Intelligent route discovery towards rushing attacks in ad hoc wireless networks

Udayakumar Allimuthu1 · K. Mahalakshmi2

Received: 29 October 2020 / Accepted: 25 March 2021 / Published online: 9 April 2021
© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

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, 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. 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 · 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.
network, in which the process will be suspended (delay) for entire data transmission (Balaji et al. 2019; Djedjig et al. 2020). 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 to evaluate the attacker-less network infrastructure (Hahn et al. 2019). 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 parallel to update the dead node and active links (Al-Zahrani 2020; Alzamzami and Mahmood 2020). 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 (Cai et al. 2018), zone-based route discovery mechanism—a link failure prediction mechanism (ZRDM-LFPM) (Khudayer et al. 2020), and evolving network model based on local-area choice (ENM-LAC) approaches (Bai et al. 2017). 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 (Bozorgi et al. 2017; Amutha and Balasubramanian 2018; Khudayer et al. 2020). 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, Sect. 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, Sect. 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 conditions 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 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. The
### Table 1  Fundamental commitments of a various research survey

| Author (Year)       | Introduction or Background                                                                 | Aim or purpose or objective                                                                 | Existing research works                                                                                      | Overcome this problem                                      | Proposed approaches                                                                 | Technology/methodology                                                                 | Data analysis                                                                 |
|---------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------|
| Li and Wu (2017)    | Optimized link state routing scheme                                                       | Smooth mobility and link reliability-based OLSR (SMLR OLSR)                                 | Semi-Markov smooth and complexity restricted mobility model (SMS CR)                                        | Reliability enhanced multi point relay (MPR) selection in SMLR OLSR | Accurate performance analysis, and can achieve longer MPR lifetime and less control overhead | Multi point relay (MPR) Selection in SMLR OLSR                                     | NA                                                                                           |
| Hurley-Smith et al. (2017) | Pre-existing routing                                                                      | The flexibility and MANET increasing popular in a wide range of use cases                   | Less popular in a wide range of use cases                                                                    | Security protocols to protect routing and application data   | Secure routing and communication security protocols implemented to provide protection | Communication security protocols                                                  | Whilst for node authentication, access control, and communication security mechanism |
| Bai et al. (2017)   | Cooperative routing in MANET                                                              | Cooperative communication in MANET can improve system capacity and energy efficiency        | Lack of a systematically designed cooperative routing scheme                                                 | NA                                                          | NA                                                                                | NA                                                                                | NA                                                                                           |

| Author (Year)       | Introduction or Background                                                                 | Aim or purpose or objective                                                                 | Existing research works                                                                                      | Overcome this problem                                      | Proposed approaches                                                                 | Technology/methodology                                                                 | Data analysis                                                                 |
|---------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------|
| Chen et al. (2017)  | A delay sensitive multicast protocol                                                       | Utilize the limited resources of MANET efficiently                                          | Measuring the busy/idle ratio of the shared radio channel, estimating one-hop delay is suggested                | Desired speed profile to be tracked by the driver           | Multicast tree, delay sensitive multicast protocol for real-time applications in multi rate | Data mining techniques                                                          | Increase the network capacity                                                   |
| Bozorgi et al. (2017) | Electric vehicles based on historical driving data                                         | A routing algorithm that leads to the extended driving range and battery longevity of electric vehicles (EV) is proposed |locating the time and energy efficient routes                                                           | NA                                                          | Data mining techniques                                                          | Data mining techniques                                                          | WarrrigalProject                               |
| Taha et al. (2017)  | Energy efficient multipath routing protocol                                                | Energy consumption significant limitations in MANET                                         | Reducing network lifetime, energy consumption                                                               | Fitness function technique                                  | Ad hoc on demand multipath routing with life maximization, ad hoc on demand multipath distance vector with the fitness function | Ad hoc on demand multipath routing with life maximization, ad hoc on demand multipath distance vector with the fitness function | 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 |

| Author (Year)       | Introduction or Background                                                                 | Aim or purpose or objective                                                                 | Existing research works                                                                                      | Overcome this problem                                      | Proposed approaches                                                                 | Technology/methodology                                                                 | Data analysis                                                                 |
|---------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------|
| Cai et al. (2018)   | Self-cooperative trust                                                                     | Multi-objective optimization model                                                           | Determine an optimal routing of packets                                                                       | NA                                                          | NA                                                                                | NA                                                                                | NA                                                                                           |
| Chintalapalli and Ananthula (2018) | Multi-objective optimization model                                                       | Secure routing in MANET                                                                     | Find the least-cost routing of nominal traffic and survivability against node failure                         | NA                                                          | NA                                                                                | NA                                                                                | NA                                                                                           |
| Kacem et al. (2018) | Multi-objective optimization model                                                         | Secure routing in MANET                                                                     | Find the least-cost routing of nominal traffic and survivability against node failure                         | NA                                                          | NA                                                                                | NA                                                                                | NA                                                                                           |
### Table 1 (continued)

| Author (Year) | Cai et al. (2018) | Chintalapalli and Ananthula (2018) | Kacem et al. (2018) |
|---------------|-------------------|-----------------------------------|---------------------|
| **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-Lion-Whale | 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) | Khudayer et al. (2020) | Zhang et al. (2020a, b) |
|-------------------|------------------------|------------------------|
| **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 |
proposed system introduces all the above requirements that turn mobile nodes into efficient route interaction in multi-purpose 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. (2020a, b) 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-Smith et al. (2017), Li and Wu (2017), Bai et al. (2017), and Taha et al. (2017) have 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 and Ananthula(2018), and Khudayer et al. (2020) 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 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 and Wu (2017), Chen et al. (2017), Taha et al. (2017), and Zhang et al. (2020a, b) node multitasking issue. 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 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.
and Ali Hussain 2020), as shown in Fig. 3 (Keerthi and Venkataram 2012).

Figure 2 discusses the attacker detection automation of the bees colony optimization (ADABCP) method employed in MANET to refine the routing issues' appropriate refinement. 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 movable node-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 (Mukhedkar and Kolekar 2020). 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 (Ghoreishi et al. 2014; Kausar et al. 2020).

The three factors are followed in the ADABCP method. First, the routing operation performs the node movement within the boundary in MANET (Priya et al. 2020). Hence, head nodes are chosen in the transmission environment. This process is also called node initialization (Allimuthu 2017). 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. Each node will then find its node grade, node id, and distances of the neighboring node in these circumstances. A source node with the lowest ID between its adjacent nodes becomes a transmission environment initiator node, and the timer starts (Robinson et al. 2019a, b; Garaaghaji and Alfi 2020).

Finally, control parameters are effectively applied to the detection automation to improve the energy efficiency on the head node of the transmission environment (Jabar et al. 2018; Chithaluru et al. 2019). 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 (Hu et al. 2003; Alzamzami and Mahgoub 2020). 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 (Robinson et al. 2019a, b). 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 coordinate 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 (Sultanuddin and Ali Hussain 2020). 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" (Taha et al. 2017; Robinson et al. 2019a, b; Sánchez-García 2020).

Figures 4, 5, 6, 7, 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. Figures 4 and 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 (Bamhdi 2020); meanwhile, the average rate (nodes) at which packets are arriving to get served is 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 (Robinson et al. 2019a, b). 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.

\[
Nodes\ Propagation\ Time = \sum_{i=\text{MN1(sender)}}^{\text{MN17(receiver)}} \left[ \frac{1}{\left( M_i - L \right)_{\text{forward}}} \right] + \left[ \frac{1}{\left( M_i - L \right)_{\text{Reverse}}} \right]
\]  

(1)

From the above Eq. 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 \( R1MN9 \rightarrow MN10 \rightarrow MN5 \rightarrow MN2 \rightarrow MN1, \) \( R2MN9 \rightarrow MN4 \rightarrow MN1, \) and \( R3MN8 \rightarrow MN4 \rightarrow MN1 \)). 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 (Allimuthu and Mahalakshmi 2018a, b; Ladas et al. 2018; Matheus et al. 2019; Kim et al. 2020).

### 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 (Ghoreishi et al. 2014; Yan et al. 2017). A partial solution with individual exploration and collective experience is generated in the pattern reorganization used in the pattern reorganization (Ho et al. 2019; Zhang et al. 2020a, b). 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 (Sultanuddin and Ali Hussain 2020).

The route factors are a significant part of route detection, which helps discover attackers in the path, as discussed in Table 2 for R1 \( \equiv MN1 \rightarrow MN9 \). 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 \( \equiv MN1 \rightarrow MN9 \). The route detection recognizes and finds attackers in the path, as discussed in Table 4 for R3 \( \equiv MN1 \rightarrow MN8 \). 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** \( R1 \equiv MN1 \rightarrow MN2 \rightarrow MN5 \rightarrow MN10 \rightarrow MN9 \),
- **The second preferable route** \( R2 \equiv MN1 \rightarrow MN4 \rightarrow MN9 \) and
- **The third preferable route** \( R3 \equiv MN1 \rightarrow MN4 \rightarrow MN8 \).

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 MANET environment session.

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 forwarding transmission between nodes, which differ in each subset length and other parameters (Ortiz Castillo et al. 2017). 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 (Garaaghaji and Alfi 2020; Zhang et al. 2020a, b).

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.

\[ \text{Algorithm:} \]

1. **Initialization**: Set the initial parameters (population size, number of iterations, etc.).
2. **Evaluation**: Evaluate the fitness function for each individual in the population.
3. **Selection**: Select the best individuals for reproduction based on their fitness.
4. **Reproduction**: Create new individuals through crossover and mutation.
5. **Replacement**: Replace the old population with the new one.
6. **Termination**: If the stopping criterion is met, stop; otherwise, go to step 2.

End of Algorithm.
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, NeighborNode)
    NodeNetworkList ← ParticipateNode + NeighborNode
  end
end
DestNode ← FindDestNode(ParticipateNodeList)
  Mobile_Node1 ← DestNode(Key)
for (NodeList ← StartNode|NodeList ← (InitialKey+RandomKey(NodeList))
  FindDestNode ← 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, PE = NS
Step 3: While PE ≤ 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 (Euler's formula is performed in Attacker detection
automaton) 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 > MaxPEs,
Step 17: output (MinPath)
end
MinPath(Node) ← Route_Factor(NodeNetworkList)
Route_Factor ← Threshold Value (StartNode=CA, DestNode=|NeighborNode)
for(Route_Factor ← StartNode=|CA & |StartNode=MinPath(NodeNetwork) ←
DestNode||NeighborNode, NodeList(DestNode + 1),
NodeList(NeighborNode + 1)
MinPath(Node) ← MinPathRoute_Factor(NodeList) > Network Size)
NodeRoute (Threshold Value (StartNode=|CA, DestNode=|NeighborNode))
MinPath ← MinPath
end
end
return (MinPath)

Pseudo code for proposed routing protocol:(rushing attack)
Manage: Path Route Attacker
  A viral 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
Fig. 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.

Fig. 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.
Fig. 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.

Fig. 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.
Fig. 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.
| 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 | Organization: route with no attacker |                      |
|                 |             | Exploration  | Individual route | Uniqueness: automation |                      |                      |
| MN2 → MN5       | Solution    | Collectives | Route stage from MN1 → MN2 → MN5 | Past interaction | 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 |
|                 |             | 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 |                      |                      |
|                 |             | 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 |                      |
The above algorithm presents a route organization and route reorganization based routing protocol for finding the rushing attack (Al Shahrani 2011; Govindasamy and Punniakody 2018; El-Semary and Diab 2019; Jaiswal 2020). 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 (Pai et al. 2020). 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 (Ghoreishi et al. 2014; Thebiga and SujiPramila 2020).

### 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 (Kanagasundaram and Kathirvel 2018; Khudayer et al. 2020). 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

---

| 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 |

| Exploration | Individual route |

| 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 |

| Exploration | Individual route |

| MN4 → MN8 | 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 | Organization: route with no attacker |

| Experience | Collective: MN9 node Ids |

| Exploration | Individual route |

| Unique: detection automation techniques | Organization: route with attacker indication much bogus |

---

The above algorithm presents a route organization and route reorganization based routing protocol for finding the rushing attack (Al Shahrani 2011; Govindasamy and Punniakody 2018; El-Semary and Diab 2019; Jaiswal 2020). 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 (Pai et al. 2020). 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 (Ghoreishi et al. 2014; Thebiga and SujiPramila 2020); ; ; ; .
mechanism scheme, the nodes allow the secure node to have a higher transmission rate.

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 every node’s node data stream status in the routing path (Sultanuddin and Ali Hussain 2020; Priya et al. 2020). 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.
3.2.1.1 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,

\[ A_e(n) = \left( \log \frac{1}{FT_{(Src,Rev)}} - T_{\text{min}} \right) \times N_s \]  

(2)

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

For minimum communication response time efficiency of attacker node,

\[ C_e(n) = (D_{\text{max}} - FT_{(Src,Rev)})^N_s \]  

(3)

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

\[ FT_{(Src,Rev)} = \sum_{k=1}^{k} \left[ \frac{PRN_{(Src,Rev)}}{K} \right] \]  

(4)

\( FT_{(Src,Rev)} \) 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 (Robinson et al. 2019a, b).

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 (Elhoseny and Shankar 2019). 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, is stable route, \( Conti \), is continuous routing then \( O_n \times R_n \) is route organization rate at reverse acknowledgment direction. Meanwhile \( Conti \) is the stable route, \( Conti \) is continuous routing at forwarding direction.

\[ Conti = \sum_{n=NM1}^{NM17} \left[ \text{thresholdcount} \cdot \text{Stable}_i \right] 

- \left[ \max_{(n-1)} \text{thresholdcount} \cdot (O_n \times R_n) \right] \]  

(5)

\[ Conti = \sum_{n=NM1}^{NM17} \left[ \text{thresholdcount} \cdot \text{Stable}_f \right] 

- \left[ \max_{(n-1)} \text{thresholdcount} \cdot (O_n \times R_n) \right] \]  

(6)

The above Eqs. 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 \( Conti \) 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 (Ramamoorthy and Sangaiah 2019a). The reserve among the various nodes is improved based on node position by Eq. 7.
\[ E_n = \text{residual}_{\text{energy}} - \max_{t(\text{Stable}_{\text{ratio}})} \left[ \text{consumed}_{\text{energy}} \right] \] (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 (Jain et al. 2020). 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 (Garaaghaji and Alfi 2020). 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 (Jabbar et al. 2018; Khudayer et al. 2020; Islabudeen and Devi 2020). 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 (Mishra et al. 2020). 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 (Hu et al. 2003; Al Shahrani 2011).

### 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 (Alzamzami and Mahgoub 2020). 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 Tables 2, 3, 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 (Li and Wang 2019). 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 (Elhoseny and Shankar 2019).

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 (Mishra et al. 2020).

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 (Muneeswari and Manikandan 2019). 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 (Matheus et al. 2019). 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 (Islabudeen and Devi 2020). This data transfer mechanism keeps the reliable and security measures of the whole participating MANET environment system.

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 (Mukhedkar and Kolekar 2020).

3.3.2.1 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 (Ladas et al. 2018). 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 (Khanna and Sachdeva 2019).

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 current packet’s time consumption is calculated concerning the amount of energy spent on the REQ/REP process.

| Table 5 | Past interaction history for trust values |
|---------|-----------------------------------------|
| Mobile_Network_ID | Host ID | Network_Src_address | Network_Mask | Network_Dest_address | Network_MASK | Sender_node | Receiver_node | Route_Perception | Structure | Trust_Value | Time taken for avg execution | Error |
| MN1—MN2 | 192.168.0.X | 192.168.0.1 | 192.168.0.2 | 255.255.255.248 | 10.35 | 1 | 9.86 |
| MN3—MN5 | 192.168.0.X | 192.168.0.2 | 192.168.0.5 | 255.255.255.248 | 10.35 | 1 | 8.65 |
| MN5—MN10 | 192.168.0.X | 192.168.0.5 | 192.168.0.10 | 255.255.255.248 | 10.35 | 1 | 9.33 |
| MN10—MN9 | 192.168.0.X | 192.168.0.9 | 192.168.0.12 | 255.255.255.248 | 10.35 | 0 | 4.65 |
| MN9—MN1 | 192.168.0.X | 192.168.0.1 | 192.168.0.6 | 255.255.255.252 | 10.35 | 1 | 7.66 |
| MN4—MN8 | 192.168.0.X | 192.168.0.4 | 192.168.0.8 | 255.255.255.252 | 10.35 | 1 | 9.89 |
This process is expressed as the following process,

\[
\text{NLT}^{(S \leftrightarrow D)} = \frac{\text{Energy}_{1\text{st pkt tran}} - \text{Energy}_{\text{nth pkt tran}}}{\text{Energy}_{\text{total pkt tran}} - \text{Energy}_{\text{nth pkt tran}}}
\] (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 \( \times 204 \))/(188 \times BpS). To convince this byte per symbol information (BpS), this research can be used in the hybrid random late detection (HRLD) routing protocol (Kirst et al. 2016), which is constituted based on the past interaction history with route interaction from network id 0.0.0.1 to an end-user node (Shen et al. 2020).

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 (Kanaagasundaram and Kathirvel 2018). 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 (Jain et al. 2020; Rosas et al. 2020). 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 next sequential node packet (Li and Wang 2019).

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

| Possible Route | Network ID | Host ID | Packet life time (ms) | AvgNetwork Life time(ms) | Efficiency | Energy consumption rate | Node_final_FTIL_destination |
|---------------|------------|---------|----------------------|--------------------------|------------|------------------------|----------------------------|
| MN1 \( \rightarrow \) MN2 | 192.168.0.X | 192.168.0.1 \( \leftrightarrow \) 192.168.0.2 | 2.4970 | 2.4137 | 30.2467 | Higher | 49.6443 | 79.8915 | Minimum |
| MN2 \( \rightarrow \) MN5 | 192.168.0.X | 192.168.0.2 \( \leftrightarrow \) 192.168.0.5 | 2.1176 | 2.2829 | 33.3627 | Average | 41.6648 | 75.0276 | Minimum |
| MN5 \( \rightarrow \) MN10 | 192.168.0.X | 192.168.0.5 \( \leftrightarrow \) 192.168.0.10 | 2.5744 | 2.4440 | 30.0486 | Higher | 49.4479 | 79.4965 | Minimum |
| MN10 \( \rightarrow \) MN9 | 192.168.0.X | 192.168.0.9 \( \leftrightarrow \) 192.168.0.10 | -0.333 | 2.0311 | 153.224 | Minimum | 6.00413 | 159.228 | Maximum |
| MN1 \( \rightarrow \) MN4 | 192.168.0.X | 192.168.0.1 \( \leftrightarrow \) 192.168.0.4 | 2.2344 | 2.3222 | 32.1736 | Average | 44.7261 | 76.8997 | Minimum |
| MN4 \( \rightarrow \) MN9 | 192.168.0.X | 192.168.0.4 \( \leftrightarrow \) 192.168.0.9 | 2.3931 | 2.3761 | 30.8660 | Higher | 48.1734 | 79.0395 | Minimum |
| MN1 \( \rightarrow \) MN4 | 192.168.0.X | 192.168.0.1 \( \leftrightarrow \) 192.168.0.4 | 0.7663 | 2.1222 | 49.1705 | Lower | 24.1885 | 73.3590 | Minimum |
| MN4 \( \rightarrow \) MN8 | 192.168.0.X | 192.168.0.4 \( \leftrightarrow \) 192.168.0.8 | 2.4722 | 2.4045 | 30.3781 | Higher | 49.3661 | 79.7443 | Minimum |

| Network ID | Next hop | Current node to gateway | Cost | No of nodes presented | No. of route on the gateway |
|------------|----------|-------------------------|------|-----------------------|-----------------------------|
| 0.0.0.1 | 0.0.0.10 | 192.130.10.10 | n | 1 to N(n – 1) \( \times \) n | R1 |
| 125.0.0.0 | 232.0.10 | 197.1.10 | n | 1 to N(n – 1) \( \times \) n | R2 |
| 198.162.0.1 | 255.255.255.255 | 198.162.0.100 | n | 1 to N(n – 1) \( \times \) n | Rr |

(Bozorgi et al. 2017; Jabbar et al. 2018).
neighbor group or the nearby controller would be based on the key assignment, past interaction (Robinson et al. 2019a, b). 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 (Kanagasundaram and Kathirvel 2018). 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.

3.3.2.2 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 (Manolopoulos et al. 2020). 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 Fig. 10.

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.

3.3.2.3 Sender-receiver address status This sender-receiver destination address status has taken the communication over the radio range. SDN data rate for finding the exact route between the sender and receiver by using the command includes 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.

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 Fig. 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 assist improve MANET communication with the environment, or is MANET making the route determination to offer “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 (Santos et al. 2018). 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.

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

- It uses the sender/receiver nodes for an individual transaction.

| 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 $MN_P$-1 | Node $MN_D$ |
| Node 1 | Node1 | ... | ... | ... | ... | ... | ... |
| Node 2 | 1 | Node2 | ... | ... | ... | ... | ... |
| Node 4 | 2 | Node4 | 3 | 4 | ... | ... | ... |
| Node 5 | ... | Node5 | 5 | ... | ... | ... | ... |
| ... | ... | ... | ... | ... | ... | ... | ... |
| Node $MN_P$-1 | ... | ... | ... | ... | ... | ... | ... |
| Node $MN_S$ | ... | ... | ... | ... | ... | ... | ... |

| 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 |
• 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.

• 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.

• 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 to successfully improve 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 (Kalpana and Karthik 2020).

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 (Hurley-Smith et al. 2017; Djedjig et al. 2020).

This conclusion is enhanced in the coming circumstances. In a particular route, to enhance the initial packet distribution (MN_p) from the source to nearby nodes, Euler’s formula can be used to make the manipulation on the destination determination. The participation nodes (MN_s) are considered as the till end nodes (MN_p) concerning the throughput (f). The individual nearby nodes (MN_near) are determined by the following Euler’s formula by Eqs. 9–14,

\[ MN_{p_{total}} = e^{-rT} \sum_{MN_p=1}^{MN_0} e^{-r \frac{2\pi MN_{near}MN_s}{\tau}} \] (9)

From the first refinement, Euler’s 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 (f) becomes null. i.e., (0) and is applied in Eq. 9.

For individual node determination,

\[ MN_{p} = e^{-r \frac{2\pi MN_{near}MN_s}{\tau}} \] (10)

In this stage, Euler’s formula is applied to the whole network; hence the corresponding route node is calculated concerning the packet distribution (MN_p).

\[ MN_{p} = e^{-r \frac{2\pi MN_{near}MN_s}{\tau}} \] (11)

The enhancement bandwidth (γ) and node speed (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).

\[ MN_{p} = e^{-r \frac{2\pi (\gamma + s)}{\tau}} \] (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.

\[ MN_{p} = e^{-r \frac{2\pi fT}{\tau}} \] (13)

Finally, the route finding manipulation is formed based on Eq. 13 for each node, which tabulated with respect to the route finding manipulation

\[ MN_{p} = e^{-r \delta T} \] (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. It uses the delimiting of the nearby nodes to improve 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.
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 signal switch inputs (route (r)))

**For** Route Estimation in route (r) do

**Route_Estimation deducted Source Node (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 = getPessimistic (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

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 (Taha et al. 2017; Al-Zahrani 2020; Srivastava et al. 2020). 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 (Al Shahrani 2011; Hammi et al. 2020).

The maximum secure route of the mobile nodes ensures the easiest communication if the $S_t$ is a stable route, $C_t$ is rushing routing $T_n \times E_n$ participating node (MNp) route and rate (Eq. 15).

$$C_t = \sum_{MN_p=1}^{MN_p} \left[ \text{threshold}_t[S_t] - \left[ \max_{t=(node-1)} \left( \text{threshold}_t(T_n \times E_n) \right) \right] \right]$$

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.
Intelligent route discovery towards rushing attacks in ad hoc wireless networks

between nodes in the routing path. The proposed $C_r$ 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

$$E_n = \text{residual}_{\text{energy}} - \max_{\text{t}=(\text{Stable}_{\text{node}})} \left[ \text{consumed}_{\text{energy}} \right] \quad (16)$$

The proposed scheme is used to detect the attacker route with the exact maximum damage route (Eq. 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 (Garaaghaji and Alfi 2020). 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 than the remaining paths. It minimizes the packet transmission traffic to show improvement in the network lifespan (Li and Wang 2019; Khudayer et al. 2020).

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 (Sánchez-García 2020). 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

| 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: RR X (mm) @0.025 ms| 150–200 m                      |
| propagation model               | Propagation: RR Y (mm) @0.025 ms| 200–250 m                      |
|                                 | Propagation: RR Z (mm) @0.025 ms| 150–250 m                      |
| Simulation time                 | 0.5 × 102 ms                    | 0.5 × 102 ms                   |
| Traffic source                  | Set time steps to 2400 ms       | 2400 ms                        |
| 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                        | HRLD routing protocol           |                                |
spread and processed with $0.5 \times 10^2$ ms simulation time with traffic source time steps to 2400 ms. 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 0.025 ms by 150–200 m, Y (mm) at 0.025 ms by 200–250 m and propagation of Z (mm) at 0.025 ms by 150–250 m. It has a different transmitting range that varies from 150 to 250 m. 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) End to end delay: Figs. 12, 13, 14, 15, 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, 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).

End to end delay = End time − Start time × 100
Fig. 14 Graph for an end-to-end delay vs. mobility count

Analysis of end to end delay

Fig. 15 Graph for an end-to-end delay vs. network size

Average end to end delay Vs Network Size

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

Analysis of Average end-to-end Delay
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. There are 100 samplings 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 attacker (Kleineberg and Helbing 2017).

The Figs. 12, 13, 14, 15, 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 (Kleineberg and Helbing 2017). 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.

![Graph for communication overhead vs. number of attackers](image-url)

**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 |
(ii) Communication overhead: Figs. 17, 18, 19, 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 com-
pared to existing ESCT, ENM-LAC, and ZRDM-LFPM methods.

*communication overhead*  
\[
\text{Communication overhead} = \frac{\text{Number of packet losses}}{\text{received}} \times 100
\]

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 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 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

### Table 12 Performance result analysis of communication overhead

| Nodes mobility count | Communication overhead (pkts/ms) | Average communication overhead (%) |
|----------------------|----------------------------------|-----------------------------------|
|                      | 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                                           | 55.26% decrease |
|                      | 20.0000                          | 77.65                             | 66.46                             | 60.89             | 25.63                                           | 62.492% decrease |
|                      | 30.0000                          | 71.39                             | 61.95                             | 54.34             | 21.19                                           | 66.128% decrease |
|                      | 40.0000                          | 68.99                             | 56.96                             | 48.94             | 20.91                                           | 64.131% decrease |
|                      | 50.0000                          | 65.39                             | 51.28                             | 43.64             | 19.93                                           | 62.703% decrease |
|                      | 60.0000                          | 61.66                             | 40.93                             | 31.15             | 15.22                                           | 65.859% decrease |
|                      | 70.0000                          | 56.09                             | 27.94                             | 20.97             | 11.35                                           | 67.571% decrease |
|                      | 80.0000                          | 52.96                             | 22.35                             | 13.94             | 8.68                                            | 70.823% decrease |
|                      | 90.0000                          | 47.99                             | 21.46                             | 11.38             | 6.88                                            | 74.464% decrease |
|                      | 100.0000                         | 43.46                             | 20.12                             | 10.96             | 4.61                                            | 81.446% decrease |

**Fig. 21** Graph for packet delivery ratio vs. number of attackers

**Performance comparison of Packet Delivery Ratio**

- ESCT
- ENM-LAC
- ZRDM-LFPM
- SIRT–ADABCP-HRLD

![Graph for packet delivery ratio vs. number of attackers](image-url)
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 150 ms. The proposed method packet delivery ratio is enhanced compared to the existing ESCT, ENM-LAC, and ZRDM-LFPM methods.

\[ \text{Packet delivery ratio} = \frac{\text{Number of packet received}}{\text{generated packets}} \times 100 \]

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

| 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 Performance result analysis of packet delivery ratio (PDR)

Fig. 22 Graph for packet delivery ratio vs. network lifetime.
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
Intelligent route discovery towards rushing attacks in ad hoc wireless networks

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, 24, 25, 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.

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 (Srivastava).
et al. 2020; Mukhedkar and Kolekar 2020). 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 (Ramamoorthi and Sangaiah 2019). 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 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 in the active routing stage. The network lifetime of the suggested protocols is expressed in Fig. 27.

Network Lifetime = length of energy usage/overall energy

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 and Sangaiah 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 Fig. 27.

Figure 27 clarifies the values of the speed of packets delivered vs. energy consumption per bit during a single relay (from 1 to 100 node). The nodes speed 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.

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 (Hayashi and Uchiyama 2018). 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.

| Nodes mobility count | Network lifetime (J/ms/bits/pkts) | Average network lifetime (%) |
|----------------------|----------------------------------|------------------------------|
|                      | ESCT—Cai et al. (2018) | ENM-LAC—Liu et al. (2019) | ZRDM-LFPM—Khadayer et al. (2020) | SIRT—ADABCP-HRLD | Inference for existing system with proposed system |
| NLT versus mobility | 10.0000 | 32.50 | 53.51 | 70.04 | 83.06 | 59.67% increase |
|                      | 20.0000 | 34.08 | 53.72 | 71.50 | 84.08 | 58.33% increase |
|                      | 30.0000 | 34.75 | 54.07 | 72.08 | 85.07 | 58.61% increase |
|                      | 40.0000 | 34.95 | 55.03 | 72.50 | 86.06 | 58.89% increase |
|                      | 50.0000 | 35.00 | 56.04 | 73.04 | 86.50 | 58.15% increase |
|                      | 60.0000 | 36.06 | 57.08 | 73.50 | 87.07 | 56.75% increase |
|                      | 70.0000 | 37.08 | 57.50 | 74.06 | 88.06 | 56.63% increase |
|                      | 80.0000 | 37.50 | 58.01 | 74.50 | 88.50 | 56.16% increase |
|                      | 90.0000 | 38.08 | 59.07 | 74.75 | 88.75 | 54.88% increase |
|                      | 100.000 | 38.55 | 59.50 | 75.11 | 89.08 | 54.33% increase |
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 Fig. 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 from 190 J/s 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/s to execute all transactions within the stipulated time interval.

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

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

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 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 compared 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 30 to 66 kbps. As shown in Fig. 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 to 981.26 kbps; the AOMDV also decreases from 968 to 880 kbps.
Intelligent route discovery towards rushing attacks in ad hoc wireless networks

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 Fig. 31, the performance is analyzed from two-speed ranges. As the node speed increases (0, 0.5, 1, 1.5 ms), the throughput of the proposed SIRT-ADABCP-HRLD decreases from 950 to 800 kbps. 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, 40 ms), the throughput of SIRT-ADABCP-HRLD decreases from 500.86 to 100 kbps. SIRT-ADABCP-HRLD has the best performance in the range of 0–10 ms 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 Fig. 32, the mean

**Average Throughput Vs Execution Time**

![Graph showing average throughput vs. execution time for various routing protocols under rushing attack conditions.](image)

**Fig. 32** Performance result analysis of for throughput
throughput of the MANET is 50% when there is no attack. For rushing attacks, the malicious agent is launched at 68 ms 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 30 ms, 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, Fig. 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 Fig. 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: attack and without attack. The existing techniques for the comparison are AODV, SAODV, PCBHA, Bp-AODV. At the maximum time limit, SIRT-ADABCP-HRLD had a throughput of 3750 kbps, while AODV, SAODV, PCBHA, Bp-AODV had below 3000 kbps. In Fig. 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.

Acknowledgements We thank Mrs. Indu Murugesan, Vice-Chairperson, KIT–Kalaignarkarunanidhi Institute of Technology-Coimbatore, for their support throughout all aspects of our research and also provided the KIT Incubation Centre for writing the manuscript.

Declarations

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

Ethical Approval This article does not contain any studies with human participants or animals performed by any authors.

References

Al_shahrani AS (2011) Rushing attack in mobile ad hoc networks. In: 2011 Third international conference on intelligent networking and collaborative systems. IEEE, pp 752–758. https://doi.org/10.1109/INCoS.2011.145

Allimuthu U (2017) BAU FAM: biometric-blacklisting anonymous users using fictitious and adroit manager. J Adv Res Dyn Control Syst 12(Special):722–737

Allimuthu U, Mahalakshmi K (2018a) Observed survey on efficient route interaction of mobile nodes in MANET. J Adv Res Dyn Control Syst 10(Special):952–965

Allimuthu U, Mahalakshmi K (2018b) Efficient object-route interaction for finding old unused scrap car in Coimbatore Municipality. J Adv Res Dyn Control Syst 10(Special):984–988

Al-Zahrani FA (2020) On modeling optimizations and enhancing routing protocols for wireless multihop networks. IEEE Access 8:68953–68973. https://doi.org/10.1109/ACCESS.2020.2986010

Alzamzami O, Mahgoub I (2020) Link utility aware geographic routing for urban VANETs using two-hop neighbor information. Ad Hoc Netw 106:102213. https://doi.org/10.1016/j.adhoc.2020.102213

Amutha S, Balasubramanian K (2018) Secured energy optimized ad hoc on-demand vector routing protocol. Comput Electr Eng 72:766–773. https://doi.org/10.1016/j.compeleceng.2017.11.031
Elhoseny M, Shankar K (2019) Reliable data transmission model for MANETs. IEEE Syst J 12(2):1743–1754. https://doi.org/10.1109/jsyst.2017.2721543

Balaji S, Julie EG, Robinson YH, Kumar R, Thong PH (2019) Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. Comput Stand Interfaces 66:1–10:103358. https://doi.org/10.1016/j.csi.2019.103358

Bamhdi AM (2020) Efficient dynamic-power AODV routing protocol based on node density. Comput Stand Interfaces 70:103406. https://doi.org/10.1016/j.csi.2019.103406

Bozorgi AM, Farasat M, Mahmoud A (2017) A time and energy efficient routing algorithm for electric vehicles based on historical driving data. IEEE Trans Intell Veh 2(4):308–320. https://doi.org/10.1109/TIV.2017.2771233

Cai RJ, Li XJ, Chong PHJ (2018) An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE Trans Mob Comput 18(1):42–55. https://doi.org/10.1109/TMC.2018.2828814

Chen YH, Wu EHK, Lin CH, Chen GH (2017) Bandwidth-satisfied and coding-aware multicast protocol in MANETs. IEEE Trans Mob Comput 17(8):1778–1790. https://doi.org/10.1109/TMC.2017.2778262

Chen Z, Zhou W, Wu S, Cheng L (2020) An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET. IEEE Access 8:44760–44773. https://doi.org/10.1109/ACCESS.2020.2978582

Chintalapalli RM, Ananthula VR (2018) M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network. IEEE Access 6:1406–1415. https://doi.org/10.1049/iet-com.2017.1279

Chithaluru P, Tiwari R, Kumar K (2019) AREOR–adaptive ranking based energy efficient opportunistic routing scheme in wireless sensor network. Comput Netw 162:106863. https://doi.org/10.1016/j.comnet.2019.106863

Djedjig N, Tandjaoui D, Medjek F, Romdhani I (2020) Trust-aware and cooperative routing protocol for IoT security. J Inf Secur Appl 52:102467. https://doi.org/10.1016/j.ijsa.2020.102467

Elhoseny M, Shankar K (2019) Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Trans Reliab 69(3):1077–1086. https://doi.org/10.1109/10.2019.2915800

El-Sennawy AM, Diab H (2019) BP-AODV: blackhole protected AODV routing protocol for MANETs based on chaotic map. IEEE Access 7:95185–95199. https://doi.org/10.1109/ACCESS.2019.2928804

Garaaghaji A, Afifi A (2020) A fuzzy-hierarchical routing algorithm for MANET networks allocation rates problem. Iran J Sci Technol Trans Electr Eng 44(2):1003–1011. https://doi.org/10.1007/s40998-019-00253-z

Ghoreishi SM, Abd Razak S, Isinif IF, Chizari H (2014) Rushing attack against routing protocols in mobile ad-hoc networks. In: 2014 international symposium on biometrics and security technologies (ISBAST), IEEE, pp 220–224. https://doi.org/10.1109/ISBAST.2014.7013125

Govindasamy J, Punniakody S (2018) A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. J Electr Syst Inf Technol 5(3):735–744. https://doi.org/10.1016/j.jesit.2017.02.002

Hahn F, Pappa A, Eisert J (2019) Quantum network routing and local complementation. npj Quantum Inf 5(1):1–7. https://doi.org/10.1038/s41534-019-0191-6

Hammi B, Zeadally S, Labiod H, Khatoum R, Begriche Y, Khouchli L (2020) A secure multipath reactive protocol for routing in IoT and VANETs. Ad Hoc Netw 103:102118. https://doi.org/10.1016/j.adhoc.2020.102118

Hayashi Y, Uchiyama N (2018) Onion-like networks are both robust and resilient. Sci Rep 8(1):1–13. https://doi.org/10.1038/s41598-018-29626-w

Ho MC, Lim JMY, Soon KL, Chong CY (2019) An improved pheromone-based vehicle rerouting system to reduce traffic congestion. Appl Soft Comput 84:105702. https://doi.org/10.1016/j.asoc.2019.105702

Hu YC, Perrig A, Johnson DB (2003) Rushing attacks and defense in wireless ad hoc network routing protocols. In: Proceedings of the 2nd ACM workshop on wireless security, association for computing machinery, pp 30–40. https://doi.org/10.1145/941311.941317

Hurley-Smith D, Wetherall J, Adekunle A (2017) SUPERMAN: security using pre-existing routing for mobile ad hoc networks. IEEE Trans Mob Comput 16(10):2927–2940. https://doi.org/10.1109/TMC.2017.2649527

Islabdeen M, Devi MK (2020) A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks. Wirel Pers Commun 112(1):193–224. https://doi.org/10.1007/s11271-019-07022-5

Jabbar WA, Saad WK, 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. https://doi.org/10.1109/ACCESS.2018.2882853

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 Trans Sustain Comput. https://doi.org/10.1109/TSC.2020.2974727

Jaiswal RK (2020) Position-based routing protocol using Kalman filter as a prediction module for vehicular ad hoc networks. Comput Electr Eng 83:106599. https://doi.org/10.1016/j.compeleeng.2020.106599

Kacem I, Sait B, Mekhifel S, Saeur N (2018) A new routing approach for mobile ad hoc systems based on fuzzy petri nets and ant system. IEEE Access 6:65705–65720. https://doi.org/10.1109/ACCESS.2018.2878145

Kalpana V, Karthik S (2020) Route availability with QoE and QoS metrics for data analysis of video stream over a mobile ad hoc networks. Wirel Pers Commun 114:2591–2612. https://doi.org/10.1007/s11277-020-07491-z

Kanagasundaram H, Kathirvel A (2018) EIMO-ESOLSR: energy efficiency and security-based model for OLSR routing protocol in mobile ad-hoc network. IET Commun 13(5):553–559. https://doi.org/10.1049/iet-com.2018.5564

Kausar S, Habib M, Shabir MY, Ullah A, Xu H, Mehmood R, Iqbal MS (2020) Secure and efficient data transfer using spreading and assimilation in MANET. Softw Pract Exp 50(11):2095–2109. https://doi.org/10.1002/spe.2782

Keerthi TDS, Venkataram P (2012) Locating the attacker of wormhole attack by using the honeypot. In: 2012 IEEE 11th international conference on trust, security and privacy in computing and communications. IEEE, pp 1175–1180. https://doi.org/10.1109/trustcom.2012.196

Khanna N, Sachdeva M (2019) Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation. Int J Commun Syst 32(12):e40121-e401223. https://doi.org/10.1002/dac.4012

Khudayer BH, Anbar M, Hanshi SM, Wan TC (2020) Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks. IEEE Access 8:24019–24032. https://doi.org/10.1109/ACCESS.2020.2970279

Kim BS, Ullah S, Kim KH, Roh B, Ham JH, Kim KI (2020) An enhanced geographical routing protocol based on multi-criteria decision making method in mobile ad-hoc networks. Ad Hoc Netw 103:102157. https://doi.org/10.1016/j.adhoc.2020.102157
Kleineberg KK, Helbing D (2017) Collective navigation of complex networks: participatory greedy routing. Sci Rep 7(1):1–9. https://doi.org/10.1038/s41598-017-02910-x

Ladas A, Deepak GC, Pavlatos N, Politis C (2018) A selective multipath routing protocol for ubiquitous networks. Ad Hoc Netw 77:95–107. https://doi.org/10.1016/j.adhoc.2018.04.013

Li Y, Wang X (2019) A novel and efficient address configuration for MANETs. IEEE Commun Lett 21(7):1529–1532. https://doi.org/10.1109/LCOMM.2017.2654439

Liu S, Zhang DG, Liu XK, Zhang T, Gao JX, Cui YY (2019) Dynamic routing protocol for wireless ad-hoc visible light communication networks. Ad Hoc Netw 94:101941. https://doi.org/10.1016/j.adhoc.2019.101941

Manolopoulos I, Kontovasili K, Stavrakakis I, Thomopoulos SC (2020) Methodologies for calculating decision-related event occurrence times, with applications to effective routing in diverse MANET environments. Ad Hoc Netw 99(1–17):102068. https://doi.org/10.1016/j.adhoc.2019.102068

Matheus LM, Vieira AB, Vieira MA, Vieira LF (2019) DYRP-VLC: a dynamic routing protocol for wireless ad-hoc visible light communication networks. Ad Hoc Netw 94:101941. https://doi.org/10.1016/j.adhoc.2019.101941

Mishra A, Saha S, Makhiya S, Sinha S, Raychoudhury V, Sobin CC (2020) Empirical study of dynamics of amoebiosis transmission in mobile ad hoc networks (MANETs). Int J Commun Syst 33(2):1–28 e4186. https://doi.org/10.1002/dac.4186

Mukhedkar MM, Kolekar U (2020) E-TDGO: an encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network. Int J Commun Syst 33(7):e4252. https://doi.org/10.1002/dac.4252

Muneeswari B, Manikandan MSK (2019) Energy efficient clustering and secure routing using reinforcement learning for three-dimensional mobile ad hoc networks. IET Commun 13(12):1828–1839. https://doi.org/10.1049/iet-com.2018.6150

Ortiz Castillo E, Starnini M, Serrano Moral M (2017) Navigability of temporal networks in hyperbolic space. Sci Rep 7:15054. https://doi.org/10.1038/s41598-017-15041-0

Pai KJ, Chang RS, Chang JM (2020) A protection routing with secure mechanism in Möbius cubes. J Parallel Distrib Comput 140:1–12. https://doi.org/10.1016/j.jpdc.2020.02.007

Priya JS, Femina MA, Samuel RA (2020) APSO-MVS: an adaptive particle swarm optimization incorporating multiple velocity strategies for optimal leader selection in hybrid MANETs. Soft Comput. https://doi.org/10.1007/s00500-020-05034-z

Ramamoorthi JS, Sangaihak AK (2019) SCGR: Self-configuring greedy routing for minimizing routing interrupts in vehicular communication networks. Internet Things 8:100108. https://doi.org/10.1016/j.jiot.2019.100108

Robinson YH, Julie EG, Saravanan K, Kumar R, Abdel-Basset M, Thong PH (2019a) Link-disjoint multipath routing for network traffic overload handling in mobile ad-hoc networks. IEEE Access 7:143332–143323. https://doi.org/10.1109/ACCESS.2019.2943145

Robinson YH, Krishnan RS, Julie EG, Kumar R, Thong PH (2019b) Neighbor knowledge-based rebroadcast algorithm for minimizing the routing overhead in mobile ad-hoc networks. Ad Hoc Netw 93:101896. https://doi.org/10.1016/j.adhoc.2019.101896

Rosas E, Garay F, Hidalgo N (2020) Context-aware self-adaptive routing for delay tolerant network in disaster scenarios. Ad Hoc Netw 102(1–17):102095. https://doi.org/10.1016/j.adhoc.2020.102095

Sahu R, Sharma S, Rizvi MA (2020) ZBLE: zone based efficient energy multipath protocol for routing in mobile ad hoc networks. Wirel Pers Commun 113(4):2641–2659. https://doi.org/10.1007/s11277-020-07345-8

Sánchez-García RJ (2020) Exploiting symmetry in network analysis. Commun Phys 3(1):1–15. https://doi.org/10.1038/s42005-020-0345-z

Santos BP, Goussevskaia O, Vieira LF, Vieira MA, Loureiro AA (2018) Mobile matrix: routing under mobility in IoT, IoMT, and social IoT. Wirel Pers Commun 78:84–98. https://doi.org/10.1016/j.wpc.2018.05.012

Shen J, Wang C, Wang A, Liu Q, Xiang Y (2020) Moving centroid based routing protocol for incompletely predictable cyber devices in cyber-physical-social distributed systems. Future Gener Comput Syst 108:1129–1139. https://doi.org/10.1016/j.future.2017.10.024

Srivastava A, Prakash A, Tripathi R (2020) Location based routing protocols in VANET: issues and existing solutions. Veh Commun 23:100231. https://doi.org/10.1016/j.vehcom.2020.100231

Sultanuddin SJ, Ali Hussain M (2020) Token system-based efficient route optimization in mobile ad hoc network for vehicular ad hoc network in smart city. Trans Emerg Telecommun Technol 31(12):e3853. https://doi.org/10.1002/ett.3853

Taha A, Alsauqur 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. https://doi.org/10.1109/ACCESS.2017.2707537

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. Wirel Pers Commun 114(2):975–993. https://doi.org/10.1007/s11277-020-07403-1

Yan C, Yang KY, Martin OJ (2017) Fano-resonance-assisted metasurface for color routing. Light Sci Appl 6(7):e17017. https://doi.org/10.1038/lsa.2017.17

Zhang L, Hu L, Hu F, Ye Z, Li X, Kumar S (2020a) Enhanced OLSR routing for airborne networks with multi-beam directional antennas. Ad Hoc Netw 102:102116. https://doi.org/10.1016/j.adhoc.2020.102116

Zhang T, Zhao S, Cheng B (2020b) Multipath routing and MPTCP-based data delivery over manets. IEEE Access 8:32652–32673. https://doi.org/10.1109/ACCESS.2020.2974191

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.