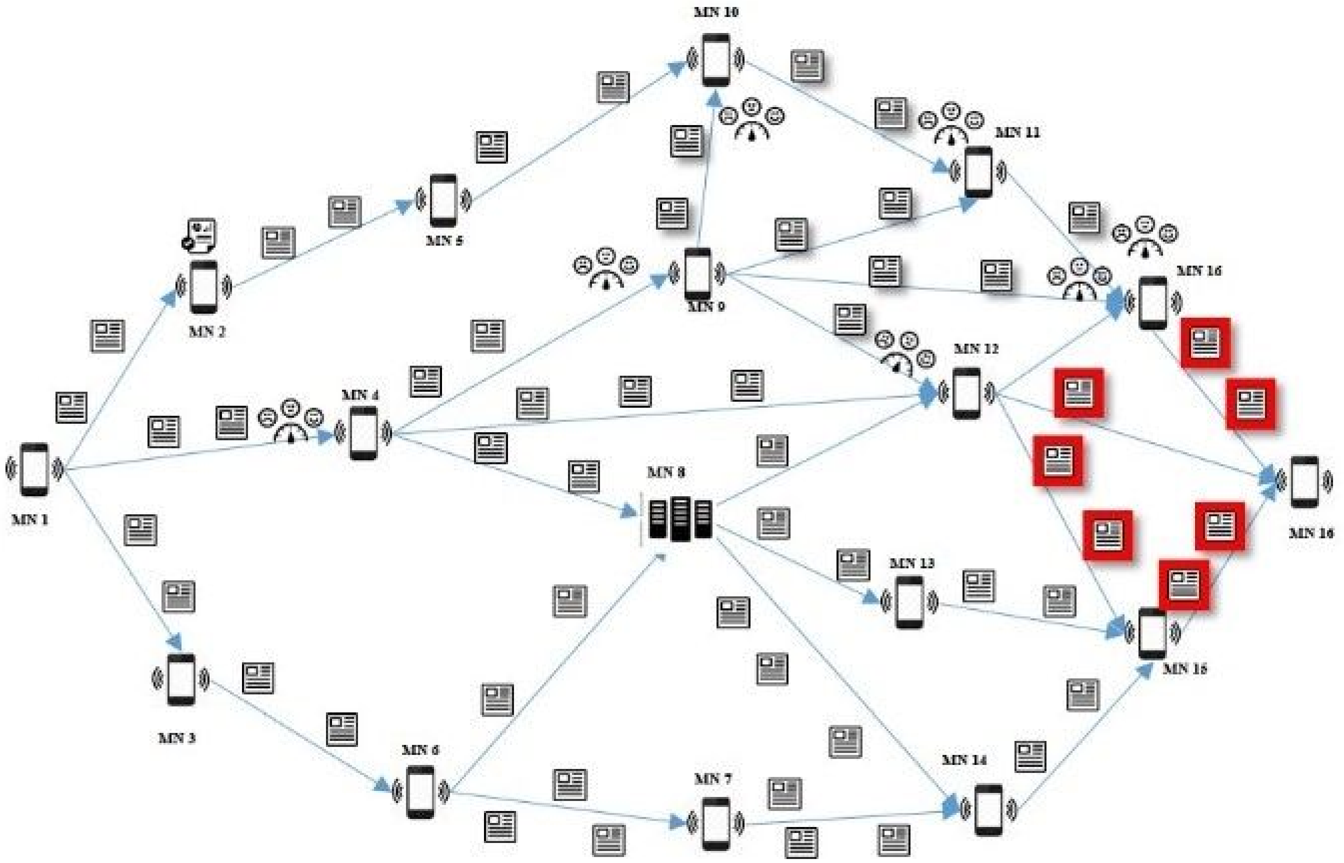


Figure 7

rushing attack prevention for MANET using random route selection to make attacker detection automation more efficient. A set of malicious nodes is rushing anywhere within the network.

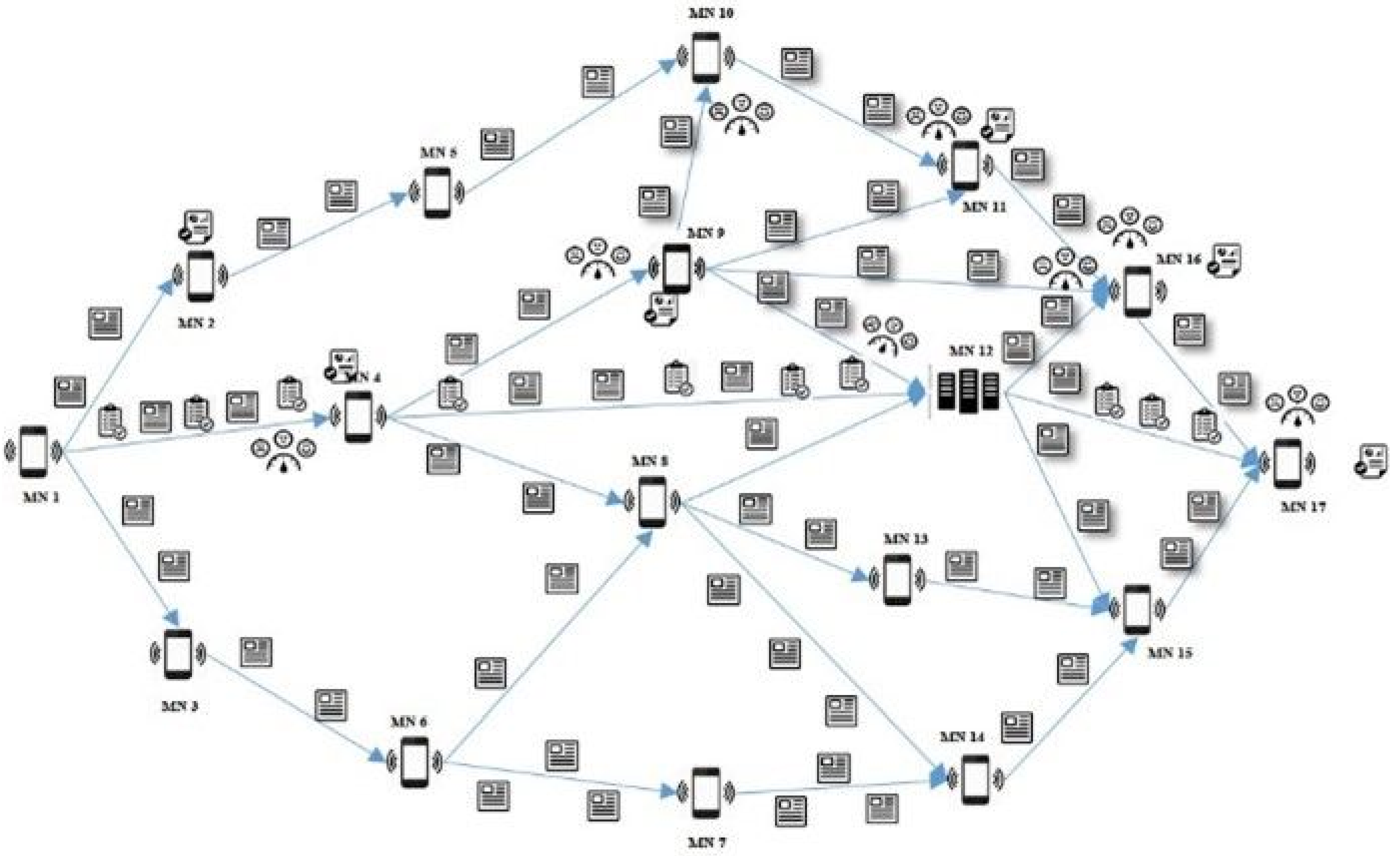


Figure 8

Our combined mechanisms to secure route discovery protocol against the rushing attack. The topology of an Optimum route selection in MANET after invoking early route detection with final multicast tree

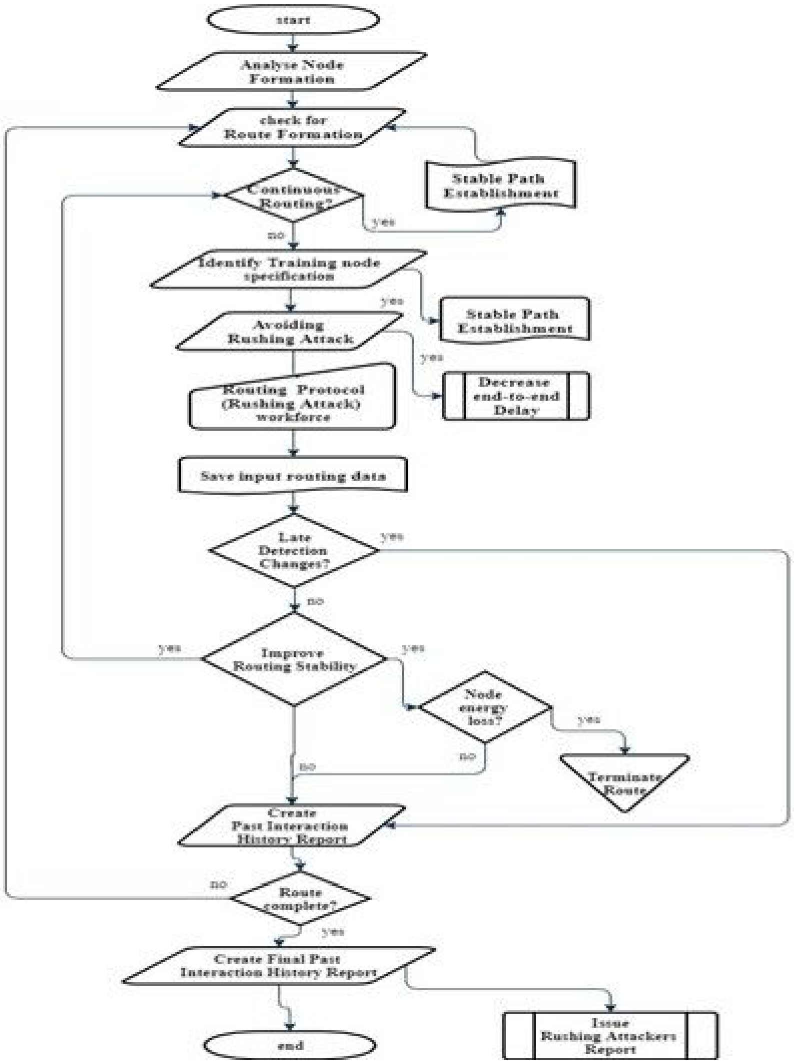

start
Analyse Node Formation
check for Route Formation
Stable Path Establishment
Continuous Routing?
yes
no
Identify Training node specification
yes
Stable Path Establishment
Avoiding Rushing Attack
yes
Decrease end-to-end Delay
Routing Protocol (Rushing Attack) workforce
Save input routing data
Late Detection Changes?
yes
no
yes
Improve Routing Stability
yes
Node energy loss?
yes
no
no
Terminate Route
Create Past Interaction History Report
no
Route complete?
yes
Create Final Past Interaction History Report
end
Issue Rushing Attackers Report

Figure 9

Flowchart of proposed MANET convergence scenario in the Swift Implicit Response Round Trip Time

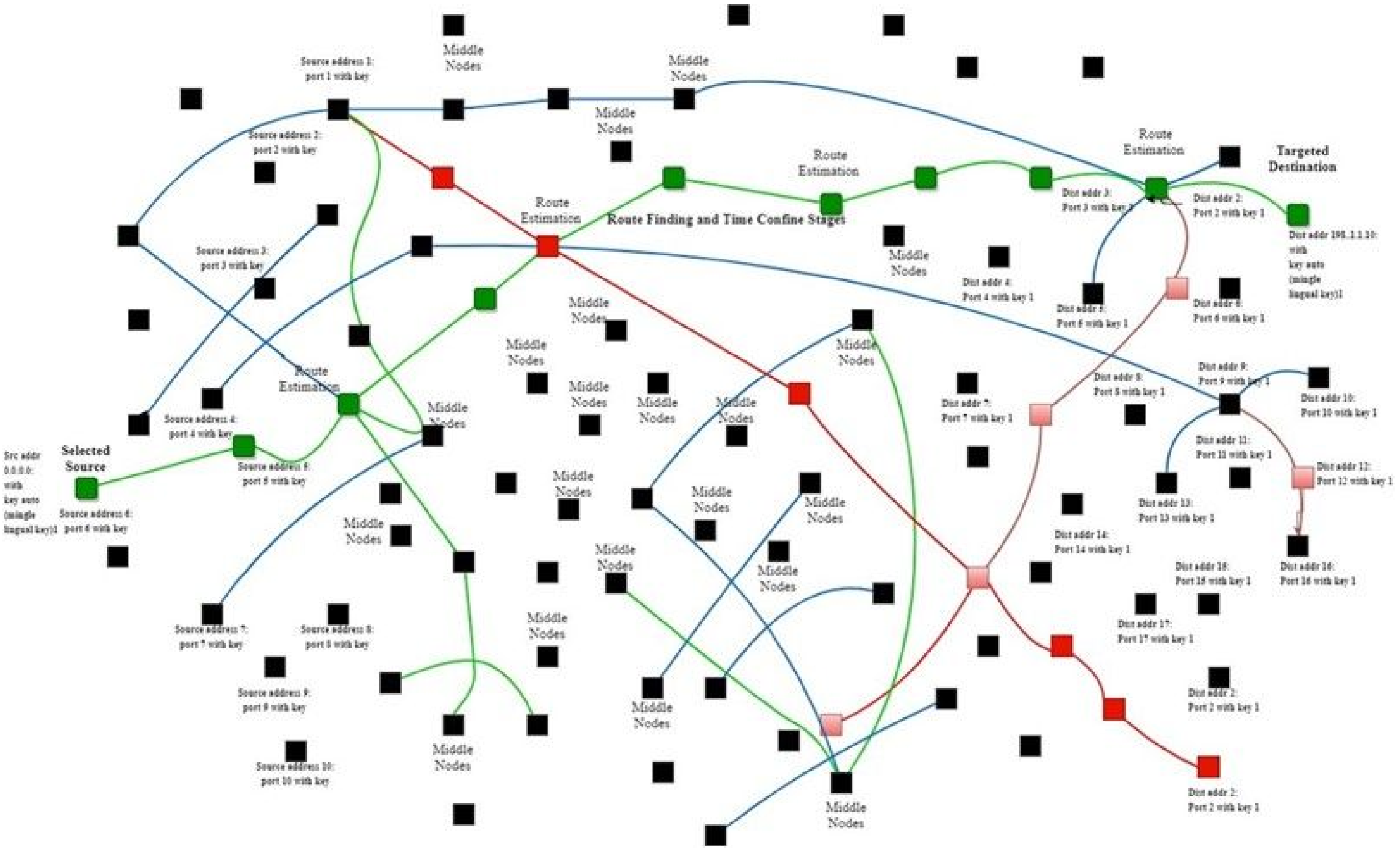

Middle Nodes
Source address 1: port 1 with key
Source address 2: port 2 with key
Source address 3: port 3 with key
Source address 4: port 4 with key
Source address 5: port 5 with key
Source address 6: port 6 with key
Source address 7: port 7 with key
Source address 8: port 8 with key
Source address 9: port 9 with key
Source address 10: port 10 with key
Selected Source
Src addr 0.0.0.0: with key auto (mingle lingual key)1
Route Estimation
Route Finding and Time Confine Stages
Targeted Destination
Dist addr 198..1.1.10: with key auto (mingle lingual key)1
Dist addr 2: Port 2 with key 1
Dist addr 3: Port 3 with key 1
Dist addr 4: Port 4 with key 1
Dist addr 5: Port 5 with key 1
Dist addr 6: Port 6 with key 1
Dist addr 7: Port 7 with key 1
Dist addr 8: Port 8 with key 1
Dist addr 9: Port 9 with key 1
Dist addr 10: Port 10 with key 1
Dist addr 11: Port 11 with key 1
Dist addr 12: Port 12 with key 1
Dist addr 13: Port 13 with key 1
Dist addr 14: Port 14 with key 1
Dist addr 15: Port 15 with key 1
Dist addr 16: Port 16 with key 1
Dist addr 17: Port 17 with key 1

Figure 10

Conceptual framework and proposed rushing attacker route structure, functionalities and processing model packet data transmission with route finding and time confine

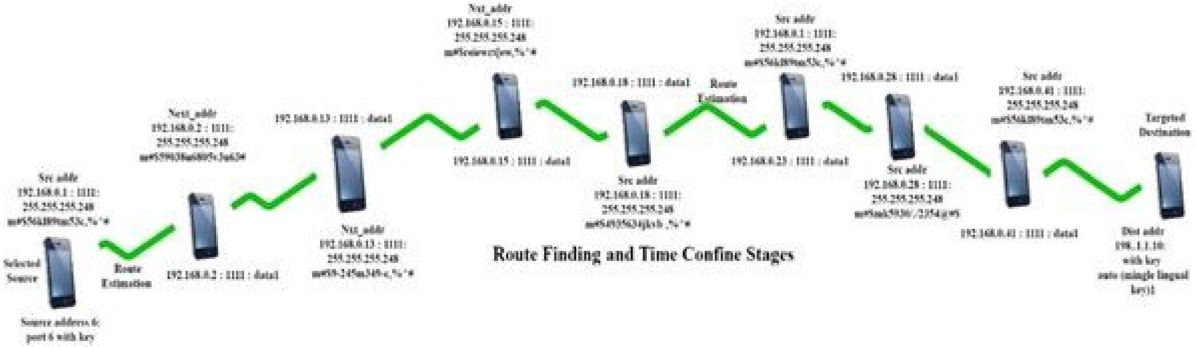

Src addr 192.168.0.1 : 1111: 255.255.255.248
Selected Source
Source address 6: port 6 with key
Route Estimation
Next_addr 192.168.0.2 : 1111: 255.255.255.248
192.168.0.2 : 1111 : data1
192.168.0.13 : 1111 : data1
Nxt_addr 192.168.0.13 : 1111: 255.255.255.248
Nxt_addr 192.168.0.15 : 1111: 255.255.255.248
192.168.0.15 : 1111 : data1
192.168.0.18 : 1111 : data1
Src addr 192.168.0.18 : 1111: 255.255.255.248
Route Estimation
Src addr 192.168.0.1 : 1111: 255.255.255.248
192.168.0.23 : 1111 : data1
192.168.0.28 : 1111 : data1
Src addr 192.168.0.28 : 1111: 255.255.255.248
Src addr 192.168.0.41 : 1111: 255.255.255.248
192.168.0.41 : 1111 : data1
Targeted Destination
Dist addr 198..1.1.10: with key auto (mingle lingual key)1
Route Finding and Time Confine Stages

Figure 11

Sender-receiver destination addresses status

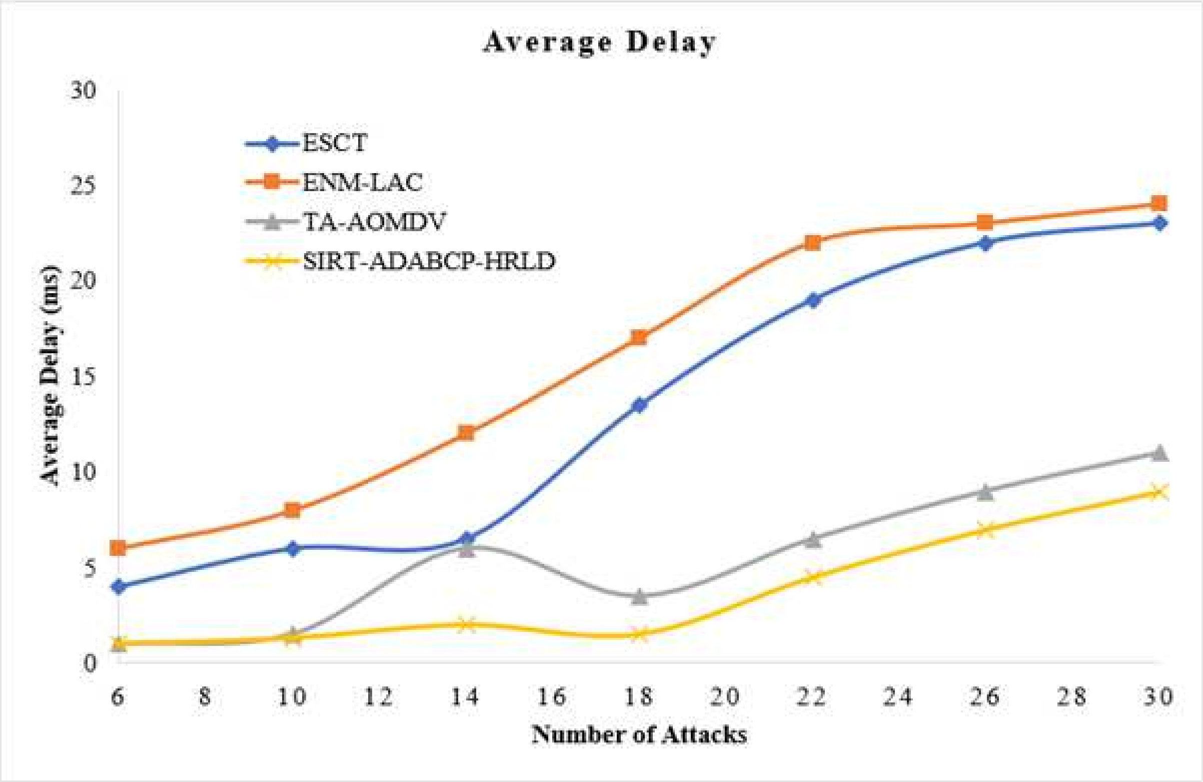


Figure 12

Graph for an end-to-end delay Vs. number of attackers

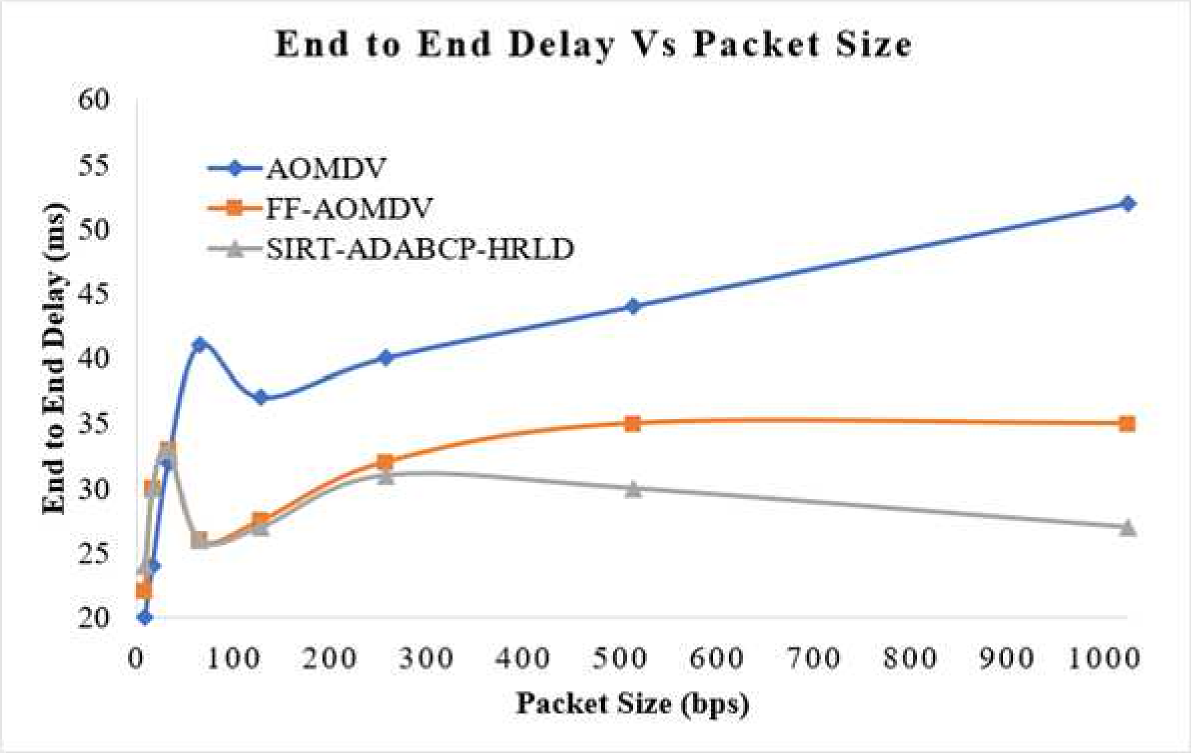


Figure 13

Graph for End to End Delay Vs. Packet Size

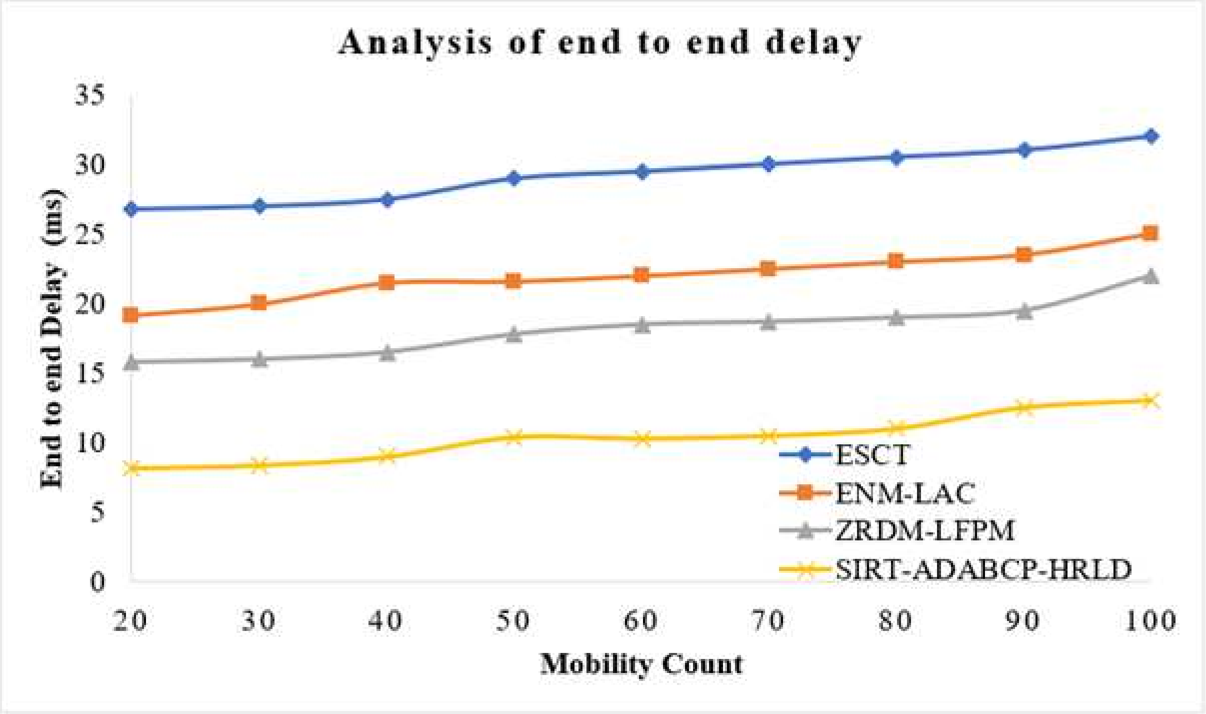


Figure 14

Graph for an end-to-end delay Vs. mobility count

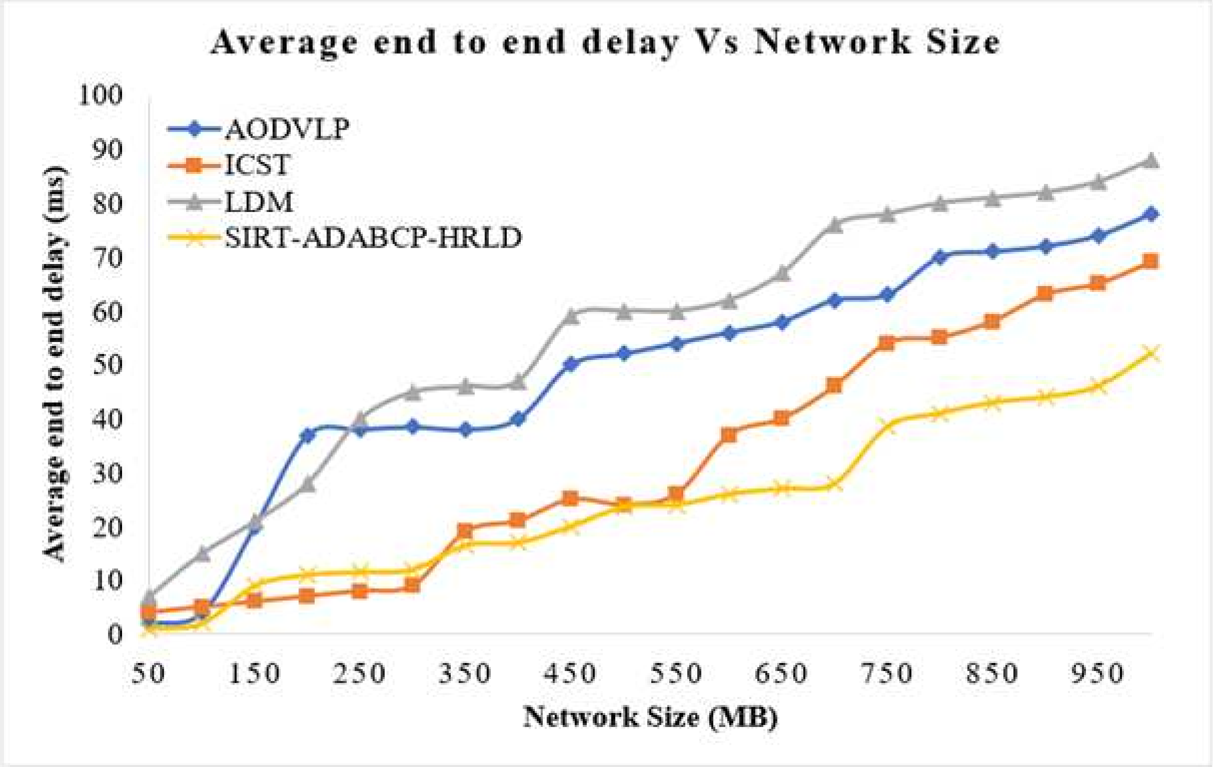


Figure 15

Graph for an end-to-end delay Vs. network size

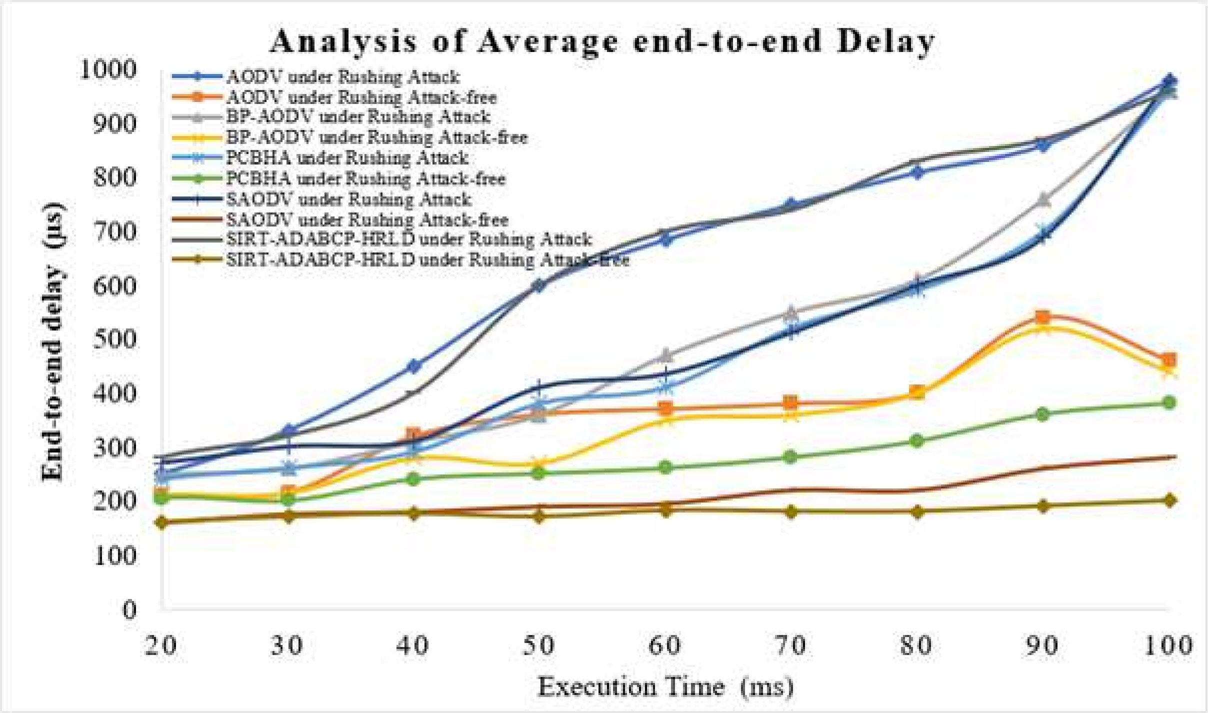


Figure 16

Consolidated performance result analysis of end-to-end delay

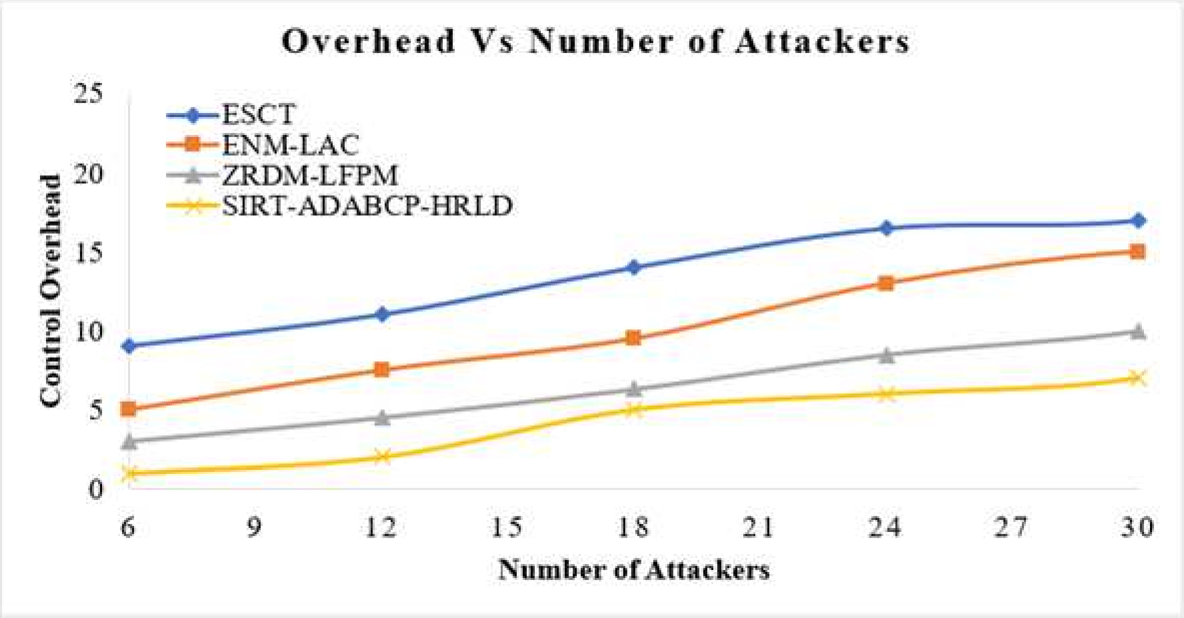


Figure 17

Graph for communication overhead Vs. number of attackers

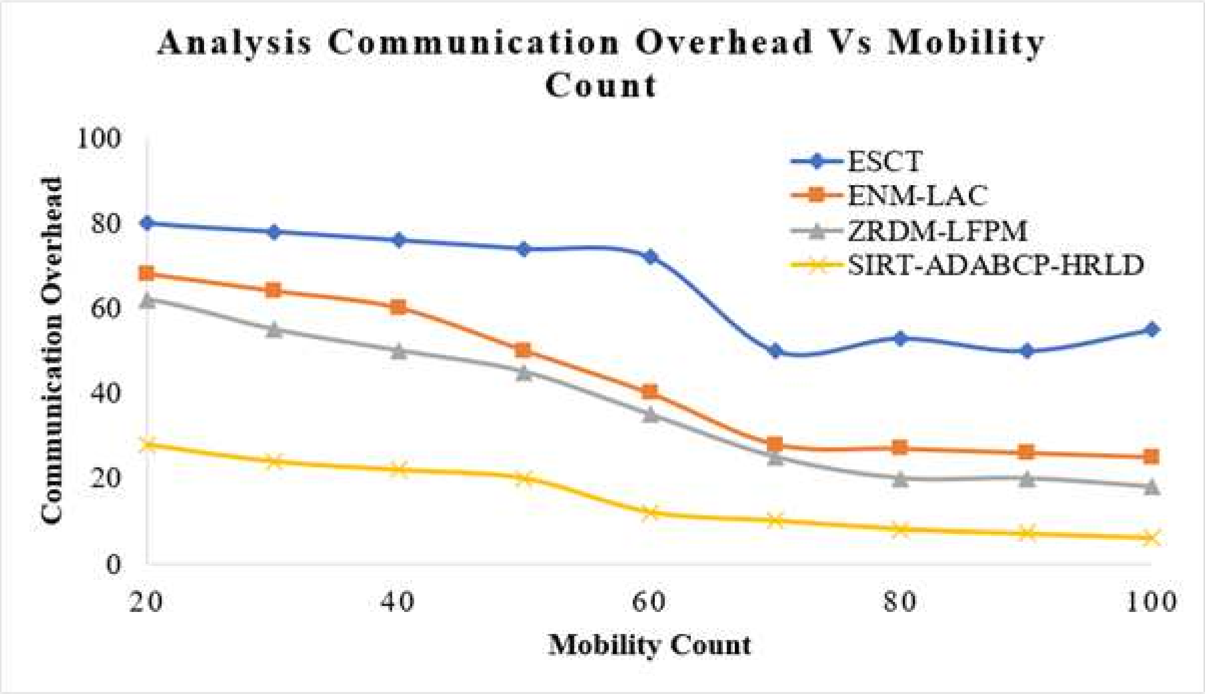


Figure 18

Graph for communication overhead Vs. mobility count

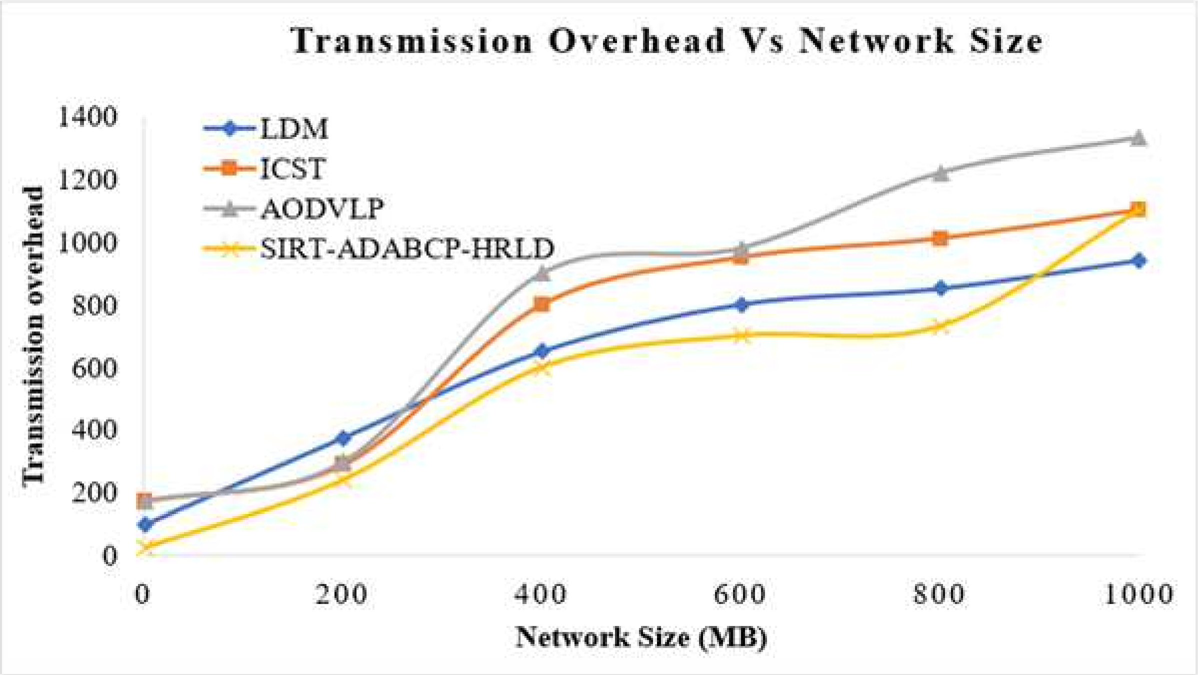


Figure 19

Graph for transmission overhead Vs. network size

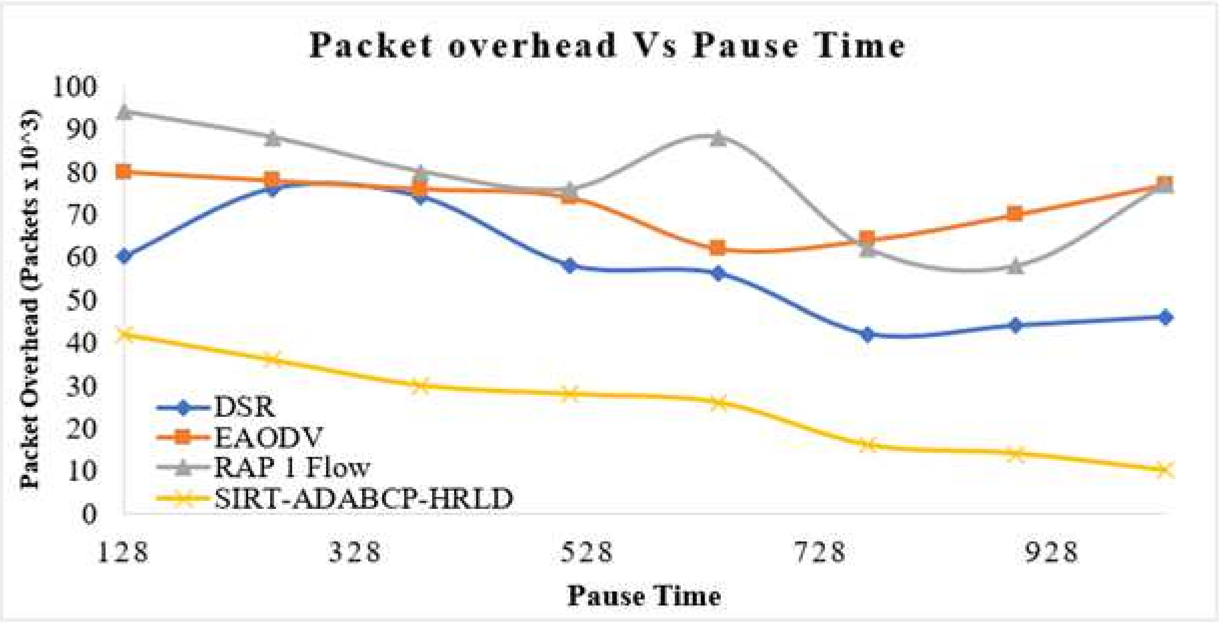


Figure 20

Graph for communication overhead Vs. network lifetime

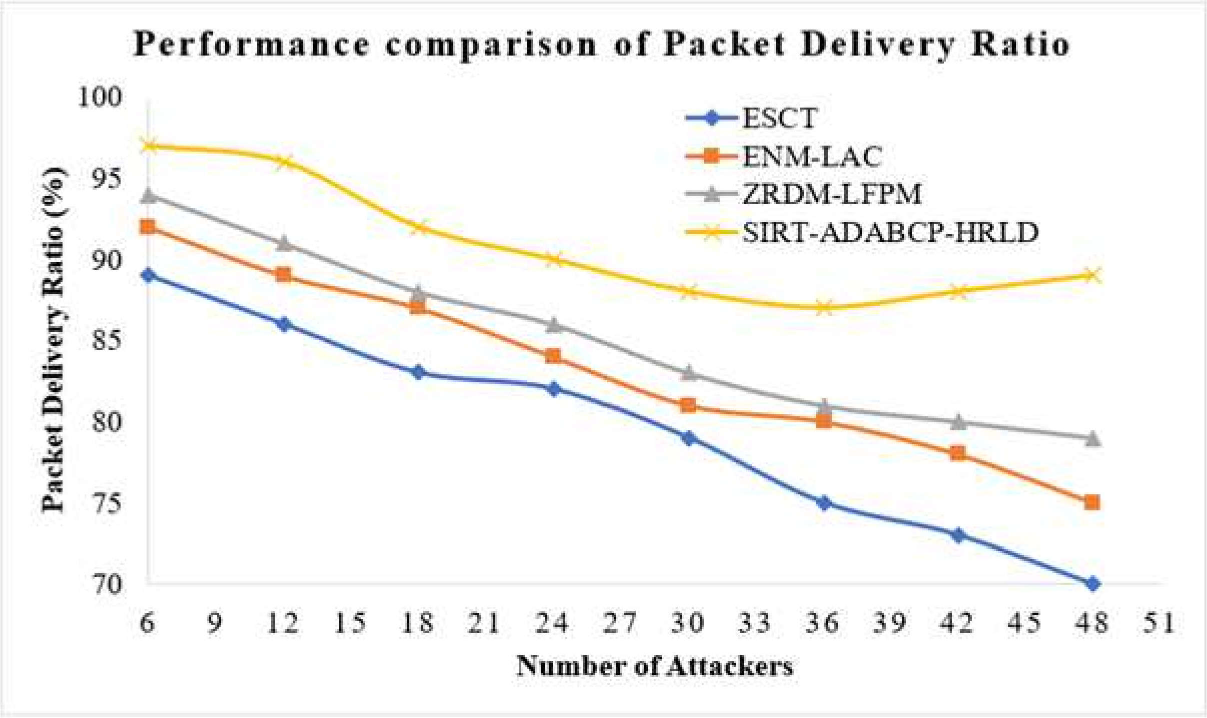


Figure 21

Graph for packet delivery ratio Vs. number of attackers

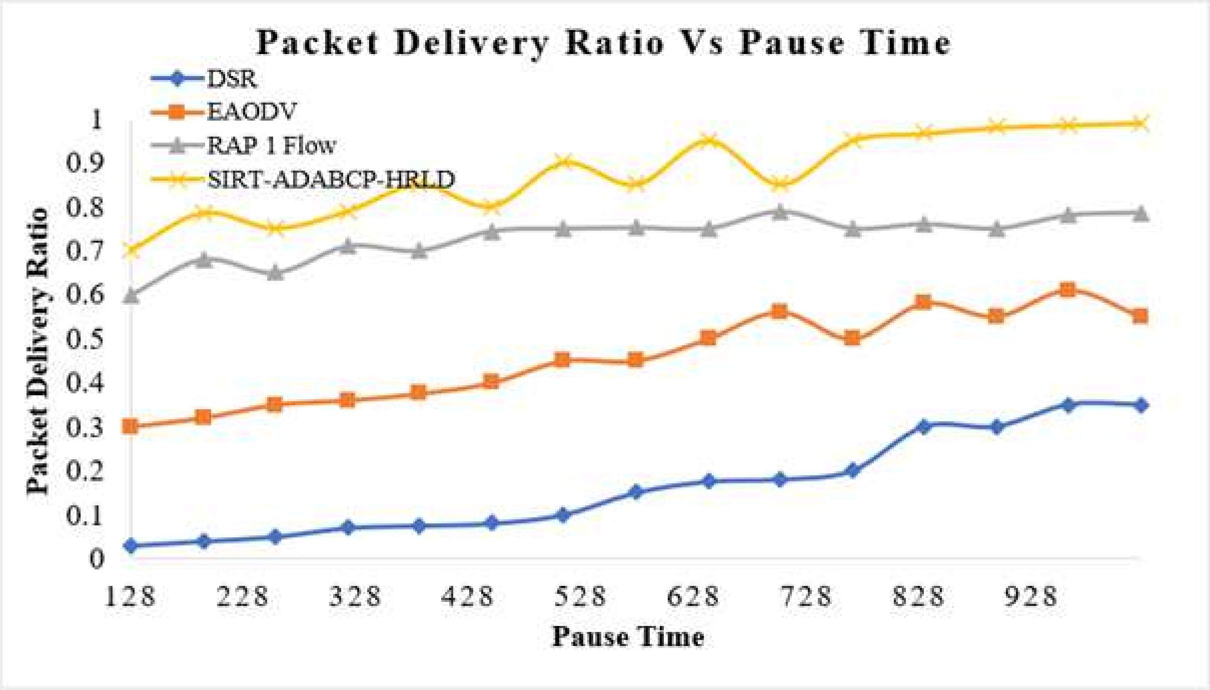


Figure 22

Graph for Packet Delivery Ratio Vs. Network Lifetime

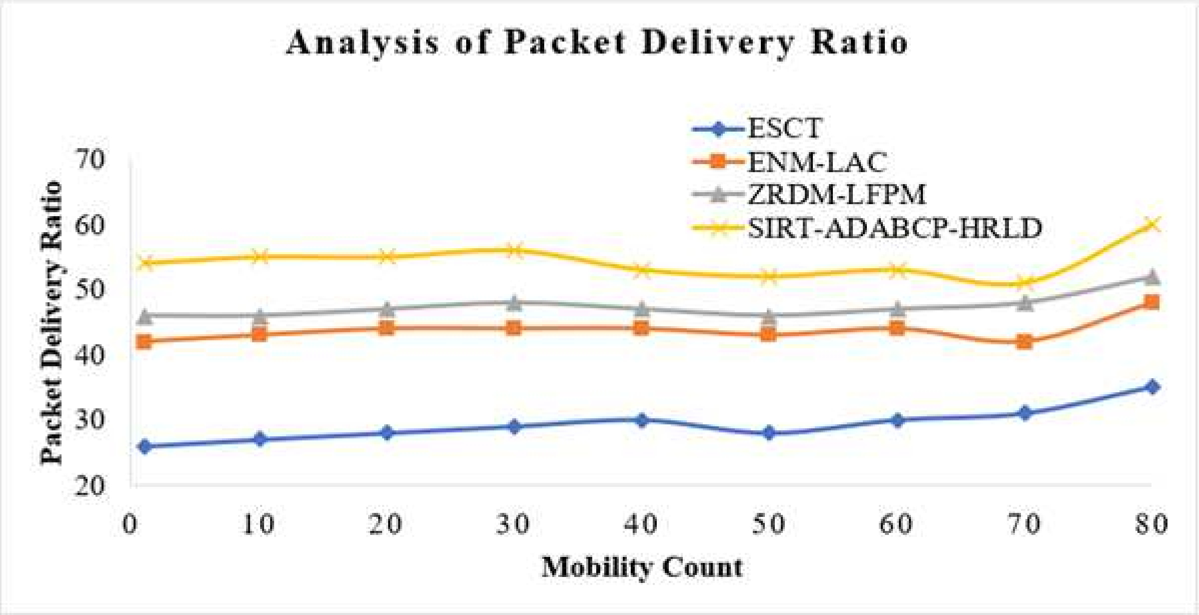


Figure 23

Graph for packet delivery ratio Vs. mobility count

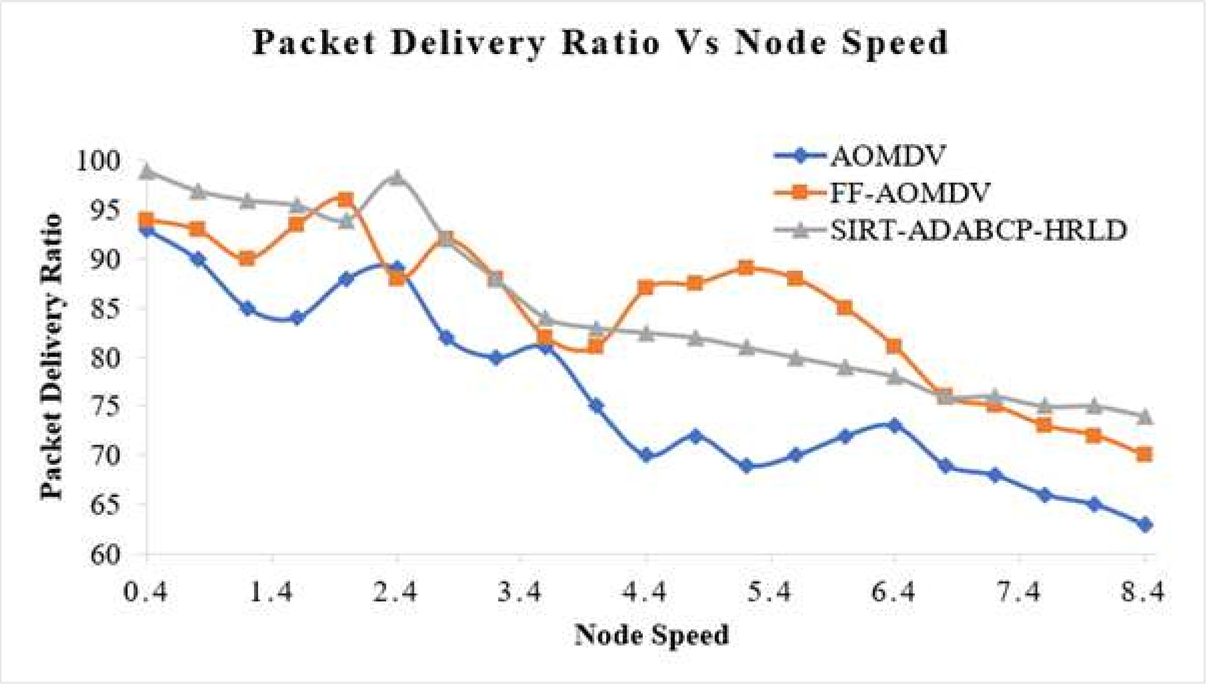


Figure 24

Graph for Packet Delivery Ratio Vs. Node Speed

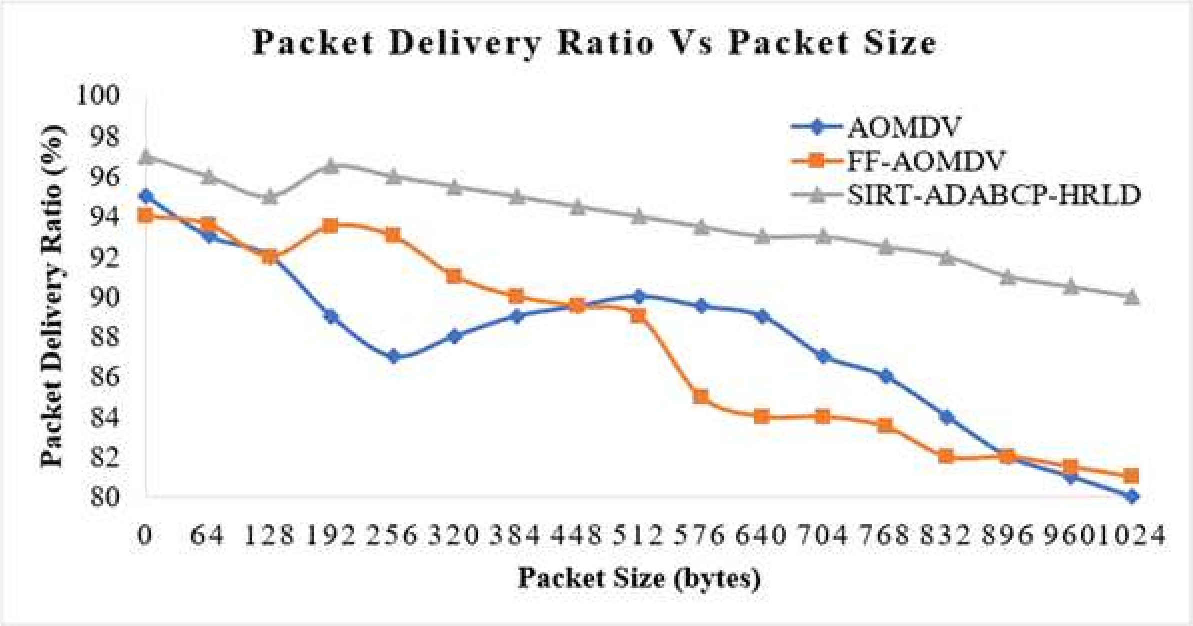


Figure 25

Graph for packet delivery ratio Vs. packet size

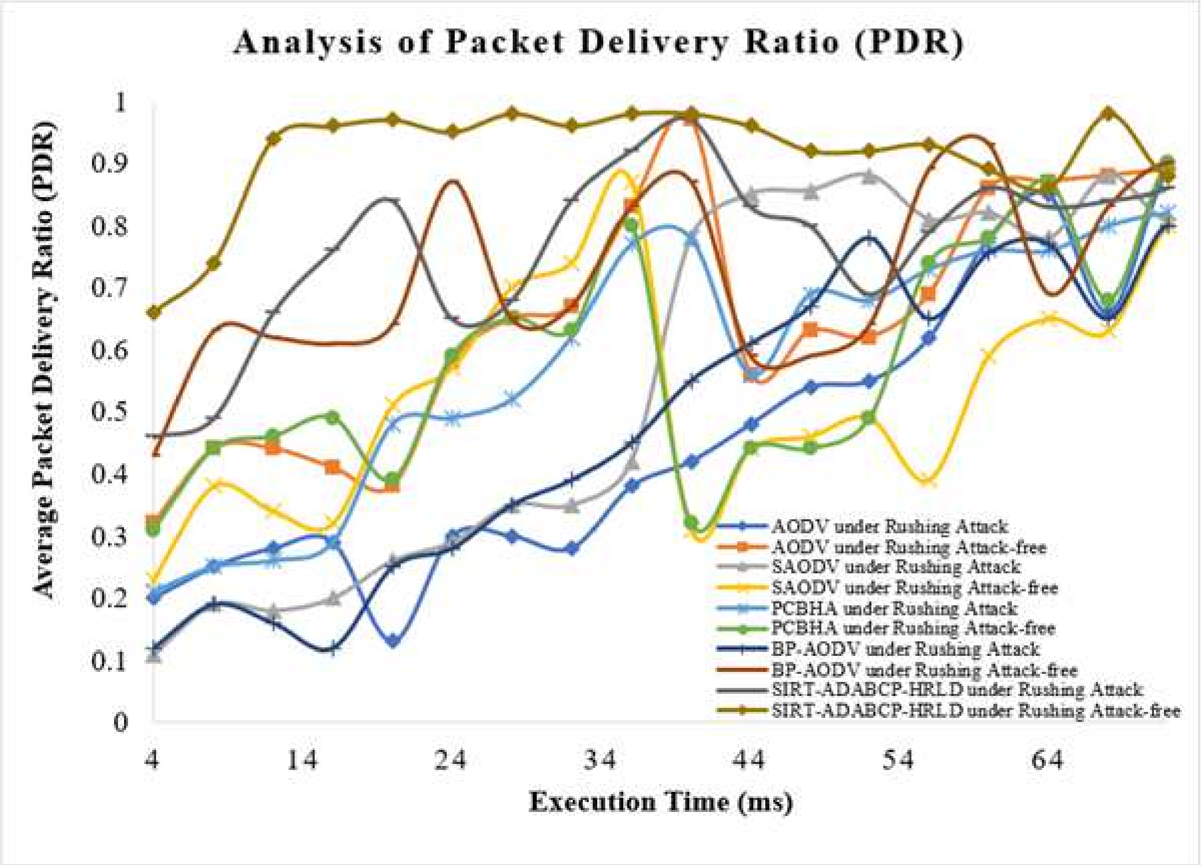


Figure 26

Performance result analysis of Packet Delivery Ratio (PDR)

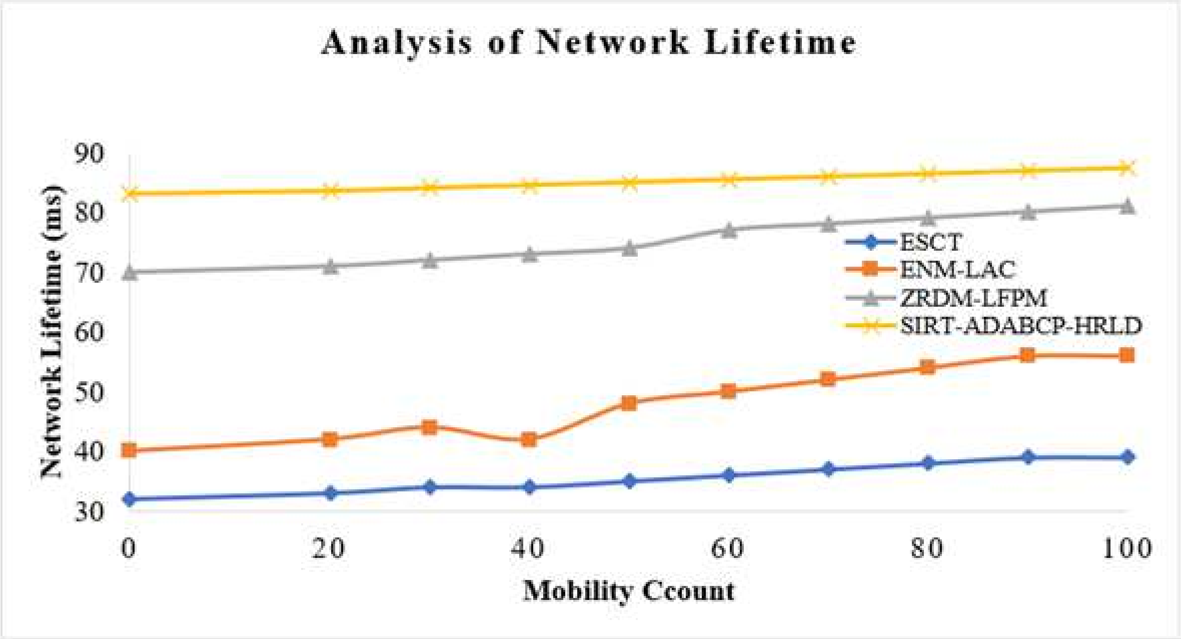


Figure 27

Graph for network lifetime Vs. mobility count

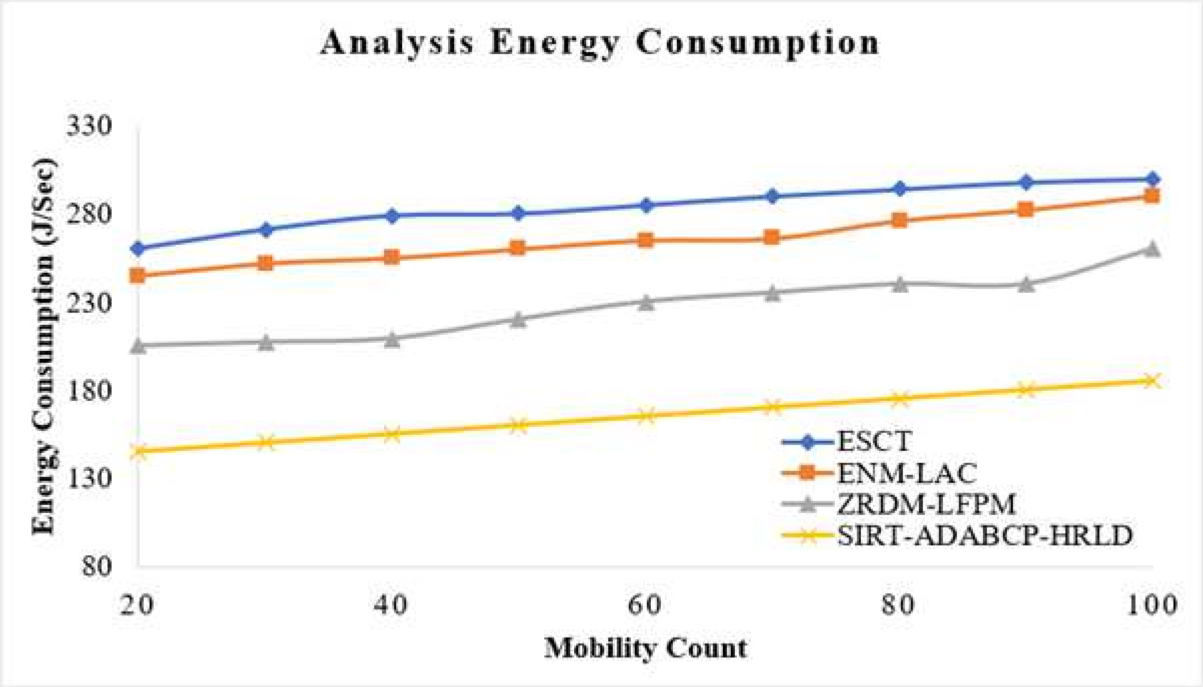


Figure 28

Graph for Energy Consumption Vs. Mobility Count

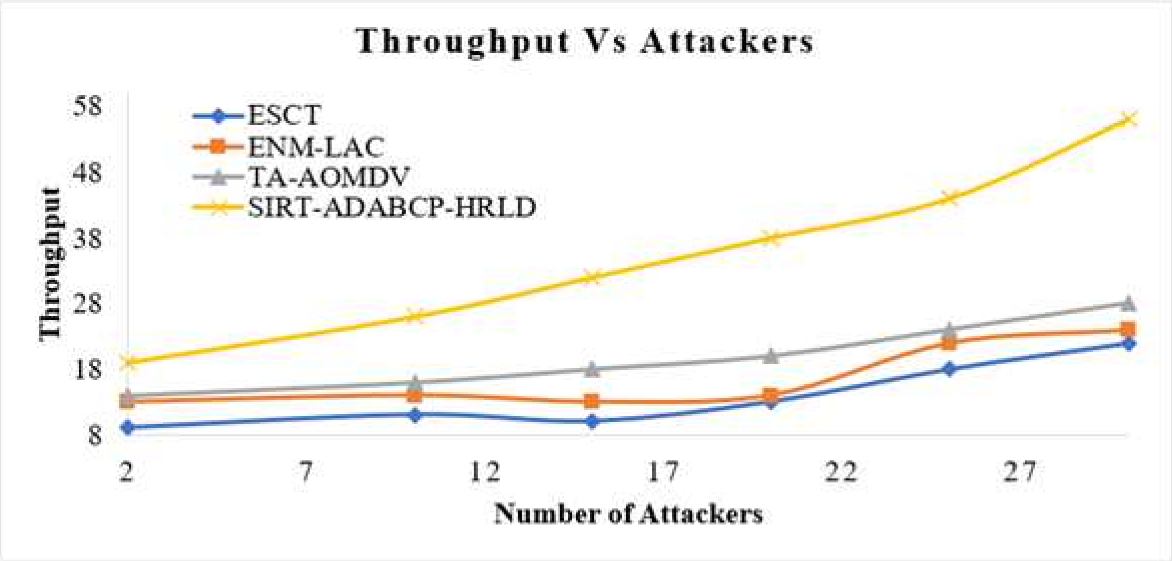


Figure 29

Graph for throughput Vs. attackers

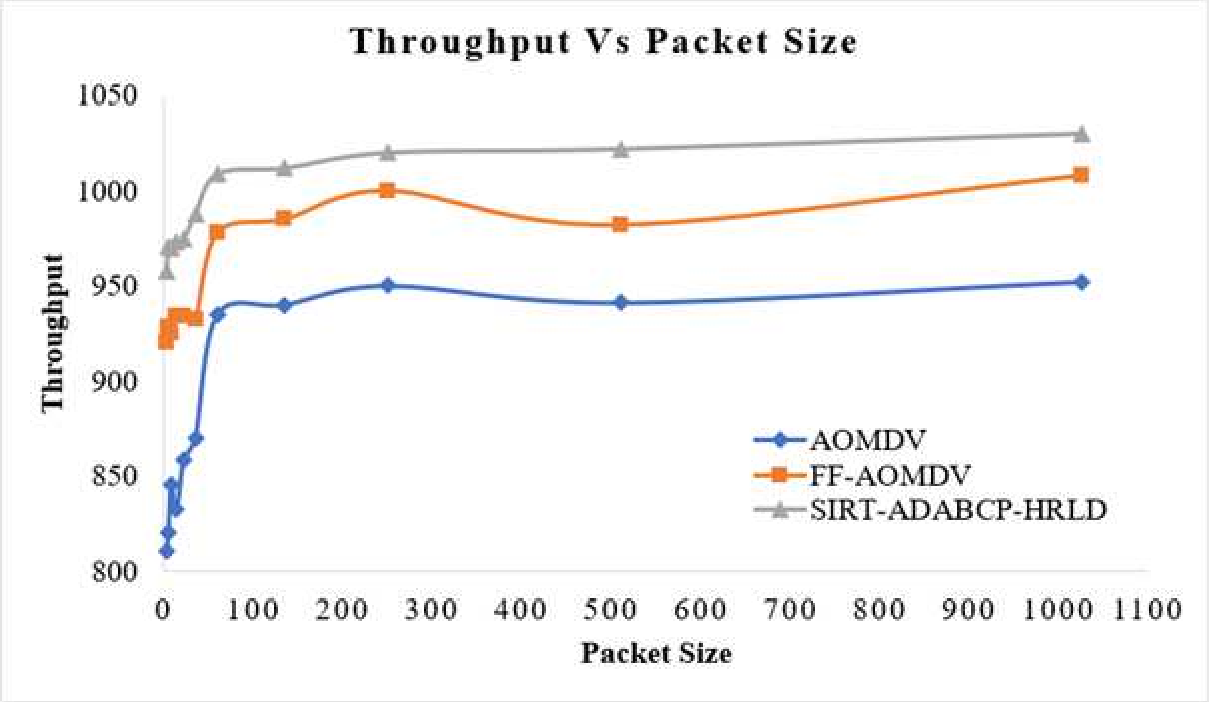


Figure 30

Graph for throughput Vs. packet size

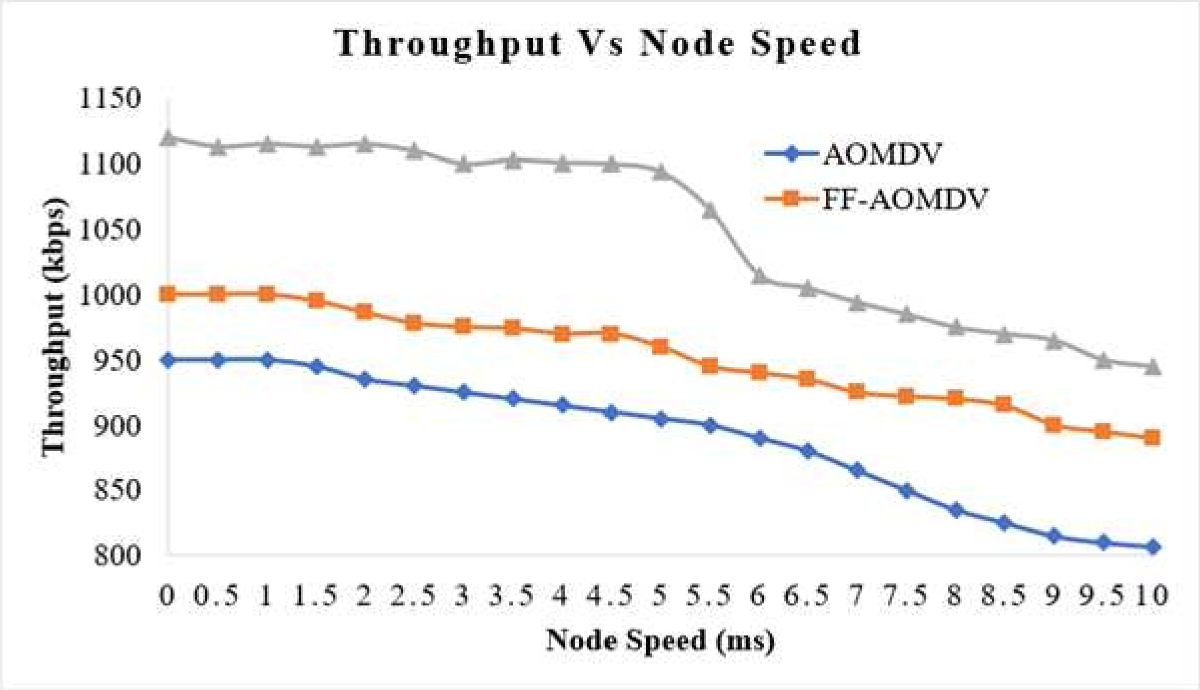


Figure 31

Graph for throughput Vs. node speed

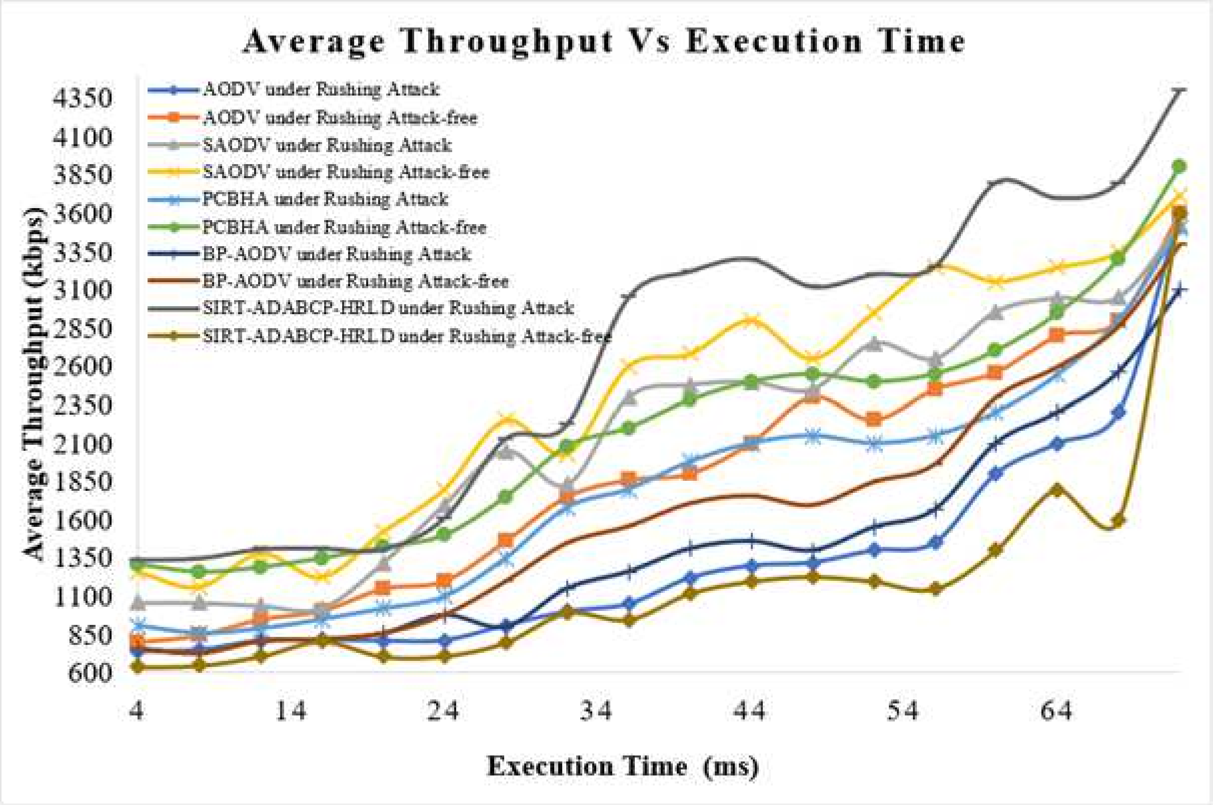


Figure 32

Performance result analysis of for throughput