Efficient Mobile Ad Hoc Route Maintenance Against Social Distances Using Attacker Detection Automation

Udayakumar Allimuthu · K. Mahalakshmi

Accepted: 15 August 2022 / Published online: 1 October 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
In MANET, routing plays a vital role in packet interaction and data transmission. It is always easy to manage the data transmission over the MANET because of uncentralized control on the MANET nodes. Since the efficient route on MANET controls the packets and does not simplify the route between the source and destination. Hence the maintenance of route interaction becomes a crucial process. Methods: It is critical to enhance the route and decrease the attacker to sustain successful data transfers via the MANET Network. MANET, on the other hand, permits route interaction with security threads. The four processing schema are proposed in this study work to retain the security safeguards against Routing Protocols. The Rushing Attacker has significantly influenced MANET packet-based data transfer, particularly node communication. The Attacker Detection Automation of Bee Colony Optimization (ADABCP) Method is proposed in this article. Results: Existing ESCT, ZRDM-LFPM, and ENM-LAC techniques were compared to the suggested outcome. Consequently, routing and data transfer have enhanced the proposed illustration (SIRT–ADABCP-HRLD). Compared to the recommended approach, the end-to-end latency, communication overhead, packet delivery ratio, network lifetime, and energy usage are all improved. Discussion: The performance evaluation results of SIRT–ADABCP-HRLD with existing methods in terms of low End to End Delay (ms) of 49.8361% compared to existing methods ESCT, ENM-LAC, and ZRDM-LFPM. In terms of low Communication Overhead, an 81.4462% decrease compared to existing methods. However, it improves packet delivery by 56.9775%, more than ESCT, ENM-LAC, and ZRDM-LFPM. The energy consumption decreased by 36.31% less value than the existing process.

Keywords Attacker detection · Dead node · Implicit response · Late detection · Node ranking · Route finding

1 Introduction
In an infrastructure-less network with an incredible number of mobile nodes, the migratory route is valid in terms of data transference, data security, and time delay. Finally, the research perspectives are made and provided to the user for communication between a mobile node with no trouble. In the current tendency, the infrastructure-less network mainly works on the Transfer rate, security, and time. These domains have their operational style that must apply the infrastructure-less network, and the process will suspend (Delay) for the entire data transmission [6, 14]. To systematically select the efficient infrastructure-less network, it must have to do 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" is used to locate the appropriate attackers in terms of initial matching with the other nodes, which is used to the automatic reduction of the attacker which is accommodating to determine the attacker less 'infrastructure-less network' ultimately with the help of "Swift Implicit Response Round Trip Time" mechanism [19]. Data delivery time interval for mobility node is possibly increased by using Hybrid Random Late Detection (HRLD). This HRLD scheme ensures secure route-finding and data transmission by using "Use Best Approximation,"

Udayakumar Allimuthu
udayakumar.allimuthu@gmail.com

K. Mahalakshmi
prof.dr.mlk@gmail.com

1 Department of Information and Communication Engineering, Anna University, Chennai, Tamil Nadu, India
2 Department of CSE, KIT-Kalaignarkaranadi Institute of Technology, Coimbatore, Tamil Nadu, India
which is helpful in routing problem observation. The route-finding approach retrieves the confidential route between the mobile nodes. This confidential route helps find an optimal solution for dead node reduction by using interaction history in a well-organized manner. The dead node reduction is worked depending on the time interval assignment, i.e., the time interval has been assigned to each node for a reply to the sender node; this happened on mobile node critical assignment. Within this time interval transmitted node is directing the reply messages to the transmit node for proving node confirmation. From this, we reduce the End-to-end Delay for one-way communication. Finally, node ranking is taken from the "Past Interaction History" for every transmission. It is used to rank the nodes to select an excellent short time process. The Attacker Detection Automation of Bees Colony Optimization (ADABCP) is run paralleled to update the dead node and active links [2, 3]. These apprisiongs are applied to past interaction history.

The cyclic processes of node ranking express the continuous monitoring system of an 'infrastructure-less network,' which produces an enhanced alternative for existing strategies. In conclusion, our proposed research makes the attacker less efficient route interaction between the node by using route finding, time confine, node ranking criteria, interaction history, and dead node reduction. In our result part, the proposed techniques are compared with the existing methods like Evolutionary Self-Cooperative Trust (ESCT) scheme, Zone-based Route Discovery Mechanism—a Link Failure Prediction Mechanism (ZRDM-LFPM), and Evolving Network Model based on Local-Area Choice (ENM-LAC) approaches [5]. The proposed SIRT-ADABCP-HRLD process provides efficient transmission in terms of end-to-end Delay, communication overhead, packet delivery ratio, network lifetime, and energy consumption [4, 8, 37]. Research aspects are implemented with the help of Network simulator 2.

In recent days much research has failed to notice this type of problem. However, this is extremely important to reduce because this has been useful in supporting emerging applications. This suggested research is classified based on the position finding [2] concerning the time and location. To increase the performance degradation of humans against the social distancing constrain, the automatically-reacting alarm hints at the short high tone produced as a signal sound of a forgotten formal accusation of social distancing. This accusation is come into being the embedding sensors-based social distancing model. This SDA scheme helps find simultaneous optimization in a secure, intelligent way. The real-time way of processes is imitated and located concerning features of relying upon observation [10, 12].

In addition to this, maintaining the social distancing between mobile living or extinct members is essential in distance utilization networks. The system servers will watch social distancing. The suggested system preserves the social distancing constrain over the mobile ad hoc networks. If the user cannot act according to social distancing deny, commands, or alerts, that type of user is considered immoral behavior human. They are regarded as the attacker. To remove the attacker (misbehavior extinct member) from the grocery shopping mall, by using manual removing [15, 22].

This article discussed the effects of individual social distance maintaining perception by examining how minimal social distance affects unknown persons. The two experimental conditions are explored to maintain the customers [6]. First, maintain distance from the people in the shopping mall. Second, suppose it does not keep space against the people in the shopping mall. In that case, the management instructs them to make the distances against the people [11, 14].

To investigate and address the research issues based on the routing strategies the routing nodes make. The objective of the research article is to propose route discovery in MANET platforms over a stipulated time interval. The route interaction is analyzed in dynamic aspects to find an efficient route for data communication. The research methodology has the following process to satisfy the various research questions.

- To enrich the performance of data communication using Swift Implicit Response Round Trip Time (SIRT) mechanism, to make the effective packet transmission without losing the control and data packets
- To suggest a route verification process suitable for security scrutiny that enables the optimal route to concentrate on the scrutinized route with reduced path count using Route Finding Manipulation (RFM)
- To make a heterogeneous and attacker-free route for data communication. The Attacker Detection Automation of the Bees Colony Optimization (ADA-BCO) method improves the routing process.
- To develop a high-performance SIRT-ADABCO-RLD (Attacker Detection Automation of the Bees Colony Optimization-Swift Implicit Response Round Trip Time-Random Late Detection) architecture, which uses efficient route interaction to reduce the attackers.
- To analyze the performance of the existing system with the proposed method with respect to throughput, packet delivery ratio, end-to-end Delay, communication overhead, network lifetime, and energy consumption
- To analyze the public spot’s impact on "social distance" by sensor-based social distancing plan of action.

The rest of the paper is organized as follows: an earlier introduction to the research article is discussed in Sect. 1. The literature review is discussed in the related review section. The proposed routing protocols communication for rushing attacker detection are discussed in Sect. 3. finally,
Sect. 4 discusses various result-oriented parameters like an end to end delay, communication overhead, packet delivery ratio (PDR), network lifetime, and energy consumption. Finally, this concludes in the conclusion section with related reference articles.

2 Related Review

MANET has provisions for efficient route interaction and data transfer. It is a collection of interactions between mobile nodes. Route interaction and data transmission via the MANET network are increasingly vulnerable to attackers. As a result, the effectiveness of route interactions is critical. The main focus of this research is on route interaction and data movement throughout the network to defend against rushing assaults. MANET (rushing assaults) is safeguarding data in a MANET network using a hybrid random late detection algorithm and a quick implicit response. Attacker Detection Automation, Hybrid Random Late Detection, Use Best Approximation, and Past Interaction History is the different node interaction types. All of these strategies are required for the nodes to interact effectively. This study offers a comprehensive overview of the state of route interaction on MANETs for efficient routing, particularly against Rushing Attacks, Time Delay, Attacker Detection, Route Finding, Time Confine, Node Ranking Criteria, and Interaction History. It analyses the most recent routing-based approaches that make route interaction on MANET as simple as possible. The following survey accompanies the core commitments of this study.

Compelling route integration scenarios still face challenges after existing research inquiry into the exhibited contribution schemes. These studies usually lack efficient route interaction models, which do not ensure data delivery, security, or time delay. Furthermore, [38, 40] in terms of node ranking criteria, interaction history, dead node reduction, and alive node boost-up for agreeable designs in efficient route interaction, it may create dangerous circumstances. All of the above needs are introduced in our suggested system, resulting in efficient route interaction of mobile nodes under multifunctional settings. The recommended component of the research helpful plans that have been demonstrated in previous domains may have possible issues.

Cai et al. [12], Kacem et al. [45], and Zhang et al. [81] [9, 31, 56] discussed the Mobile node transmission and high dead node issues. Even though MANET means to measure such problems, the proposed system can expose the problem and establish regularity and routing. Hurley et al. (2017), Li Zhinan et al. [51], and Bai et al. [8] are [5, 23, 43, 79] discussed the security. Trust Issues and their proposed frameworks require additional disclosure in regularity-based routing security and further work on the MANET. These different contribution actions promote them regularly based on routing safety. Bozorgi et al. [11], Chen et al. [13], Chintalapalli et al. (2018), and [8, 10, 12, 37] discussed the Transferring Time Issues. The Systems with numerous mobile nodes passing data between nearby route nodes require a more efficient route. It is found by the proposed interaction history, which adds multi-routing history to the framework. Liu et al. [53] suggested [44] Source routing in MANET network topology and discussed the mobile Nodes Discover Issue. Their Proposed frameworks commonly expect source hubs to disclosure trust in mind the end goal to determine the best node to coordinate and accomplish an ideal routing. This may be the extreme idea for solving the mobile node discovery issue in MANET; in any case, it likewise can be the toughest one within sight of inactive mobile node issues. Li Zhinan et al. [51], Taha et al. [68], and Zhang et al. [82] node multitasking issue [23, 41]. Mobile nodes can have a specific IP address as well as routing information. In this manner, data transformation goals must expect the need to adjust and standardize node correspondence to accomplish an ideal data transfer. Liu et al. [53] and Khudayer et al. [47] discussed [8, 10, 12] the node failure. their perspective views adaptation to internal failure separation of the mobile node, cause the lifetime, which correspondence to node failure. With set request/response periods, the preserved interaction history inside node interaction must create a warning to prevent future contact with the inactive failed node. It is then necessary to identify the node, retrieve the previous transaction, and retransmit it to the destination mobile nodes from the beginning nodes. This study thoroughly examines the most up-to-date research on mobile nodes’ most effective route interaction in MANETs. A comprehensive survey of route interaction and extensive data processing was also carried out—however, an assessment of all of the noteworthy route interaction models available in MANET. Even though the same process is displayed, it is in different domains such as WSN, Communication, etc. It focuses on the many challenges that arise throughout the efficient route interaction.

3 Routing Protocols Communication for Rushing Attacker Detection

The routing protocols communication for rushing attacker detection is explained in Figs. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and to 18. It demonstrates the viewed process of the rushing attack establishment communication channel. In this circumstance, MN1 –sender, MN17 –receiver, t – the distance between MN1 and MN17. (MN8) and (MN9) is the rushing attack route and the actual route of the routing protocols Communication, index sender to receiver [4, 7, 11]. It is referred to as the MN1 –sender,
index MN8 to the receiver MN8, R1 is the general rushing route, $R1MN1 \rightarrow MN2 \rightarrow MN5 \rightarrow MN10 \rightarrow MN9$ is the total amount of nodes directivity between MN1 –sender, MN17 –receiver, without (R1, MN1) and (R1, MN17) is 5. It is referred to as the MN1 –sender, index to the receiver MN9, R2 is the general rushing route, $R2MN1 \rightarrow MN4 \rightarrow MN9$, and R3 is the available rushing route, $R3MN1 \rightarrow MN4 \rightarrow MN8$ is the total amount of nodes directivity between MN1 –sender, MN17 –receiver, without (R2, MN1) is three and (R3, MN17) is 3. The distance from MN1 –sender, MN17 –receiver to the center of the area routing protocols Communication, concerning the distance from the attackers to the sender and receiver (MN8) and (MN9) [2, 14, 56, 77].

Figures 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, and 20, determined for Routing Protocols Communication for Rushing Attack concerning 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" mechanism, "Use Best Approximation" and "Past Interaction History" [77, 80, 83].

The nodes considerations on a proposed network model that set the network model following the nodes counts and packet distribution on each node [7]; meanwhile, the average rate () at which packets are arriving to be serviced based on the Packet Distribution Range parameters of the transmitter and receiver arrays are standard time interval of every
Fig. 3 Route estimation for R2 ↔ R5 by the Relative Coordination Systems using PSO. R2 ↔ R5, R2(config)#ip extroute-number R2 ↔ R5 deny rt 1:7:12 (R4), R2(config)#router hrld-sirt (R1,R2,R5), R2(config-router)#neighbor < ip_addr of R5 > new rt R5 ↔ R10, Out

Fig. 4 The dotted block highlighted nodes describe the successive route scenario on the proposed routing protocol. Interconnected systems clarify by giving an example of the following consecutive route

Fig. 5 Route estimation for R5 ↔ R10 by the Relative Coordination Systems using PSO. R5 ↔ R10, R5(config)#ip extroute-number R5 ↔ R10 deny rt 1:7:18 (R9), R5(config)#router hrld-sirt (R1,R2,R5,R10), R5(config-router)#neighbor < ip_addr of R10 > new rt R1 ↔ R4, Out
package is arriving at the destination that is fixed based on the request/response round trip time/delay.

In the proposed mechanism, the request/response round trip time/delay is the time demanded for a packet to travel from an origin to a finishing terminus. This might be calculated by combining the packet’s time 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 on the MANET packet transmission are calculated based on the following Eq. 1

\[
\text{Nodes Propagation Time} = \sum_{i=1}^{\text{all nodes}} \left( \frac{1}{(M_i - D)_{\text{forward}}} + \frac{1}{(M_i - D)_{\text{reverse}}} \right)
\]  

(1)

From the above Node propagation time calculation, \( M_i \) is the number of data requests (packets) per second transmitted concerning each node’s distance (\( t \)) on the MANET boundary. Perhaps the forwards are described based on the MN1 –sender, MN17 –receiver forward transmission. Any legitimate packet transmission between nodes (preferably by our concern on the forward route \( R_1 \equiv MN1 \rightarrow MN2 \rightarrow MN5 \rightarrow MN10 \rightarrow MN9 \), \( R_2 \equiv MN1 \rightarrow MN4 \rightarrow MN9 \), and \( R_3 \equiv MN1 \rightarrow MN4 \rightarrow MN8 \)) is considered as the bold’s transmission. Meanwhile, the reverse might be the acknowledgment of individual communication. (preferably by our concern on the reverse route \( R_1 \equiv MN9 \rightarrow MN10 \rightarrow MN5 \rightarrow MN2 \rightarrow MN1 \), \( R_2 \equiv MN9 \rightarrow MN4 \rightarrow MN1 \), and \( R_3 \equiv MN8 \rightarrow MN4 \rightarrow MN1 \)). This average rate at which packets are sent and arriving is calculated. From this consideration, the Node Detection Model and its parameters were generalized, and tunneling will allow simulating the process of node propagation with different time duration of attacker nodes under other route
Fig. 8 The dotted block highlighted nodes describe the alternative route scenario on the proposed routing protocol. Interconnected systems clarify by giving an example of the first alternate route.

Fig. 9 Route estimation for R4 ↔ R9 by the Relative Coordination Systems using PSO. R4 ↔ R9, R4(config)#ip extroute-number R4 ↔ R9 deny rt 1:7:17 (R8), R4(config)#route lrlid-sirt (R1,R4,R9), R4(config-router)#neighbor <ip_addr of R9> new rt R10 ↔ R11, Out.

Fig. 10 The dotted blue highlighted nodes describe the alternative route scenario on the proposed routing protocol. Interconnected systems clarify by giving an example of the first alternate route.
Fig. 11 Route estimation for R10 ↔ R11 by the Relative Coordination Systems using PSO. R10 ↔ R11, R10(config)#ip extroute-number R10 ↔ R11 deny rt 1:7:18 (R9), R10(config)#router hrld-sirt (R1,R2,R5,R10,R11), R10(config-router)#neighbor <ip_addr of R11> new rt R7 ↔ R12, Out.

Fig. 12 The dotted block highlighted nodes describe the successive route scenario on the proposed routing protocol. Interconnected systems clarify by giving an example of the fourth consecutive route.

Fig. 13 Route estimation for R9 ↔ R12 by the Relative Coordination Systems using PSO. R9 ↔ R12, R9(config)#ip extroute-number R9 ↔ R12 deny rt 1:7:17 (R8), R9(config)#router hrld-sirt (R1,R4,R9,R7,R12), R9(config-router)#neighbor <ip_addr of R12> new rt R11 ↔ R16, Out.
**Fig. 14** Interconnected system clarifies by giving an example of the third alternate route. The dotted block highlighted nodes describe the alternative route scenario on the proposed routing protocol.

**Fig. 15** Route estimation for R11 ↔ R16 by the Relative Coordination Systems using PSO. R11 ↔ R16, R11(config)#ip extroute-number R11 ↔ R16 deny rt 1:7:87 (R12), R11(config)#router hrld-sirt (R1,R2,R5,R10,R11,R16), R11(config-router)#neighbor < ip_addr of R16 > new rt R12 ↔ R16, out

**Fig. 16** Interconnected system clarifies by giving an example of the fifth successive route. The dotted block highlighted nodes describe the following route scenario on the proposed routing protocol.
conditions. However, 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 [23, 40, 50].

### 3.1 Proposed Attacker Detection Automation of Bees Colony Optimization (ADABCP)

In this section, the proposed Attacker Detection Automation of Bees Colony Optimization (ADABCP) uses a routing framework based on Bees Colony Optimisation that offers improved network traffic routing in the MANET scenario to improve the energy efficiency in terms of three factors [17, 19] such as routing operation, detection automation application, control parameters.

This Attacker detection automation of Bees Colony Optimization (ADABCP) deals with the Mobile ad hoc-network attacker finding technique, where mobile nodes are randomly distributed in a large field of the environment [25, 78].

The Attacker detection automation mainly applies to the MANET environment. These environments permit the nodes to communicate with each node in the MANET environment and gather information about the nodes, which is most helpful for sharing safely. This information is sent to the Base station to control the node’s activities. There are three processes used in an Attacker detection automation. The report includes sending data, receiving date, time, and communication validation.
When the node is moving, the nearby nodes and all other nodes are enabled, which gathers a surrounding of a node, and simply shows how the node ascertains its range.

The source node is capable of gathering the data of the surrounding nodes. The source node identifies the route traffic, traffic signals, and objects on the route. The nearby subsequent nodes measure the distance between the source and destination on the route. The source node will not work perfectly every time. So, this research can use the efficient location sensor to detect the object and the distance and time taken for the nodes to reach the destination. This research can identify blind-spot monitoring and node parking aids for short-range radio waves. For long-range radio waves, this research can identify an object and control the assistance.

If the node speed is greater than the speed limit, then the proposed routing system gives an alert message to the source, and then the source node reduces the node speed. Similarly, if the node speed is lesser than the actual packet speed limit, the system maintains the node speed. Observing the surroundings and data capturing process continuously happens. If the data is the same as an obstacle, the system identifies the obstacle and brakes. The system will turn according to the given direction if the input data nodes are nearby. If the right-side node direction is given as input, the system turns to the right-side node direction. If the left-side node direction is given as input, the system turns to the left-side node direction. Otherwise, the system maintains the straight route.

Nodes Activities as Per the Speed Analysis method employed in MANET to accomplish appropriate refinement on the routing issues. In comparison to the “intrusion detection automaton,” “Hybrid Random Early Detection,” and “node ranking technique,” the suggested ADABCP approach
Algorithm 1  Algorithm for working principles of nodes activities as per the speed analysis

```plaintext
input; nodes info_data
output; nodes speed analysis
while the node is moving
    enable Base station sensor
    capture data speed limit
    if (nodes speed = high)
        check → nodes in the range
        identify the nodes data
        convert → nodes speed to numerical data & send → Base station
    if (nodes speed > near mode speed)
        automatically reduce nodes speed
    else if (nodes speed < near mode speed < Actual speed limit)
        increase the nodes speed to Actual speed limit
    else
        maintain Actual speed limit
    end if
    nodes are not detected
    continuous observing
end if
capture a data of the obstacle
    if (data of obstacle = high obstacle rate)
        identify obstacle on the Route
        convert → numerical data to obstacle speed & receive → Base station
        convert → numerical data to obstacle speed numerical data → Base station
        if (detects → obstacle)
            manage → action
    end if
end if
capture data of Nearby_Next_Node
if (data = high Speed)
    identify path on the Nearby_Next_Node
    convert → numerical data to Nearby_Next_Node speed & receive → Base station
    if (sign=right side node)
        convert → numerical data to right side node speed & receive → Base station
    else if (sign=left side node)
        convert → numerical data to left side node speed & receive → Base station
    else
        maintain correct sufficient route
    end if
end if
end while
```
has finalized the secure and optimum MANET routing pathways. The number of given live movable nodes-based agile methods, namely "Use Best Approximation" and the "Swift Implicit Response Round Trip Time" mechanism, were recommended in a routing operation. This Use Best Approximation estimates the most optimal route in the most efficient way possible. Swift Implicit Response Round Trip Time can also help global optimization management [52]. The combination of “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). Our research took the rushing attacks because it allows for a denial-of-service, especially since this attack makes duplicate copy process of original mechanism and spread attacks activities to the nearby nodes route by accessing route and gain access to original sending data from source to destination [26].

The three criteria are considered in the Attacker Detection Automation of Bee Colony Optimization (ADABCP) approach. First, in MANET [73], a Routing Operation to Perform a Node Movement Within the Boundary. As a result, in the transmission environment, head nodes are picked. This is also known as node initialization. The second is a program that automates the identification of attackers to optimize the path. The Node-id determination is established whenever the head nodes of the specified transmission environment form a time limit, i.e., each node has generated individual packet transmission around the neighboring nodes. The increment values from the beginning node to the end node of a transmission environment were used to assign this Node-id determination. The nodes begin the packet transaction around the neighboring nodes based on this assessment. Suppose the node is sharing information based on inter-connectivity. In that case, the routing path is developed using communicating nodes to integrate all nodes' coordinate systems. All nodes are randomly positioned in a large transmission environment field in this period, and RREQ/RREP messages are disseminated. Each node will determine its node grade, ID, and nearby node distances in these conditions. The transmission environment initiator node is the source node with the lowest ID between nearby nodes, and the timer begins [17, 61].

Finally, control parameters are successfully used to detect automation to increase energy efficiency on the transmission environment's head node [13, 26, 33]. Suppose it gets a cluster head declaration from other nodes before the timer expires. In that case, the node will end the timer and become a member of the transmission environment. Head-node declaration messages are flooded to hops in the head-node transmission environment. This packet of RREQ/RREP messages broadcasting was discovered in two situations. First, any member of MANET is a node from the transmission MANET environment head nodes. Second, every node between the head node of the class and the MANET surrounds becomes a candidate for a new head node. A declaration message with a high time to live value is sent to some border nodes in a temporary transmission environment from the head of a nearby transmission environment. With one or more numbers, these nodes are referred to as attacker nodes. The rushing attacker node is what it's called. [3, 66, 69].

These nodes are used later in the system integration coordination procedure in the transmission environment. The transmission environment head node chooses one of these potential nodes at random. It then sends information about the targeted attacker node to the head node for the nearby transmission environment. For information from a Node-id with increment packet transaction, values examine the sender node's route and the route of the surrounding node with their environment [75].

The Attacker detection automation of the Bees Colony Optimization (ADABCP) technique provides a single relative coordinate system by merging comparative coordination systems across nodes. As a result of this consideration, each node has two neighboring nodes that overlap with each of its MANET surrounds. The relative coordinate systems of two subsequent mobile nodes are integrated into two overlapping nodes due to this process. Each head node will complete the routing using distance information based on the "Received Signal Strength Indicator" and the IDs of nearby nodes. Members of its overlapping node will back each head node. Each node belongs to at least two routes and receives relative addresses from all head nodes. This permits the aggregate node to have a close address for each of the surrounding nodes it belongs to, and it's utilized to integrate neighboring coordinate systems [28, 78].

Attacker detection automation of Bees Colony Optimization (ADABCP) was developed to overcome route optimization concerns on the MANET against rushing assaults. Route Organization and Route Reorganization are two steps of the ADABCP [22, 83]. A significant data stream is evaluated while defining Route Organization, which gets values for numerous mobile node attributes. This research uses Route Organization and Route Reorganization to optimize the Route State issue based on this consideration.

Where there are N f total characteristics on forwarding transmission between nodes, there will be 2 N f types of subsets accessible on forwarding transmission between nodes, each with a different length and parameters [29]. Each subset of parameters may be seen as a place in this space. The best position is the lowest length subset with the most negligible difference in correlation between the original set and sub-set parameters. In this scenario, a swarm of bees is introduced, which flies to the ideal location. They want to fly and change their position over time, connect, and search for the best and most optimal place globally, i.e., “Location Route Organization Node.” Convergence in the process is achieved iteratively [17, 48].
In this scenario, a swarm of bees is introduced, which flies to the ideal location. They want to fly and check their position over time, interact with one another, and search for the best and most optimal place globally, i.e., "Location Route Reorganization Node." The best position is the comparative length subset with the most negligible difference in correlation between the original set and sub-set parameters. The following algorithm can be used to achieve this optimum routing.

Algorithm 2: Algorithm for Attacker detection automation of Bees Colony Optimization (ADABCP)

$$\text{StartNode} \leftarrow \text{Mobile}_{-}\text{node1}$$
$$\text{DestNode} \leftarrow \text{StartNode(Mobile}_{-}\text{Node1)}$$
$$\text{NodeNetworkKey} \leftarrow \text{null}$$
while (start node != (Mobile_node 1))
$$\text{ParticipateNode} \leftarrow \text{null}$$
for(StartNode in NeighborNode)
if(not NodeNetwork(ParticipateNode, NeighborNode))
$$\text{NodeNetworkList} \leftarrow \text{ParticipateNode + NeighborNode}$$
end
$$\text{DestNode} \leftarrow \text{FindDestNode(ParticipateNodeList)}$$
$$\text{Mobile}_{-}\text{Node1} \leftarrow \text{DestNode(Key)}$$
for (NodeList—StartNode(NodeList=(InitialKey+RandomKey(NodeList)))
$$\text{FindDestNode(ParticipateNodeList(Mobile}_{-}\text{Node1)$$
if(NodeRoute(NodeList) > (StartNode(DestNode))
$$\text{NodeRoute} \leftarrow \text{MinPath(StartNode, DestNode)}$$
end
end
end

Algorithm 3: Algorithm for attacker detection automation of Bees Colony Optimization (ADABCP)

$$\text{MinPath(Node)} \leftarrow \text{Route Factor(NodeNetworkList)}$$
$$\text{Route \_Factor} \leftarrow \text{ThresholdValue (StartNode!=CA, DestNode| NeighborNode)}$$
for(Route \_Factor = StartNode!=CA && StartNode=MaxPath(NodeList) — DestNode(Node(NeighborNode, NodeList(DestNode + 1),
NodeList(NeighborNode + 1))
$$\text{MinPath(ListNode)} \leftarrow \text{MinPath(Route \_Factor)}$$
while(Route \_Factor(NodeList) > Network Size)
$$\text{NodeRoute (ThresholdValue(StartNode!=CA, DestNode| NeighborNode))}$$
$$\text{MinPath} \leftarrow \text{(ThresholdValue (StartNode|DestNeighborNode))}$$
$$\text{MinRoutePath} \leftarrow \text{MinPath}$$
end
return (MinPath)

Algorithm 4: Algorithm for proposed routing protocol: (Rushing Attack)

Manage: Path Route Attacker
Avail in Route
Route Reorganization → Positive
Gives
Malicious Node : Positive
$$\text{do :}$$
pkt(<<Route Reorganization | pkt send to location disclosure | traffic pattern | actual pattern>>) as network node,
result value is Route Reorganization

Algorithm 5: Algorithm for route reorganization

Route Organization (sent pkt 1 | receive pkt 1 | target packet 1)
end : node recognize
$$\text{do :}$$
The same as another network
infected
$$\text{malicious node}$$
while : Route organization (sent pkt 2 | receive pkt 2 | target pkt 2)
End with (N Packets,1 time)
Node: select → attacker → positive,
Do: Route Reorganization
Through node
For discovering the Rushing Attack, the following five algorithms offer a Route Organization, and Route Reorganization based Routing Protocol [16, 18, 31, 48]. Following the detection of a Rushing Attack on a MANET path, the path selection might be completed using the Swift Implicit Response Round Trip Time mechanism-based secure path selection [35]. This approach generates an effective communication path after avoiding rushing attacks. This technique determines if the communication node is active or not. The nodes create rushing assaults if they are dormant. Thus attackers appear in the routing path [80, 83].

3.2 Swift Implicit Response Round Trip Time (SIRT) Mechanism

The Route Organization and Route Reorganization-based Routing Protocol are unsatisfactory packet broadcasting among the nodes in the transmitting environment [32, 37]. Because the attacker node abruptly changed its mode of operation by lowering the packet delivery ratio. Our proposed research aims to discover and eliminate the impacted communication channel from the Swift Implicit Response Round Trip Time (SIRT) mechanism, which would fix this transformation. By employing the SIRT mechanism technique, nodes allow a secure node with a better transmission rate to operate.

3.2.1 SIRT Mechanism

This will be expressed in the MANET network by employing stable path construction and continuous routing. The attacker-free path with the uncommon nodes delivery time is identified by the Swift Implicit Response Round Trip Time (SIRT) Mechanism-based secure path Selection technique. Every node in the routing path has its node data stream status monitored using the Attacker detection automation of Bees Colony Optimization (ADABCP) algorithm [33, 78]. This aids in increasing the SIRT Mechanism’s packet delivery ratio. To reduce the misbehavior of attacker node transmission, every node must lower the abnormal route detection with the node’s usual behavior—this aids in updating the insecure route between communication nodes via the routing path.

The mobile nodes in a MANET do not update their position as frequently in this situation. If the procedure requires establishing a secure connection node, the route’s path flow has been adjusted energetically to prevent harm to nodes (attackers) in the particular course. The relay node, responsible for the attacker’s destruction, logically restores the route. Using the “Use Best Approximation” method, this rushed attacker kills the process that affords closer to the target node in the routing path. The MANET provides the Static route with continuous routing by Use Best Approximation [36].

3.2.2 Use Best Approximation

When the sender refuses to transmit the route, the recipient node repeatedly receives packets from the sender. The proposed Static route with continuous routing was used to avoid that communication. These ongoing routing packet delivery communications aim to convey many control packets to their destination. The traffic density rose due to the large packets on the static path. The minimal packet delay for data transmission was allowed to avoid traffic occurrence on the network [15]. This minimal packet delay transmission prevents undesirable extra data packet broadcasting in the MANET system. This procedure aids in the reduction of data corruption and wormhole attackers while also increasing packet delay.

This study uses Hybrid Random Late Detection (HRLD) to limit the efficacy of rushing attacks and lengthen the data delivery time interval to facilitate data transmission against the rushing flagging procedure [10]. These HRLD models were created to provide secure data transfer [41, 42, 48 Against the rushed flagging protocol, this approach assures data delivery over a secure channel.].
routing. This suggested method ensures effective transmission across a network with no infrastructure. Furthermore, the Attacker Detection Automation is utilized to find the right attackers. The suggested Swift Implicit Response eliminates MANET routing congestion communication. The first matching with other nodes is used to automatically reduce an attacker using the "Swift Implicit Response Round Trip Time" method.

By employing interaction history in a well-organized manner, the limited route may be used to discover an effective solution for dead node reduction and active links node boost-up [3, 37, 40]. The time interval assignment determines how the dead node reduction and active links node boost-up are handled. By employing a critical assignment, each node will allocate time for replying to the sender node. The transmitted node will send reply messages to the transmitting node within the set time interval to prove node confirmation. For one-way communication, this confirmation helps to decrease the end-to-end latency. Routing efficiency is maintained via route interaction to reduce performance deterioration. This routing strategy aids in the secure and intelligent discovery of the best routing. Finally, each transmission's node rating is derived from the previous contact history. In addition, the Attacker detection automation is executed concurrently for updating the Dead node and active connections [38]. These changes are made to the history of previous interactions. The cyclic processes of node ranking represent the continuous monitoring system of an "infrastructure-less network," resulting in an enhanced alternative to current tactics. The standard routing path on Mobile Ad Hoc Networks is not a proven path for the entire period of data transmission in this continual circular operation [15, 39].

3.3.1 Mechanism Against the Late Detection

The routing protocol of mobile nodes mentions late detection algorithmically. In most critical situations, mobile nodes share important messages over the network via end-to-end communication via a data-transfer application [42, 55, 76]. This study conducted a survey based on the benefits of two-way communication, such as node-to-node and node-to-controller communication. These two types of communications each have issues in enabling reliable and secure data flow between nodes or between nodes and controllers.

3.3.2 Hybrid Random Late Detection (HRLD) Routing Protocol

This study uses the following two assumptions to design the Hybrid Random Late Detection (HRLD) routing protocol. On the MANET, the HRLD routing protocol is primarily intended for path optimization [49, 78].

Increase the packet delivery ratio of each node and reduce packet delay on specified routes from the Past Interaction History (PIH) to construct node transmission range patterns [58, 65]. The same technique was used for a different group to improve the routing protocol for each subsequent zone [61]. These approaches also aid in determining the network's transmission acceleration, regardless of whether the node is transmitting data or not. The transmission speed is calculated using the node transmission accelerate Table 1 below. The target node path will be placed in the node transmission accelerate table using the proactive protocol after establishing a node route without any intrusion.

The suggested data transmission acceleration techniques have also been tested against the routing protocol [67, 76]. The nth destination address for MANET completion was discovered using this protocol. The input Ratio Range for Bandwidth Modulation was guaranteed based on the MANET Environment scenario.

i. Route finding and time confine

This route finding and time confinement took the communication between the sender and receiver to find the exact route between the source and destination by the get_route(). The two aspects were considered for forming Sender-receiver path manipulation [77]. Firstly, the mobile node was checked based on the node lifetime and energy. These mobile node platforms continuously correspond to the route based on the switch inputs over the broadcasting of the packet signal to the nearby nodes.

ii. Sender-receiver address status

This Sender-receiver destination addresses status was taking the communication over the Ratio Range and Data Rate of SDN for finding the exact route between the sender and receiver by the Include find (). The next possible nearby node is summarized concerning the throughput of each ratio range and the data rate of each transaction. The two conditions were considered for forming the destination of particular data transmission.

3.3.3 Route Finding Manipulation (RFM)

Is routing or data communication assisting to improve MANET communication with the environment in demand, or are MANET making the route determination into offering "RFM?". This research committed this demand with the "Hybrid Random Late Detection (HRLD)".

The Route Finding Manipulation (RFM) is elementary support for the sender and receiver and the middle node.
Route Finding Manipulation supports precisely the best route from the sender to the receiver. It considers the significance of the contribution to data communication. The Route Finding Manipulation is formed below.

The Sender-Receiver Destination Addresses MANET Routing Protocols for Path Nodes were explored in this method. A MANET’s mobile nodes do not regularly update their position [2, 77, 79]. If the process requires establishing a secure connection node, the route’s path flow has been adjusted energetically to avoid damaging nodes (rushing attackers) along the identical route. The relay node, responsible for the attacker’s destruction, logically restores the route. This rushed attack destroy procedure gets you closer to the routing path’s target node. When the sender refuses to transmit the route packets, the receiver node receives them again from the sender. The suggested Hybrid Random Late Detection (HRLD) routing Algorithm was used to avoid that communication. The goal of these continuous routing packet delivery communications is to convey many control packets to their destination. The rush traffic rose due to the large packets on the static path. Data transmission was restricted to a minimal packet delay to reduce network congestion. This minimal packet delay transmission prevents undesirable extra data packet broadcasting in the MANET system. This method aids in the reduction of data corruption and rushing attacks while also increasing packet delay [20, 56, 66].

The proposed approach is utilized to find the attacker’s precise maximum and quantity of damage routes. All nodes in the MANET network identify as the intermediary node with the lowest TTL value in between this damage route. This intermediate node indicates the malicious attackers’ nodes within the node frequency coverage area. Details about malicious attackers’ nodes are broadcast across the network, even to destination nodes. This article presented the Static route with continuous routing to avoid these dangerous actions.

Moreover, compare each node’s features in the network to assess anomalous behavior; a high score indicates hateful conduct, whereas a low score indicates an efficient node. Each destination node’s connection setup data are stored in the destination node. The ability to identify hostile nodes from routing nodes in the network environment is aided by network information that includes details for each link’s current quality level [17]. Some nodes are removed from routing paths in this era based on packet transmission speed and routing speed-accuracy rate. The quality of service paths helps for any failure node. The destination node contains all details to start a pattern recognized to the link with low packet latency without malicious nodes. The quality service paths help for any failure node. The destination node contains all details to start a pattern recognized to the link with low packet latency without malicious nodes.

The destination node arranges this information through the routing path intermediate nodes by exchanging dual procedure packets with the remaining nodes. It is the promise that the facts of the network state are contained each to restore prior routes and start initially by exclusive of the rushing attacker nodes, for more likelihood and minimum traffic. Malicious nodes can facilitate data limitation to a more stable routing path than the remaining pathways, which reduces packet transmission traffic and improves network longevity [37, 54].

### 3.4 Performance Analysis Discussed from Social Distancing Alarm (SDA)

Social distancing is the foundation of COVID-19 prevention. Social Distancing Alarm (SDA) has been introduced to counter the social distancing during the pandemic to prevent the invasion of health issues. Social distancing has focused on diminishing vulnerability to public health and sustenance of one meter (three feet) distance as the primary natural object corresponding to people [72, 76]. The careless imperfect social space is one where there is a chance of exposure or contact, as can be caused in the public place [27, 46, 62, 75]. WHO standards policies, including lockdown and unlocking, have been carried out across India to alleviate the social distancing process. Central and state governments, health departments, and every citizen have access to quickly adapt to these pandemic measures, often in absence of experience and direction [48].

| Network Id | Next hop | Current node to gateway | Cost | No.of. route on the gateway |
|------------|----------|-------------------------|------|-----------------------------|
| Network destination | Net Mask | Gateway Interface | Metric |                                  |
| 0.0.0.1 | 0.0.0.10 | 192.130.10.10 | 192.130.10.0 | n R1 |
| 125.0.0.0 | 232.0.0.10 | 197.1.1.10 | 197.120.10.10 | n R2 |
| . . . . . . | . . . | . | . | . |
| 198.162.0.1 | 255.255.255.255 | 198.162.0.100 | 198.162.0.142 | n Rr |
This research has given the procedural aspect and integrated technologies names as social distancing alarm with sensors accomplishing COVID-19 prevention to maintain this issue. This social distancing alarm helps focus on the mobile devices/ intelligent personal assistant devices that have been contemplated with the intervention communication, monitoring, remote location, screening, and user outreach. In this social distancing alarm, the automatically-reacting notice can also be being incorporated into mobile devices/intelligent personal assistant devices, such as by making distance alarms and routing customers to conquer place or next gateway for shopping based on availability [71, 80].

3.4.1 Automatically-Reacting Alarm

An automatically-reacting alarm is a non-wearable remote sensor device that can help make the distance in a particular moving object, especially in human behavior monitoring such as distance, vital signs, etc. Automatically reacting sensors track movement activity, temperature, breathing, and coughing symptoms. The automatically-reacting alarm resolves the addressed potential issues quickly like customer engagement, device costs, ethical monitoring, risk monitoring, and staffing demands [70]. Automatically reacting sensors also are used to route supervising and keep social distance [64, 69]. This process is also called the Digital Contact Tracing (DCT). The DCT can help to make the social distancing between customers amongst COVID-19 patients and healthy customers by distinguishing whether people have been social/ physical distancing by measuring spaces among two or more mobile devices/intelligent personal assistant devices. Nevertheless, the digital contact tracing examines results is helps to remotely monitor customer and keep them shopping more without any fear and suspicion. Even though, this research has worked and formed the applied tools above to help remotely monitor customer and their use in an effective manner [74].

Trends in the carrying out of automatically-reacting alarm process. On the place of SDA1, initial node ranking will be made; At the same instant, on the position of SDA2 monitoring user location with a device; SDA3

---

Algorithm 7 Algorithm for Hybrid Random Late Detection (HRLD) routing

**Input:** Ratio.Range, Data Rate, Bandwidth Modulation, Mobile Platform, throughput, switch inputs, MANET completion (C)

**Output:** Efficient Data Transmission

- \( C = \text{getRoute}(\text{Sender node communication}, \text{Receiver node communication}) \)

- **Process:** by default: Mobile Platform \( \leftarrow \) Null connection
  MANET Environment || operating system (starting position(C))
  \( \text{route} (r) = [\text{Null connection}] \leftarrow \text{switch} \) inputs (Open)
  While (Mobile Platform active node \( < \text{switch} \) inputs (route (r))):
    For Route Estimation in route (r) do
      Route.Estimation. deductSourceNode (MANET completion C)
      throughput = []
      While (possible.Near.Node = End position(C))
        If (Sender node communication = ProValve(throughput))
          throughput = ratio of favourable cases(C)
          Else
            Ratio.Range = getPossibility(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\(\neq\)throughput = [])
        nextNode = Call Include find()
      Else
        possible.Near.Node = End position(C)
        If (Receiver node communication\(\neq\)ProValve(throughput))
          throughput = Acknowledgement probability(getRoute)
        Else
          find:next_possible.Near.Node \(\neq\) throughput (Ratio Range|| Data Rate)
          If (next_possible.Near.Node\(\neq\)throughput = [])
            nextNode = destination node ()
            nextNode.append(destination node ())
          End
          Route.append((destination node ()))
        End
        nextNode +
      End
  End
**return efficient data transmission**
normal response to implicit response; SDA4 maintaining distance with the social distance navigator; SDA5 reroute next path row; SDA6 regular route; SDA7 getting authorized investigator; SDA8 avoidance of crews; aero mark indicates the path between each row (Fig. 21).

An automatically-reacting alarm has the following properties to make the social distancing of individual customers across the shopping center. The following terms are applicable to create the perfect social distancing [30, 55, 60].

i. **Ability Outstripping Indicator (AOI)**

This Ability Outstripping Indicator (AOI) establishes how persons that make the distance with the neighbor have the hierarchy of distance tree and route among the crews of a shopping center or any public place. The higher ability outstripping indicator indicates a substantial walking order in the distance tree and route (Young and Schneider 2020).

ii. **Doubt Preventing Indicator (DPI)**

Doubt Preventing Indicator (DPI) represents that persons are unpleasant or unknown. Therefore, this preventing indicator can effectively conquer persons with a minimum distance that a group favors representation in an interpretations manner [39, 71].

iii. **Individual Versus Grouping (VGI)**

This Individual Versus Grouping (VGI) strengthen and support individual or behaviors.

An individual's entry is chosen to initiate customer identification details with personal details. When some time allocations (TA = 30 min) are formed, a contact partner also checks with neighbor probability distance (one meter (three feet)) with the following networks that result from maximizing distance-reduction strategies [32, 72].

Fig. 21 Prudent infrastructure with the help of Simultaneous Optimization (SO) and Imprecise Ramification (IR)
If either single customer is not maintaining the distance from others and the other is also not warned by an alarm. Since, among all individuals in the simulation, those who are not keeping the space for more than 30 s to the nearby person are in the warning stage for more than 30 s [83]. Hence the alarm gets continuous warning exposed with minimal probability distance. Therefore, Individuals who were warned were alarmed by the least possible space. On the foundation of the automatically-reacting alarm, the minimum length is ordinarily set to determine position limits or a fixed distance (one meter (three feet)) of crowding behavior in the assortment of directions (DV) [59, 70]. These algorithmic steps are repeated until all susceptible might change the position described in Fig. 22.

The simulation model discussed the customer experience crowd viewing behaviors in an assortment of directions is not sufficient to make the fixed distance (one meter (three feet)); hence, it is crucial to look into the actions and activities that customers experience crowd viewing behaviors on in identifies and a different location [79]. Prompted by these two existences, ad-hoc network-based sensors on social distancing towards the public environment are formulated in this research phenomenon, which inhibited both social distancing and Social Distancing Alarm (SDA). We attempt to study the relationship between sensors-based social distancing and manual social distancing without staff management. By comparing the social distancing follower’s ratio, we can obtain that both sensors-based and manual social distancing had equal influence [32, 72].

However, on a day-to-day basis, the social distancing follower’s ratio was increased based on the sensors-based social distancing model. These experiments are given by objects moving through the shopping mall of customers and an informal photograph of the sensors-based social distancing process [56, 73, 74]. Furthermore, the consequences of sensors based social distancing for different customers are examined scientifically, which are primarily manifested by the maximum distance reduction that is shown in Fig. 23.

Figures 23, 24, and 25 represents the behavior with the Embedding sensors-based social distancing model is works based on birds clustering in 3D space. The form of each customer is set as one meter (three feet) circular region, but the neighbor and some other obstructions will block part of the specific environment.

3.4.2 Imprecise Ramification (IR)

i. Temporary sudden disposal of the misbehaved customer

The temporary sudden disposal of the misbehaved customer is based on the behavioral activities of the customers. The following procedural aspects are used to yield the misbehaved customer separation [61, 79, 83]
ii. Initial distance maintenance of customers

An initial distance can follow while entering in into the shopping mall. In this research aspect, the most extensive principles of the social distancing notification distribution measurements were used. In distinction from others, that social distancing consists of the least possible one-meter (three feet) ranges in diameters from one another [57].

iii. Nearby Obstruction Conditions

Nearby obstruction comes, once the customer crosses the involving spatial location, it has been recorded as the disobeys activities on the environment [59].

3.4.3 Sensors Based Social Distancing Model

Sensors-based social distancing model is shown to reproduce customer (i) behavior against the movement of neighbor in the nearby obstruction conditions. Different from the initial distance maintenance (DV) in a normal temporary sudden disposal of the misbehaved customer (j) that knows the position of the exit and the desired directions point (fi) is described in the following Fig. 26 [69]. Customer will change their position after seeing the boundary to avoid touching the neighbor [15, 24, 63].

3.4.4 Factors on Embedding Sensors Based Social Distancing Model

In this place, concisely discuss the factors that affect the sensors-based social distancing position.

Figure 26 represents the behavior with the Embedding sensors-based social distancing model based on birds clustering in 3D space. From the position of each node is called a source (i) which is represented in the 3D X–Y–Z coordinates area as a point. The node relative coordination systems concept is used to find an objective neighbor (k). Each node experiences the best value (pbest) and its current position. Each nearby neighbor (j) and its nodes know the global best value (gbest). The function of each actual source node is modified using velocity (dv), and the speed of each neighbor node (δ(i,j)) is calculated by Eq. 2 and Eq. 3

\[
\delta(i,j,k) = \delta(i,j) + \delta(i,k) - \delta(j,k)
\]

\[
(d_v)_{(i,j)\text{(act src node}}} = \left[\text{Dist}_\text{act src node}\right] \left[\delta(i,j)\text{(actual source)}\right] + \left[\text{Dist factor}_\text{act src node}\right] \left[\text{random number}_\text{act src node}\right] + \left[\text{random number}_\text{act src node}\right] \times (gbest - \left[\text{current position}_\text{act src node}\right])
\]

Fig. 23 Symbolic form of field (block dotted) customer with sensors

Fig. 24 Representative diagram of “social distancing” behavior

Fig. 25 Representative diagram of “social distancing”
\[ \delta(i,j,k) = \delta(i,j) + \delta(k,j) + \delta(j,k) \]

where \( \delta(i,j)(act_{src}_{node}) \) is the actual source node velocity \( i \) at iteration \( k \), simultaneously \( \delta(i,j)(neigh_{node}) \) is the neighbor node velocity \( i \) at iteration \( k \), and \( Dist_{act}_{src}_{node} \) and \( Dist_{factor}_{neihg}_{node} \) are distance concerning the random numbers between 0 and 1, \( currentposition_{k} \) is the current position of actual source node \( i \) at iteration \( k \), \( pbest_{act}_{src}_{node} \) and \( pbest_{neihg}_{node} \) is the pbest of an actual source node and neighbor node \( i \) and \( gbest \) is the best value so far in the group among the pbest of all source nodes and neighbor nodes. The distance function is calculated as following Eq. 4 and Eq. 5.

\[
D_{cn} = \text{Tot\_nod\_cnt} - \frac{\text{nodcnt}_{ini} - \text{nodcnt}_{final}}{\text{Rutecnt}_{i\_tern}} \times \text{curr\_tern} \\
D_{nn} = \text{Tot\_nod\_cnt} - \frac{\text{nodcnt}_{nn} - \text{nodcnt}_{nn}}{\text{Rutecnt}_{i\_tern}} \times \text{succ\_tern}
\]

where, \( D_{nn} \) is the Dist_{neihg}_node and \( \text{Tot\_nod\_cnt} \) is the Total\_nod\_cnt, the \( \text{nodcnt}_{ini} \) – \( \text{nodcnt}_{final} \) is the initial and final node count. \( \text{Rutecnt}_{i\_tern} \) is the maximum iteration number and \( \text{curr\_tern} \) is the current iteration number and \( \text{succ\_tern} \) is the next iteration number. Most researchers select a single test pad position of a prominent that contains the independent users. That single test pad position provides a single nearby neighbor identification only. Hence it could not accomplish regular maintenance of social distance at all times [49, 50, 80].

A prominent customer's single test pad position: More than one test pad position nodes are close by, as shown in Fig. 26. The number of sensor nodes \( i,j,k \) Typically, enhancing the number of position \( i',j',k' \), \( i'',j'',k'' \), \( i''',j''',k''' \) will amend the performance notice the nearby neighbour. An extreme point is explained in Eq. 6.
The above constitutive leads to maximum distance from neighbor. Simultaneously, in the other cases (Eqs. 7, 8 and 9),

\[ \delta(i,j,k) = \delta(i) + \delta(k) \delta(j,k) \]  
\[ \delta'((i,j,k)) = \delta'(i,j) + \delta'(i,k) \delta'(j,k) \]  
\[ \delta''((i,j,k),m) = \delta''(i,j,m) + \delta''(i,k,m) \delta''(j,k,m) \]  
\[ \delta'''((i,j,k),m) = \delta'''(i,j,m) + \delta'''(i,k,m) \delta'''(j,k,m) \]  

This constitutive represents computing's most inadequate neighbor. This process is shown in the following algorithm [34].

From Eq. 1 to 4, novel work called embedding sensors based social distancing model, for figuring the most inadequate distance with a neighbor on any position [34]. In this research, a node pair \((i,j)\) and position \((i,j,k)\) are used to discover a nearby node closer to the source node. The proposed universal position in a global embedding sensors-based social distancing model finds the approximate shortest distance between source and destination. It is computed as the sum of their lengths to all participating customer positions. Consequently, sensors-based social distancing measures have focused more on the following criteria. To measure the social distance the sound signal has traveled, we use the formula:

\[ \delta_{i,j,k}^{(T \geq t)} = \delta \left( \sum_{i,j,k=1}^{m} \frac{(i-j)^2 \delta(i,j,k)}{2 \delta(i,j,k)^2 + 1} \right) \]  

Algorithm 8 Algorithm for Sensors distance schema validation procedure

| Line | Code | Description |
|------|------|-------------|
| 1    | δ(i,j,k) = δ(i) + δ(k) δ(j,k) | (6) |
| 2    | δ'(i,j,k) = δ'(i,j) + δ'(i,k) δ'(j,k) | (7) |
| 3    | δ''((i,j,k),m) = δ''(i,j,m) + δ''(i,k,m) δ''(j,k,m) | (8) |
| 4    | δ'''((i,j,k),m) = δ'''(i,j,m) + δ'''(i,k,m) δ'''(j,k,m) | (9) |
| 5    | Algorithm for Sensors distance schema validation procedure |

 Springer
\[ \delta_{i,j,k}(T > t) = \frac{\delta^2}{2\pi^2} \left( \sum_{t=0}^{\infty} \frac{(t-1/2)^2}{2(t+1)} \exp \left( -\frac{\delta}{T} \right) \right)^{1/2} \]  

(11)

Equation 6 describes the probability of maximum distance between the object concerning the T time and position \( c \) [15].

Measure 2: Cautionary advice in a direction opposite to going out of a whole shopping complex.

The distance between the origin and the neighbor region approaches infinity. This condition returns the vents people from highly affected regions such from shopping.

\[ \lim_{ML \to \infty} \frac{1}{ML^2} \log \delta_{i,j,k} \left( T_{ML}^{(\delta_{0,i})} \leq T \right) = -\frac{1}{2T} \]  

(12)

The distance between the origin and the neighbor region approaches infinity. This condition returns the vents people from highly affected regions such from shopping. This nearby obstruction is calculated based on Eq. 12.

\[ \lim_{ML \to \infty} \frac{1}{LN^2} \log \delta_{i,j,k} \left( T_{ML}^{(\delta_{0,i})} < T \right) = -\left( \frac{1}{2T} \right)^0 \]  

(13)

Here the Minimum Distance (ML) between origin and the destination region comes near to specified maximum distance of nearly one meter (three feet) [48, 77].

Measure 3: distance measures by self. This measure prevents people from highly affected regions such from shopping.

The distance between the origin and the neighbor region approaches infinity. This condition returns the vents people from highly affected regions such from shopping.

\[ \lim_{ML \to \infty} \frac{1}{LN^2} \log \delta_{i,j,k} \left( T_{ML}^{(\delta_{0,i})} < T \right) = -\left( \frac{1}{2T} \right)^0 \]  

(14)

Here the Neutral distance (LN) between origin and the destination region comes near to a specified Maximum length (D), nearly more than one meter (three feet).

This nearby obstruction with maximum distance is calculated based on Eq. 15

\[ \lim_{ML \to \infty} \frac{1}{LN^2} \log \delta_{i,j,k} \left( T_{ML}^{(\delta_{0,i})} < T \right) = -\left( \frac{1}{2T} \right)^0 \]  

(15)

From the above notation, the social distancing alarm form of the following derivation (Eq. 16).

\[ \text{SDA}^{\delta_{0,i}}_{(t)} : t \geq 0 \forall \delta_{0,i}, i = 1, 2, 3, \ldots D \]  

(16)

There are the following determines available in the social distancing alarm (Eq. 17)

\[ \delta_{i,j,k}(T_{ML} > T) = \begin{cases} \text{SDA}_{(t)}^{\delta_{0,i}} & \text{if } t \leq 0 \\ \text{SDA}_{(t)}^{\delta_{0,i}} & \text{if } t > 0 \end{cases} \]  

(17)

Initialization: \( t \leq 0 \)

The following conditions are available in the maximum social distancing in the initial stage (Eq. 18).

\[ \text{SDA}_{(t)}^{\delta_{0,i}}_{(\text{D} = 0)} \text{ when } t = 0 \]  

(18)

In this stage (Eq. 19), the proposed system produces the two possible distances, such as

\[ \left\{ \text{SDA}_{(t)}^{\delta_{0,i}}_{(D = 0)} \text{ and } B_{(t)}^{\delta_{0,i}}_{(D = 0)} \right\} \]  

(19)

From (from Eq. 20 to Eq. 30) Starting condition: \( t > 0 \)
Here \( t = 0, 1, 2, 3, \ldots, 30 \)

Because

\[ \left\{ \text{SDA}_{(t)}^{\delta_{0,i}}_{(D = 0)} \text{ and } B_{(t)}^{\delta_{0,i}}_{(D = 0)} \right\} \forall \delta_{0,i} = 1 \text{ for minimum distance and } \delta_{0,i} > 1 \text{ for maximum distance} \]  

(20)

\[ T_{ML}^{(\delta_{0,i})} = \min \left\{ T_{ML}^{(\delta_{0,i})}, T_{ML}^{(\delta_{0,i})}, T_{ML}^{(\delta_{0,i})}, \ldots, T_{ML}^{(\delta_{0,i})} \right\} \]  

(21)

\[ T_{ML}^{(\delta_{0,i})} = \max \left\{ T_{ML}^{(\delta_{0,i})}, T_{ML}^{(\delta_{0,i})}, T_{ML}^{(\delta_{0,i})}, \ldots, T_{ML}^{(\delta_{0,i})} \right\} \]  

(22)

\[ T_{ML} = \left\{ t > 0 : \text{SDA}_{(t)}^{\delta_{0,i}}_{(D = 0)} \geq \text{LN} \text{ or } \text{SDA}_{(t)}^{\delta_{0,i}}_{(D = 0)} \geq \text{LN} \right\} \]  

(23)

\[ T_{ML}^{(\delta_{0,i})} = \delta_{i,j,k} \left( \max \left\{ T_{ML}^{(\delta_{0,i})}, T_{ML}^{(\delta_{0,i})}, T_{ML}^{(\delta_{0,i})}, \ldots, T_{ML}^{(\delta_{0,i})} \right\} < T \right) \]  

(24)
\[(T_{ML}^{(δ_{i,j,k})}) = 1 - \left[ \begin{array}{c} \delta_{(i,j,k)} \left( \max \left\{ T_{ML}^{(δ_{i,j,k})} > T \right\} \right) \\ \delta_{(i,j,k)} \left( \max \left\{ T_{ML}^{(δ_{i,j,k})} > T \right\} \right) \\ \ldots \\ \delta_{(i,j,k)} \left( \max \left\{ T_{ML}^{(δ_{i,j,k})} > T \right\} \right) \end{array} \right] \] (25)

1 - \left[ \begin{array}{c} \delta_{(i,j,k)} \left( \max \left\{ T_{ML}^{(δ_{i,j,k})} \right\} \right) \\ \frac{D}{ML} \end{array} \right] = -\left( \frac{1}{2T} \right) \frac{D}{ML} \tag{26}

\[\lim_{LN,ML \to (0, \infty)} \left( \frac{1}{(LN)^2} \right) \log \delta_{(i,j,k)} \left\{ T_{ML}^{(δ_{i,j,k})} < T \right\} \] (27)

\[\lim_{LN,ML \to (0, \infty)} \left( \frac{1}{(LN)^2} \right) \log \delta_{(i,j,k)} \left\{ T_{ML}^{(δ_{i,j,k})} < T \right\} = \lim_{LN,ML \to (0, \infty)} \left( \frac{1}{(LN)^2} \right) \log \delta_{(i,j,k)} \left\{ \frac{D}{ML} \right\} \left\{ T_{ML}^{(δ_{i,j,k})} < T \right\} \] (28)

= \lim_{LN,ML \to (0, \infty)} \left( \frac{1}{(LN)^2} \right) \log \delta_{(i,j,k)} \left\{ T_{ML}^{(δ_{i,j,k})} < T \right\} \frac{D}{ML} \tag{29}

= \left( \frac{1}{2T} \right) \frac{D}{ML} \tag{30}

Granting the above equation, the precise maximum distance between the origin and destination region becomes the maximum distance such as sensor nodes usable amongst two different locations [1], if the distance of the ML is maximum sufficiency, we have

\[\left( \frac{1}{2T} \right) \frac{D}{ML} \forall \delta_{(i,j,k)} \left\{ T_{ML} \leq T \right\} \cong e - \left( \frac{ML^2}{2T} \right) \frac{D}{ML} \tag{31}\]

The above distance formation demonstrates the limiting behavior of social distancing in the maximum distance that is to say D/ML. Here ML is taken as the maximum distance in the region even the same as in minimum distance calculation. This observation indicates that the extremely maximum distance origin improves the social distance (Eq. 31).

## 4 Result Discussion

In computer simulation to examine the about to be mentioned below specified execution factor that defines a system and determines its performance are using X graph in ns2.34 [83].

### 4.1 End to End Delay

Figure 27 demonstrates end to the end delay is calculated by the quantity of time taken for packet transmission from sender to receiver, all node connectivity stored by past integration history. In the Proposed "Optimal Aggregation of Attacker detection automation of Bees Colony Optimization" method [2] packet latency is cut down compared to the existing method ESCT—Cai et al. [12], ENM-LAC—Liu et al. [53] and ZRDM-LFPM—Khudayer et al. [47].

End to End Delay = End Time – Start Time * 100 \tag{32}\]

From Eq. 32, a mechanism is to consider mobility variation/ skew 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 Swift Implicit Response Round Trip Time (SIRT) framework. This was improving the efficiency of assigning sources in the routing process. Here we have used 100 samplings to discover the number of packets to be delivered. Also, this research implemented Hybrid Random Late Detection (HRLD) approach in a MANET environment and evaluated it by some well-known attackers [75].

Figure 27 demonstrates the simulation result of End to End Delay (ms) inference for Existing ESCT—Cai et al. [12], ENM-LAC—Liu et al. [53], and ZRDM-LFPM—Khudayer et al. [47] system with Proposed SIRT – ADABCP- HRLD System. The Proposed SIRT – ADABCP- HRLD system shows the End to End Delay (ms) of the Existing system has obtained high compared to the proposed system, due to attacker free contributions. The simulation result of End to End Delay (ms) for the proposed SIRT – ADABCP- HRLD System and existing schemes like ESCT—Cai et al. [12], ENM-LAC—Liu et al. [53], and ZRDM-LFPM—Khudayer et al. [47]. It shows the End to End Delay (ms) of proposed SIRT – ADABCP- HRLD has obtained less high position End to End Delay (ms) compared to others, due to high attacker less result. The performance evaluation results of SIRT – ADABCP- HRLD with existing methods in terms of low End to End Delay (ms) of 49.8361% compared to existing methods.
4.2 Communication Overhead

Figure 28 establishes communicating overhead is minimized in which source forward packet to an intermediate node, proposed SIRT–ADABCP-HRLD System provides secure and attacker free route path. In the proposed method communication overhead is minimized compared to Existing ESCT, ENM-LAC, and ZRDM-LFPM Methods.

From Eq. 33, the Swift Implicit Response Round Trip Time is to consider Pause Time indicating the higher pass time over the network with the exact route on the MANET environment, which examines against the overhead and node lifetime. The above graph is used to

\[
\text{Communication overhead (Number of Packet Losses/Received)} \\
\times 100
\]  

(33)

Fig. 27 Graph for end to end delay

Fig. 28 Graph for communication overhead
reduce the Communication Overhead by presenting the Swift Implicit Response Round Trip Time (SIRT) framework. This was improving the efficiency of assigning sources in the routing process. Here we have used 100 samplings to discover the number of packets to be delivered. Also, this research implemented Hybrid Random Late Detection (HRLD) approach in the MANET environment and evaluated it by some well-known attackers. To 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 has obtained high compared to the proposed system, due to the efficient route between nodes.

Figure 28 shows the simulation result of Communication Overhead for the proposed SIRT–ADABCP-HRLD System and existing schemes. It shows the Communication Overhead of proposed SIRT–ADABCP-HRLD has obtained low Communication Overhead compared to others, due to high attacker less result. The performance evaluation results of SIRT–ADABCP-HRLD with existing methods in terms of low Communication Overhead of 81.4462% decrease compared to existing methods.

4.3 Packet Delivery Ratio (PDR)

Figure 29 demonstrates the Packet delivery ratio is assessed by a packet received quantity from a packet sent count especially distinguished from other node region rates. Node speed is a constant in MANET; the simulation rate is fixed at 150 ms. In the proposed method Packet delivery ratio is enhanced compared to the existing ESCT, ENM-LAC, and ZRDM-LFPM methods.

\[
\text{Packet Delivery Ratio} = \frac{\text{Number of packet received}}{\text{Sent}} \times \text{speed}
\]

From Eq. 34, the SIRT is to consider the number of nodes indicating the higher delivery ratio over the network with the exact route on the MANET environment, which examines 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 was improving the efficiency of assigning sources in the routing process. Here we have a test with the 50 samplings to discover the number of packets to be delivered per minute. The result of Packet Delivery Ratio Inference for Existing ESCT, ENM-LAC, and ZRDM-LFPM system with Proposed SIRT–ADABCP-HRLD System. The Proposed SIRT–ADABCP-HRLD System shows the Packet Delivery ratio of the Existing system has obtained high compared to the proposed system, due to efficient packets delivery source and destination nodes. Figure 29 shows the simulation result of the Packet Delivery ratio for the proposed SIRT–ADABCP-HRLD System and existing schemes. It shows the Packet Delivery ratio of the proposed SIRT–ADABCP-HRLD has obtained a higher quantity of packets Delivered to the destination compared to the others, due to lower attacker less result. The performance
evaluation results of SIRT–ADABCP-HRLD with existing methods in terms of a high Packet Delivery Ratio (PDR) of 42.2262% increase compared to the existing methods.

### 4.4 Network Lifetime

This has been calculated by processing time for normal nodes to become dead nodes. i.e., the time taken to energy supply by any participating nodes is referred to as the Network lifetime. Figure 30 manifests the lifetime of the network is estimated by the total process of the proposed system network, effort employed to done communication successfully. In the proposed method network lifetime is enhanced 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 spent on routing protocol communication. This proposed Attacker detection automation of the Bees Colony Optimization (ADABCP) protocol is measured using the Network Lifetime. All the participants' nodes do not act in the routing stage at the same time. Some nodes acted as sleep nodes, some of the dead nodes, and most of the nodes are in the alive node.

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 happens in the data transmission to improve the network lifetime for the whole network; this postpones energy reduction and is much more useful to continuous packet delivery by the uninterrupted life of the network [76]. The proposed techniques to step-up network lifetime by node energy and routing process. Better network lifetimes are achieved on the target node by the Hybrid Random Late Detection (HRLD). HRLD protocol that is becomes 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. 30.

\[
\text{Network Lifetime} = \frac{\text{length of energy usage}}{\text{overall energy}}
\]

From Eq. 35, the packet delivery time is significantly higher for any two selected transmissions. The proposed SIRT–ADABCP-HRLD though packet delivered rate is compared to ESCT, ENM-LAC, and ZRDM-LFPM. The data transmission improves packet delivered by 56.9775%, more as compared to ESCT, ENM-LAC, and ZRDM-LFPM.

### 4.5 Energy Consumption

Figure 31 establishes energy consumption to evaluate the total energy used for the sender to the receiver node. The proposed method has a high routing delay and is used for packet transmission so 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 [21]. After that, route searching, path routing, and data transfer are usually considered. These are happened by spending the node's energy. This energy consumption was considered for data transfer alone, but some energy values are negligible on the RREQ and RRES during the routing process.
From Eq. 36, the proposed SIRT –ADABCP- HRLD, time to live and energy can be calculated on the time of data transfer. Consider the n nodes that have participated in the proposed MANET. Based on the proposed algorithm, the routing chooses the simplest route between nodes, and its energy consumption is very low compared to all existing simulations. In this Fig. 31 nodes have participated, and 1000 request transactions were done. 100 packets/nodes are request transactions before the data transmission. From this consideration, firstly energy consumption for routing with different routing parameters varies from 145 J/Sec to 190 J/Sec on the proposed system. What is 36.31% less value compared to the existing ESCT, ENM-LAC, and ZRDM-LFPM. All 100 nodes are taking 1400 J/Sec to execute all transactions within the stipulated time interval.

If the participant nodes are increased, the energy consumption was consuming higher compare to the ZRDM-LFPM. This has higher energy consumption also reduced in the proposed SIRT –ADABCP- HRLD. SIRT –ADABCP-HRLD consumes lower energy because nodes are continuously attention to the attentiveness of the MANET participants. For this reason, the energy consumption rate avoided still the number of nodes is increased. Finally, the proposed model without error rate, 38.63% times saves the energy than normal existing routing process.

\[
\text{Energy Consumption} = \text{Initial Energy} - \text{Final Energy}
\] (36)

5 Conclusion

In MANET routing, the packets’ interaction and data transmission were efficiently discussed concerning the MANET routing. This research involves managing the packets and routes between the source to 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 MANET environment is uncompromised for route interaction against security threads. In this research article, the proposed four processing schema are preserved the security measures against routing protocols such as node communication, and data transmission. Productively, Attacker detection automation of the Bees Colony Optimization (ADABCP) Method is worked against attacker detection on the routing process. Furthermore, the proposed Hybrid Random Late Detection (HRLD) routing protocol manages the MANET routing and also overcomes the congestion communication on MANET. Although the Swift Implicit Response Round Trip Time (SIRT) Mechanism helps to find the optimal routing securely and intelligently. The proposed result was compared against existing ESCT, ZRDM-LFPM, and ENM-LAC approaches. As a result, the proposed illustration (SIRT-ADABCP-HRLD) is to be improved by routing and data transmission. In comparison, the proposed method achieves a better ratio for the end-to-end Delay, communication
overhead, packet delivery ratio, network lifetime, and energy consumption. The performance evaluation results of SIRT–ADABCP-HRLD with existing methods in terms of low End to End Delay (ms) of 49.8361% compared to existing methods ESCT, ENM-LAC, and ZRDM-LFPM. In terms of low Communication Overhead of 81.4462% decrease compared to existing methods. Although improves packet delivered by 56.9775%, more as compared to ESCT, ENM-LAC, and ZRDM-LFPM. The energy consumption decreased by 36.31% less value compared to the existing process. The energy consumption rate is avoided still the number of nodes is increased. Finally, the proposed model without error rate, 38.63% times saves the energy than normal existing routing process. In the future scope, this research applied to the intrusion detection system and IoT-based suspect detection system to find the Susceptible object and cyber attackers over the internet black chain technology.

References

1. Abel T, McQueen D (2020) The COVID-19 pandemic calls for spatial distancing and social closeness: not for social distancing. Int J Public Health 65:231. https://doi.org/10.1007/s00038-020-01667-7
2. 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
3. Allimuthu U (2017) BAU FAM: biometric-blacklisting anonymous users using fictitious and adroit manager. J Adv Res Dyn Control Syst (12-Special) 722
4. Al-Zahrani FA (2020) On modeling optimizations and enhancing routing protocols for wireless multihop networks. IEEE Access 8:68953–68973
5. Alzamzami O, Mahgoub I (2020) Efficient maintenance of ad hoc network under wormhole attack. J Electr Syst Inf Technol 5(3):735–744
6. Amutha S, Balasubramanian K (2018) Secured energy optimized Ad hoc on-demand distance vector routing protocol. Comput Electr Eng 72:766–773
7. Azimdoost B, Saghaei K, Garcia-Luna-Aceves JJ (2012) Capacity of wireless networks with social behavior. IEEE Trans Wireless Commun 12(1):60–69
8. Bai J, Sun Y, Phillips C, Cao Y (2017) Toward constructive relay-based cooperative routing in MANETs. IEEE Syst J 12(2):1743–1754
9. 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 66:103358
10. Bamhdi AM (2020) Efficient dynamic-power AODV routing protocol based on node density. Comput Stand Interfaces 70:103406
11. Bozorgi AM, Farasat M, Mahmoud A (2017) A time and energy efficient routing algorithm for electric vehicles based on historical driving data. IEEE Trans Intelligent Vehicles 2(4):308–320
12. 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
13. 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
14. Chen Z, Zhou W, Wu S, Cheng L (2020) An Adaptive on-demand multipath routing protocol WithQoS support for high-speed MANET. IEEE Access 8:44760–44773
15. Cheung M, She J (2019) Detecting social signals in user-shared images for connection discovery using deep learning. IEEE Trans Multimedia 22(2):407–420
16. Chintalapalli RM, Ananthula VR (2018) M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network. IET Commun 12(12):1406–1415
17. Chithaluru P, Tiwari R, Kumar K (2019) AREOR–Adaptive ranking based energy efficient opportunistic routing scheme in Wireless Sensor Network. Comput Netw 162:106863
18. Chocotejo C, Morales R, Feliu V, Sanchez L (2014) Trajectory planning for a stair-climbing mobility system using laser distance sensors. IEEE Syst J 10(3):944–956
19. Djedjig N, Tandjaoui D, Medjek F, Romdhani I (2020) Trust-aware and cooperative routing protocol for IoT security. J Inf Secur Appl 52:102467
20. Ethonesy M, Shankar K (2019) Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Trans Reliab 69(3):1077–1086
21. El-Semary AM, Diab H (2019) BP-AODV: blackhole protected AODV routing protocol for MANETs based on chaotic map. IEEE Access 7:95185–95199
22. Garaaghaji A, Alfi A (2020) A fuzzy-hierarchical routing algorithm for MANET networks allocation rates problem. Iran J Sci Technol Trans Electr Eng 44(2):1003–1011
23. Ghoreishi SM, Razak SA, 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
24. Giordano G, Blanchini F, Bruno R et al (2020) Modelling the COVID-19 epidemic and implementation of population-wide interventions in Italy. Nat Med 26:855–860. https://doi.org/10.1038/s41591-020-0883-7
25. 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
26. Greco S, Molinaro C, Pulice C (2017) Efficient maintenance of shortest distances in dynamic graphs. IEEE Trans Knowl Data Eng 30(3):474–487
27. Gupta DD, Dong DW (2020) No more “social distancing” but practice physical separation. Can J Public Health 111(4):488–489. https://doi.org/10.17269/s41997-020-00370-x
28. Hahn F, Pappa A, Eisert J (2019) Quantum network routing and local complementation. npj Quantum Inf 5(1):1–7
29. Hammi B, Zeadally S, Labiod H, Khatoun R, Begriche Y, Khoukhi L (2020) A secure multipath reactive protocol for routing in IoT and HANETs. Ad Hoc Networks, 102118
30. Hasan SS, Kow CS, Zaidi STR (2020) Social distancing and the use of PPE by community pharmacy personnel: Does evidence support these measures?. Res Soc Adm Pharm. https://doi.org/10.1016/j.sapharm.2020.04.033
31. Hayashi Y, Uchiyama N (2018) Onion-like networks are both robust and resilient. Sci Rep 8(1):1–13
32. Hayat S, Imran M, Liu JB (2019) An efficient computational technique for degree and distance based topological descriptors with applications. IEEE Access 7:32276–32296
33. He T, Cai L, Meng T, Chen L, Deng Z, Cao Z (2018) Parallel community detection based on distance dynamics for large-scale network. IEEE Access 6:42775–42789
34. Hipp JR (2020) Neighborhood change from the bottom up: What are the determinants of social distance between new and prior residents?. Soc Sci Res 86:102372. https://doi.org/10.1016/j.socres.2019.102372
35. 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
36. 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 (pp. 30–40)
37. Huisman G (2017) Social touch technology: a survey of haptic distance computing: a query-dependent local landmark scheme. IEEE Trans Knowl Data Eng 28(7):1835–1850
38. 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
39. Huynh TLD (2020) Does culture matter social distancing under the COVID-19 pandemic? Saf Sci 130:104872
40. Islabudeen 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
41. Jabbar WA, Saad WK, Gupta N, Awad D, Garg P (2020) Performance analysis of NOMA assisted mobile ad hoc networks for sustainable future radio access. IEEE Trans Sustain Comput 6(2):347–357
42. 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 6(2):347–357
43. Jaiswal RK (2020) Position-based routing protocol using Kalman filter as a prediction module for vehicular ad hoc networks. Comput Electr Eng 83:106599
44. Jeong C, Shin WY (2018) Network-decomposed hierarchical cooperation in ad hoc networks with social relationships. IEEE Trans Wireless Commun 17(11):7606–7619
45. Kacem I, Sait B, Mekhilef S, Saebeur N (2018) A new routing approach for mobile ad hoc systems based on fuzzy Petri nets and ant system. IEEE Access 6:65705–65720
46. Kawashima T, Nomura M, Tanoue Y, Yoneoka D, Eguchi A, Shi S, Miyata H (2020) The relationship between fever rate and telomere length. J Behav Exp Econ, p 101544. https://doi.org/10.1016/j.socec.2020.101544
47. 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
48. Landi D, Ponzano M, Nicoletti CG, Cecchi G, Cola G, Mataluni G, ..., Marfia GA (2020) Adherence to social distancing and use of personal protective equipment and the risk of SARS-CoV-2 infection in a cohort of patients with multiple sclerosis. Mult Scler Relat Disord 45: 102359
49. Li J, Ding Z, Jedari B, Xia F, Lee I, Tolba A (2016) Geo-social distance-based data dissemination for socially aware networking. IEEE Access 4:1444–1453
50. Li J, Sun Y, Li M, Fan W, Zhong Y (2020) Social distance modulates prosocial behaviors in the gain and loss contexts: An event-related potential (ERP) study. Int J Psychophysiol 150:83–91
51. Li Z, Wu Y (2017) Smooth mobility and link reliability-based optimized link state routing scheme for manets. IEEE Commun Lett 21(7):1529–1532
52. Liu L, Li CF, Lei YM, Zhao JJ, Yin YJ, Sun XK (2016) A new fuzzy clustering method with neighborhood distance constraint for volcanic ash cloud. IEEE Access 4:7005–7013
53. Liu S, Zhang DG, Liu XH, Zhang T, Gao JX, Cui YY (2019) Dynamic analysis for the average shortest path length of mobile ad hoc networks under random failure scenarios. IEEE Access 7:21343–21358
restrictions. Am J Geriatr Psychiatry. https://doi.org/10.1016/j.jagp.2020.05.004

72. Vilar-Compte M, Pérez V, Teruel G, Alonso A, Pérez-Escamilla R (2020) Costing of actions to safeguard vulnerable Mexican households with young children from the consequences of COVID-19 social distancing measures. Int J Equity Health 19(1):1–3. https://doi.org/10.1186/s12939-020-01187-3

73. Wang X, Zhang Y, Zhang W, Lin X (2016) Efficient distance-aware influence maximization in geo-social networks. IEEE Trans Knowl Data Eng 29(3):599–612

74. West R, Michie S, Rubin GJ, Amlôt R (2020) Applying principles of behaviour change to reduce SARS-CoV-2 transmission. Nat Hum Behav, pp 1–9. https://doi.org/10.1038/s41562-020-0887-9

75. Xia F, Liaqat HB, Deng J, Wan J, Das SK (2015) Overhead control with reliable transmission of popular packets in ad-hoc social networks. IEEE Trans Veh Technol 65(9):7647–7661

76. Xu C, Zhu L, Liu Y, Guan J, Yu S (2018) DP-LTOD: differential privacy latent trajectory community discovering services over location-based social networks. IEEE Trans Services Comput 14(4):1068–1083

77. Yan L, Shen H, Chen K (2016) TSearch: Target-oriented low-delay node searching in DTNs with social network properties. IEEE/ACM Trans Netw 24(6):3841–3855

78. Yang CC, Ng TD (2011) Analyzing and visualizing web opinion development and social interactions with density-based clustering. IEEE Trans Syst Man Cybernetics-Part A: Syst Humans 41(6):1144–1155

79. Ye Q, Zhao H, Li Z, Yang X, Gao S, Yin T, Ye N (2017) L1-norm distance minimization-based fast robust twin support vector $k$-plane clustering. IEEE Trans Neural Netw Learn Syst 29(9):4494–4503

80. Yezli S, Khan A (2020) COVID-19 social distancing in the Kingdom of Saudi Arabia: Bold measures in the face of political, economic, social and religious challenges. Travel Med Infect Dis 37:101692

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

82. Zhang T, Zhao S, Cheng B (2020) Multipath Routing and MPTCP-Based Data Delivery Over Manets. IEEE Access 8:32652–32673

83. Zhao Y, Yang LT, Zhang R (2018) Tensor-based multiple clustering approaches for cyber-physical-social applications. IEEE Trans Emerg Top Comput 8(1):69–81

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

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.