Wireless Personal Communications (2020) 115:725–744
https://doi.org/10.1007/s11277-020-07596-5

Prediction of Node and Link Failures in Mobile Ad Hoc Network Using Hello Based Path Recovery Routing Protocol

Sunil Kumar[1]

Published online: 17 June 2020

Abstract
Mobile ad hoc network is composed of wire free nodes that are moving in nature and they are configured to form a self-configured infrastructure less network. So, the energy consumed by every node is varied due to the movement of the nodes. Open Shortest Path First is the shortest path estimating routing scheme which is created more energy and more delay for data transmission when the link fails in the network. To overcome this difficulty, this paper proposed an efficient innovative hello based path recovery (HBPR) routing protocol for the shortest path calculation. During transmission, if the link fails in the network layer then the HBPR scheme creates the alternate path, thus it reduced the delay time and energy consumption. Subsequently, the novel simplified honey pot optimization (SHPO) is introduced to predict the harmful nodes within the network. This SHPO maintains the path stability and node security of the network also it will improve the quality of service parameters. The implementation of this research is done by MATLAB R2018b and the simulation results illustrate the performance of the proposed algorithm. This approach achieves better results in packet delivery ratio, delay, average energy consumption, and throughput compared to other existing approaches.

Keywords Mobile ad-hoc network · Routing protocol · Path recovery · Link crash · Harmful nodes · Quality of service in MANET

1 Introduction

Wireless ad hoc network (WANET) is termed as a mobile ad hoc network (MANET) [1]. It consists of the number of movable nodes that linked wirelessly [2] in a self-configuring, self-organizing, and fewer infrastructure networks in which nodes move freely [3]. Also, WANET nodes are applied to change the network topology in a dynamic manner without any conditions that are the common behavior of ad-hoc networks [4]. Moreover, MANET is the set of nodes which creates the network temporarily of any form of structure [5]. Here, all nodes communicate directly using single-hop or circuitously

✉ Sunil Kumar
sunilkm.scholar@gmail.com

[1] Department of Computer Science and Applications, IIMT University, IIMT Nagar, 'O' Pocket, Ganga Nagar Colony, Mawana Road, Meerut, Uttar Pradesh 250001, India

and multi-hop routing for sending their packets to far-away end and there is no base station in MANET [6]. These routing approaches can be elaborated into hybrid, proactive [7] and reactive routing schemes based on the network scaffold [8]. Furthermore, MANET is handled in numerous applications like range sensors for the surroundings, vehicular ad hoc communication, and robots, etc., [9]. The behavior of the network is improved by re-developing the break nodes or links [10] to send the packets in the equal path proceeding in this manner the normal end-to-end delay is reduced [11]. Routing can be used to transfer the information from source node to destination that contains two concepts, initially identify the path and then transfer the information through an internetwork.

MANET is referred to as a decentralized independent operation. Here, nodes are engaged in MANET frequently operate as clients/servers. This mobile node involves a home PC, laptop, MP3 player, mobile phone, and personal digital assistants. Nodes may be located on ships, airplanes, or land, irrespective of their location as they can participate in the communication. Self-connectivity and easy deployment of MANETs makes it apt for an emergency, surveillance situations, and rescue operations.

Moreover, OSPF is a link state routing scheme and each router should know the detail about the entire view of the network. Also, the routing information is passed through the routers of an autonomous or independent system (AS). OSPF is one of the router protocol used to identify the best path for packets. Generally, AS composed of a lot of routers and communication among the routing or directing information is done by the routing scheme. Also, this protocol keeps tracking the path for sending data and the router sends periodically a hello messages for the establishment of adjacency with its neighbor and describes the link state advertisement (LSA) connection status. The shared information between two routers is called LSA and the topology changes in the OSPF scheme are detected via LSA. Because, LSA contains LSA type, destination id along with area-id, path type, its associated cost, and id of next hop. The OSPF is an active scheme that quickly detects structural or topology variations through LSA. Also, LSA is the division of information expressing the router's state over the network.

However, a node which cannot transmit the packets directly to the destination initially finds the shortest path and transfers the messages to the nearest neighboring node [12]. Also, packet losses are happened because of harmful node activities in various methods and the recovery of the broken link in the network is based upon the routing schemes [13]. Moreover, the losses between direction request and reply message create more difficulties like packet losses [14]. QoS is a better service for dissimilar application based activities [15], to broadcast under a good condition of the data stream, throughput, packet loss, delay [16], etc. In MANET, a wireless node can be the sender, receiver, or an intermediate node for data conduction [17]. The identification of node crashes is necessary for secure data transmission because wireless networks are getting the effects of attacks [18]. Hence, the network topology varies in every interval [19]. The link crash predicts the local routes then provides the low back-to-back delay, reducing packets, and raises the packet delivery rate [20]. Thus, the proposed approach introduces the innovative routing protocol for predicting link failure and communicating in a secure shortest way.

The rest of this research is ordered as follows. Section 2 presents an overview of the previous work of the prediction of node/link crashes in MANET. Section 3 details the system model of the network. Section 4 specifies the proposed methodology. Section 5 describes results about the proposed work and Sect. 6 provides the overall conclusion of the proposed work.

2 Related Work

Some of the recent works of literature related to node/link crash prediction in MANET are summarized beneath:

Dynamic features of MANET proposed numerous difficulties to achieve the protection parameters like availability, confidentiality authentication, integrity, and non-revocation. To block the typical directing task noxious hubs make utilization of the vulnerable steering conventions. Also, identifying the routing protocol act against the attacks is a difficult task. To beat this issue, Soni et al. [21] introduced the protocols secure ad hoc on interest distance vector (SAODV) and ad hoc on interest distance vector (AODV) for the action against the attacks. Furthermore, this protocol gives better protection and lastingness in MANETs.

Protection threads and vitality proficiency are estimated as the preeminent factors in MANET while poor protection may be developed because of their difficult attributes. To defeat this, Merlin et al. [22] projected a novel trust based vitality directing instrument for MANETs. The speculative and trial therapy demonstrates that trust based energy aware routing (TEAR) gadget display recouped execution than that of the prior research works. The TEAR instrument exceptionally improves the life period of the system by keeps away from the dark gap assault and drastically developing the opportunity of blasting information steering.

The MANETs are the foundation of random allocation of the nodes whereas the nodes of the actual network are usually containing self-position preference. However, these causes the collision of random boundary crashes on the MANET topology. So, Liu et al. [23] detailed the average shortest path length (ASPL) which is an imperative characteristic of the network topology. The ASPL in MANET is calculated after the random crash for enhancing the exactness and constraints of the node's power consumption and connection distance.

MANETs are founded and deployed spontaneously without any infrastructure in the geographical areas. The performance of the network is satisfied only when all the member nodes have the intensity to work in a collective manner. But, due to the lack of any centralized unit, it is vulnerable to various attacks. To overcome these types of attacks, Prabha et al. [24] proposed the Trusted-Differential Evolution algorithm that deals with malicious node and inhibits to become a member of the data communication route. Also, the dynamic of trust is handled by a modern trust-updating scheme along with the punishment factor for malicious node.

Energy is a huge basis for a decentralized system. By the pleasing physical layer arrange coding framework, the commitment of energy broadcast can be diminished. Here, Femila et al. [25] proposed by the regular power-mindful algorithms, an efficient power aware routing (EPAR) strategy to survey the information steering is performed with elevated mobility in a dynamic environment. To energy, utilization can be diminished and consequently life length of a hub can be better. The energy utilization rate is limited, so the system life period and the execution are better. The power usage rate can be diminished to 80% by utilizing the EPAR scheme in MANETs.

The novel contributions of the proposed work include the following steps,

- Initially, the HBPR protocol predicts the node/link failures in the network and identifies the alternate secure path for data transmission.

- Also, the proposed HBPR routing algorithm enhances the throughput and reliable communication upon the route crashes caused due to the movement or mobility in the networks.
- Simplified HPO is used to predict the dangerous nodes and path stability maintenance also it improves the security of the network.
- This proposed scheme handles the QoS infringement that occurs due to the mobility and traffic in the network.

In everyday life, multimedia communication plays an important function in wireless networks. Multimedia data is stipulating for QoS improved multicast routing protocol in MANETs. However, these networks are affected by various malicious attacks that break the nodes and links. The major objective of the proposed routing protocol is to predict the node/link failures in the network and to improve the QoS parameters. Initially, the nodes are created for transmission and the proposed approach predicts the node/link failures and recovers the shortest path for data transmission. Also, it enhanced the security of nodes and networks against the different categories of attacks & malware using SHPO.

3 System Model

MANET is the wireless network that has wireless transmitters and receivers with directional antennas. Moreover, the messages are sending through the mobile node and are received by neighboring nodes. If the node needs to convey the message for another node that is not in transmission range then the intermediate nodes act as the router and forward the message. Due to the various hazardous conditions create node failure at any time in the working environment that will be crash the network and decrease the energy supply. Moreover, these node failures break the links between the nodes, which is represented in Fig. 1.

Each node performs as a host and a router that sends the data packets to neighboring hosts and consumes more energy. In MANET, link failure is one of the common criteria because of weak nodes or less energy nodes. But, the proposed method overcomes these issues using innovative routing algorithms.

3.1 Link State Database (LSDB)

The collection of router's LSA data is called LSDB. The link status between two neighboring routers is explained in LSAs and these LSAs are reserved in LSDB of each router in the structure of a graph.

3.2 Splitting of Network into Areas and Segment

In OSPF, the operation is based on the area and the entire nodes are interconnected to one another. Also, the transmission delay in the OSPF routing is high when the area in the network is very large. Because all the nodes send the data packets to the entire neighboring node so this takes many periods for transmission. To overcome this delay, the network area is segmented into a lot of small network area and this reduces the congestion and delay in the network. In the segmented network, all the areas are associated with the backbone or central area or the area 0 otherwise routing will not take place. The default area is called area 0 or backbone area. The communication between area 1 and area 2, there is no

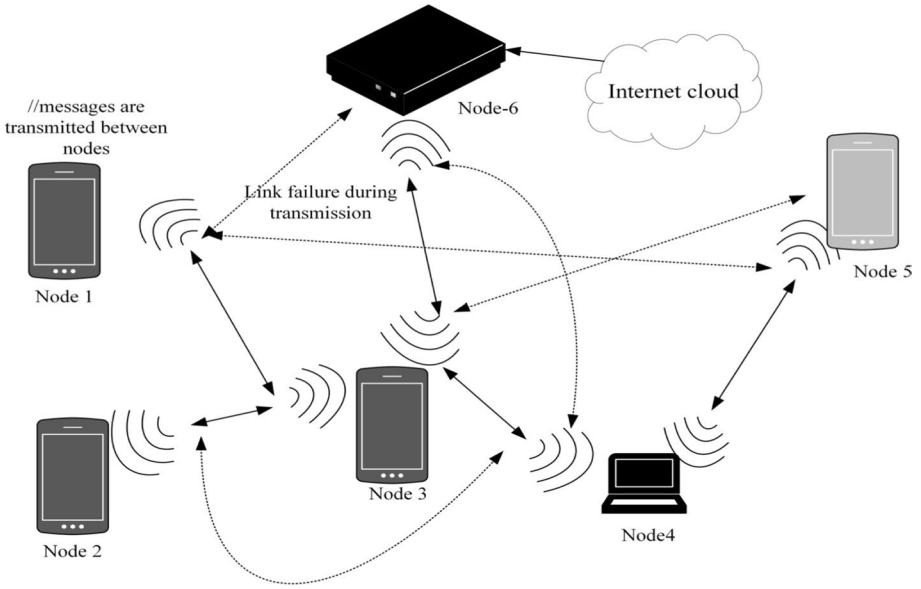

Fig. 1 Link failure in MANET

possibility to communicate directly from area 1 to area 2. For that, it should communicate via the backbone area i.e., data is transmitted from area 1 to area 0 (backbone area).

3.3 Election of Designated Router (DR)

In MANET, every node is connected to each other because there is a large possibility to form the congestion. This congestion creates traffic in the network and to solve this, designated router (DR) and backup designated router (BDR) are used. The communication is taking place via the designated router where the DR is selected through the election which is based on the priority value. DR is nothing but the ordinary router which acts as an intermediate node between source and destination that can solve the traffic in the network. The source is not having the capability to directly send the messages to the destination. The source initially sends the message to DR, the message contains the destination id, and then the DR is to send the messages to the destination. The priority value of the node is used to select the DR and the selection is dependent on the election. The node with higher priority value is assigned to DR and the next priority value is assigned to DBR. If DR crashes, then BDR performs the function of DR. If all the routes having a similar priority value then the router ID is considered as the selection process.

3.4 Routing Table

After the complete synchronization of LSDB across the routers, the routers present in the system are used to estimate the routing table by Dijkstras shortest path algorithm which contains the routing information about the destination node. The routers can able to calculate the routing table using Dijkstras shortest path algorithm for the

data forwarding function. The routing table has the necessary information to transmit a packet from source to destination by the shortest path that is calculated using Dijkstras shortest path algorithm. The routing table is decomposed into two regions. The First one has the details about destination information and the next one has the set of the shortest path to the destination.

In MANET, the link or node failures are the common issues in the message transformation of the networks that increase the network unreliability and degradation. Also, the link or node crashes increase the delay and power for transmitting the data. For this reason, the innovated routing approach is introduced for predicting the node failures. After that, the message can be transmitted in a secure way without any delay using this innovative routing.

4 Proposed HBPR-SHPO Methodology

MANET can rule the IT world in the present life but there are some difficulties in message sharing. In OSPF, if a link crash happens during the transmission then the nodes send a Route Error (RERR) message back to the source. After the reception of the error message, the source node restarts the route discovery. In OSPF, if any one of the nodes fails during data transfer which causes the delay and packet drop because the OSPF scheme must be created the alternate path from the source node and it is susceptible to several kinds of attack. To overcome this problem, this research develops the innovative HBPR routing protocol for generating the alternate shortest path when predicting the crashes of link/nodes. Moreover, the introduced SHPO provides the protection and predicts the harmful nodes then maintaining the path stability. Also, SHPO maintains the security for every node and the proposed work improves the QoS parameters. The workflow of the proposed is depicted in Fig. 2.

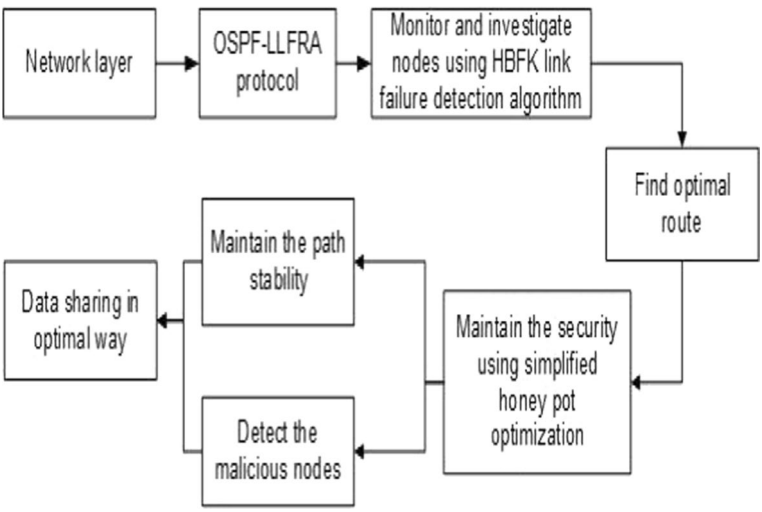

Fig. 2 Proposed HBPR-SHPO methodologies

4.1 Proposed Hello Based Path Recovery (HBPR) Scheme

MANET is represented by the number of nodes that are used for communicating between source and destination. Here, the HBPR approach creates the shortest path for communication also, it is reduced the delay and power consumption during transmission. The proposed HBPR routing scheme is deployed in every node in the network. In MANET, every node in the network layer waits for the reception of the RERR messages. If any one of the nodes fails during transmission, it can be identified using the HBPR method then it generates the optimal shortest path at the place of crashes. If the link is failed during the transmission time, then the whole packet or information will get attack or any other malicious activities have happened. Hence, the HBPR routing protocol predicts the link/node failure and creates an alternate path for data transmission, which is represented in Fig. 3.

In this HBPR scheme, every node in the network transmits the hello message to all the connected nearest nodes periodically. This will confirm the status of all the connected nodes in the network. If the verification message is not accepted or received by the nodes at a certain interval (delay) then it decides that the link or node is dead. In this, HBFK can predict the node and link failure during transmission after that, it creates the alternate path for transmission, which is exposed in Eq. (1).

$$F(u,v) = \sum_{x=1}^{m} \sum_{y=1}^{n} U_{xy} \left\| A_x - B_y \right\|^2 \tag{1}$$

where, $F(u,v)$ denotes the secure path for data transmission, U_{xy} represents the total number of nodes, $A_x (x = 1, 2, \ldots, m)$ denotes *mth* position of destination nodes and

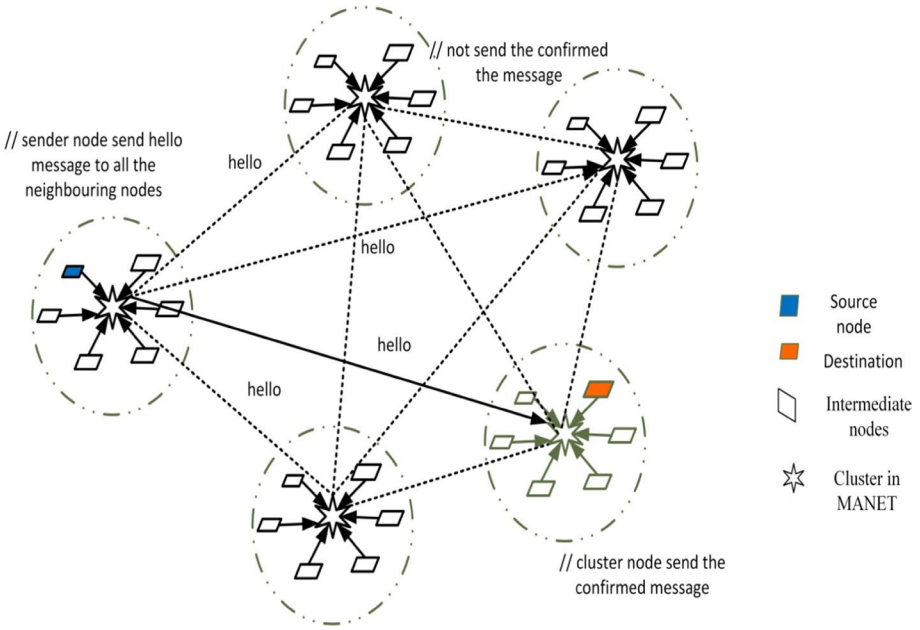

Fig. 3 Hello based path recovery scheme

$B_y(y = 1, 2, \ldots, n)$ is the *nth* position of harmful nodes. The mathematical equation for the calculation of maximum delay (δ) is exposed in Eq. (2).

$$\delta = LT + \sigma \tag{2}$$

where, L is the number of missing hellos, T denotes the hello interval and σ is the negligible variance due to channel congestion and σ has a uniform distribution on $[(L-1)T, LT]$. According to this δ average (δ') is mentioned in Eq. (3).

$$\delta' = \frac{(2L-1)T}{2} \tag{3}$$

where, L denotes the number of missing hellos. In the value of (δ) exceeds certain intervals then it checks the remaining additional parameters. If it desires the node is inactive or useless, then the position and crash of the node are predicted by the weight correlation mode. The quality of the link is measured by the expression Eq. (4),

$$Q_x = \frac{F(u, v)}{1 + U_{xy}} \tag{4}$$

where, U_{xy} represents total number of nodes, the energy consumption of the node can be calculated using Eq. (5),

$$E = \frac{T_p}{T_k(t)} \tag{5}$$

Where, T_p is the transmitted packet strength, $T_k(t)$ is represented as the time taken for transmission. The sender node transmits the 'hello' message to the neighboring nodes. These nodes are sending the accepted message when they receive the 'hello' message. At that time, the SHPO monitors the time interval of reached 'accepted' messages from neighboring nodes. When this message does not receive at the sender node at a particular time then the SHPO decides the link is weak or fails. If the condition of the link or node is weak or fails, then HBPR chooses an alternate path for data transmission. Subsequently, this research used the SHPO for the detection of harmful nodes to maintain path stability and protection.

4.2 Security Maintenance Using Simplified Honey Pot Optimization

MANETs are affected by attackers which are crash the network. The attackers can able to reduce the throughput of the network, increasing the packet latency, and collapse the link between the nodes. To avoid these limitations and maintaining the security of MANET this research introduced the innovative SHPO technique.

Initially, the SHPO monitors the network there are any harmful nodes present or not also, it can identify the path in which the attacker tries to attack the transmission nodes. Moreover, SHPO calculates the time period in which the nearest nodes are forwarding the 'accepted' message. If the attacker present in the network then they have some delay to receive or send the message. Consequently, SHPO calculates the time interval of the nodes message transmission, which is explained in Fig. 4.

Consider the network $S = \left(N, N_h, n_r\right)$ where N is the total number of nodes in the network, N_h is the harmful nodes and n_r is the connection between the neighboring

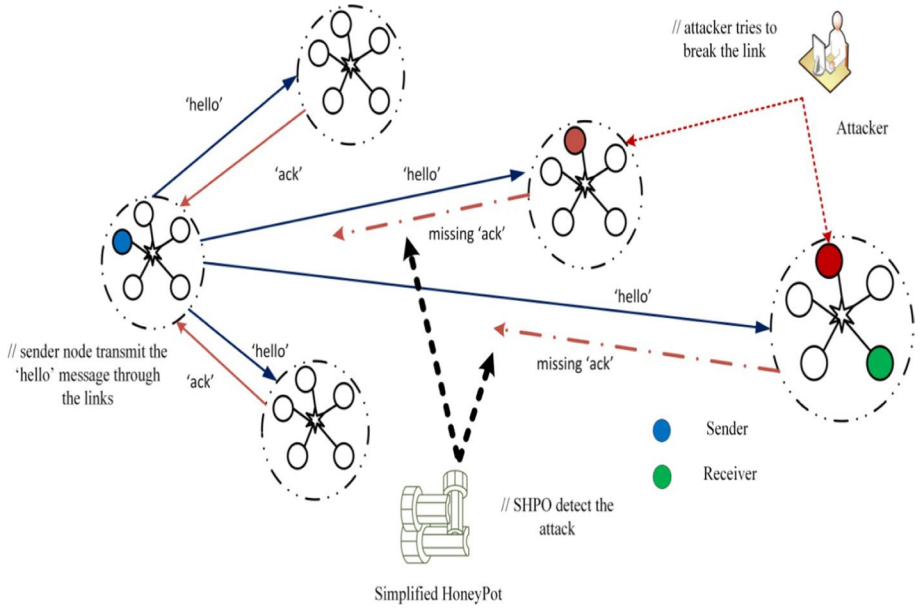

Fig. 4 Process of SHPO

node clusters (destination nodes). Here, SHPO monitor the harmful nodes and alert the source node $S_N = N/n_r$. The time interval of the node transmitting path is calculated using Eq. (6).

$$T_k(t) = \frac{\min T_i(t) * H}{N - nr} \tag{6}$$

where, $T_k(t)$ lifetime of path k, $T_i(t)$ is the predicted lifetime of node in path k, H denotes the frequently transmitted 'hello' messages.

In this technique, the SHPO can detect the harmful nodes and transmit the data through the safest node. So, the detection behavior of the SHPO can be adopted for detecting the malicious nodes during transmission. Consequently, SHPO sends an acknowledgment to the admin of the network when the attacker attacks a node and then provided a message to the client to monitor the activities of the attacker. During transmission, if any harmful nodes are present in the network or any attacker tries to attack the node, which is detected by SHPO then the HBPR algorithm regulates the data transmission through the safest nodes also maintains the path stability.

Initially, the source node transmits the 'hello' message to the neighboring nodes in the transmission region of the network. If the neighboring nodes receive the message then it will send the 'accepted' message to the source node. Sometimes the nodes or links not able to receive the message because, the node or links crashed by attacks. It was monitored by the proposed SHPO approach that is alert to the source node. So, the innovative HBPR routing protocol creates the alternate path for secure transmission, which is elaborated in Fig. 5.

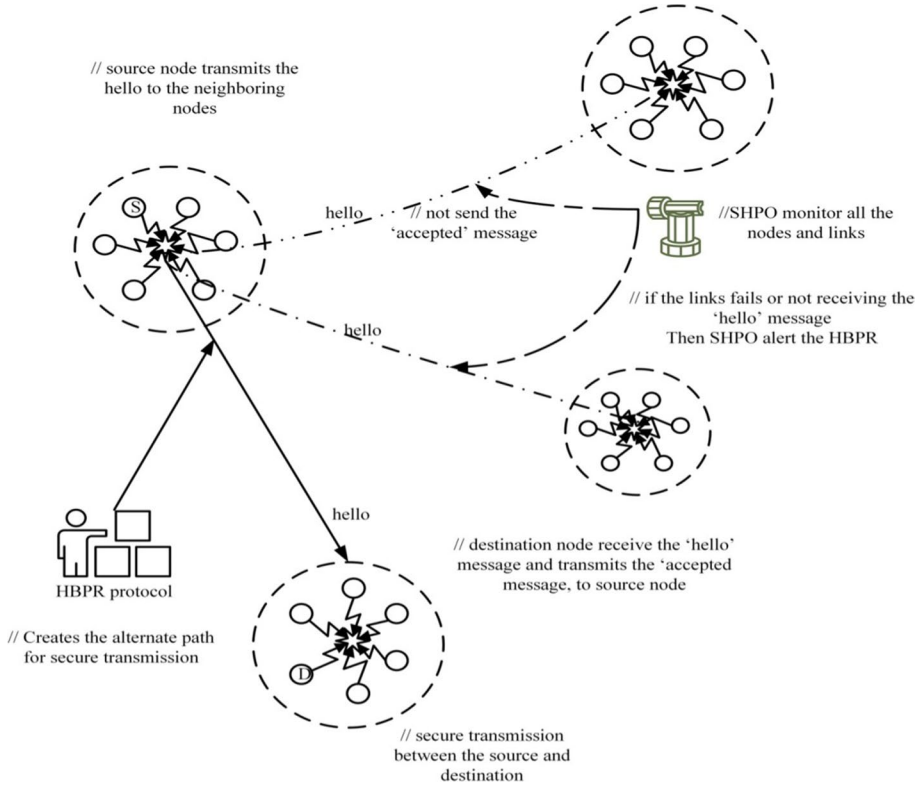

Fig. 5 Work flow diagram for HBPR-SHPO

5 Results and Discussion

To represent the effectiveness of the proposed technique, the node formation of MANET implementation is done using MATLAB library. The projected scheme aims to achieve the task in the MANET nodes and transmit the data in a secure path. During data transmission between the nodes, the nodes or links may be crashed by the attackers, which is predicted by the innovative SHPO approach. Consequently, the proposed novel HBPR routing protocol generates an alternate path for data transmission with low delay and lower energy. Also, the proposed approach provides low PDR, end-to-end delay, and throughput ratio.

5.1 Case Study

Let us assume the ad-hoc network is formed by connecting all mobile nodes in a group of people gathered in the conference at a place when no network services are accessible. If any message is transmitted by the mobile node then it should be received by all its neighboring nodes. Also, the source node transmits a message to a mobile node but it is not in the transmission range so the intermediate nodes act as a router and forward the message.

Considered ten numbers of mobile nodes and one source node for transmitting the message also, this network has six destination nodes. The information is transmitted from source

node to destination without any node and link failure. In this network, all destination nodes and intermediate nodes are monitored before transmitting the messages. Initially, the source node sends 'hello' messages for all the neighboring nodes, if the neighboring nodes receive the 'hello' message then it sends the 'accepted' message to the source node.

The neighboring mobile nodes transmit the 'accepted' message in a particular interval of time, which is calculated using Eq. (6) then obtained results are mentioned in Eq. (7),

$$T_k(t) = \frac{5(21)}{10-1} = 11.6s \tag{7}$$

Thus, the nodes are sending a reply message at the time interval 11.6 s that is measured using SHPO. When the neighboring nodes are not sending the message in a particular time then SHPO considered that node is crashed node. Let us considered the number of missing hellos as L=5, hello interval between the nodes T=11.6 s are substituted in Eq. (3) then the delay time is obtained in Eq. (8),

$$\delta' = \frac{(2*5-1)11.6}{2} = 52.2s \tag{8}$$

Thus, the mobile nodes taking more 52.2 s for sending the accepted message, which is assumed as link/node failure in the network, which is predicted by SHPO and alert the source node. Subsequently, the alternate path was created by the HBPR routing protocol based on Eq. (1).

$$F(u,v) = 10\|6-5\|^2 = 10s \tag{9}$$

where, $F(u,v)$ denotes the secure path, $U_{xy} = 10$ denotes the total number of nodes, thus Eq. (9) details created an alternate path in the interval of 10 s by the HBPR routing protocol.

Also, the quality of the mobile nodes and links are measured using Eq. (4) and the created alternate path provides high quality which is represented in Eq. (10),

$$Q_x = \frac{10}{1+10} = 0.90 \tag{10}$$

Thus, the HBPR routing protocol created a 90% high-quality alternate path for transmission between the mobile nodes Moreover, the energy consumption of the mobile nodes can be calculated using Eq. (5). Where, T_p is the transmitted packet strength, $T_k(t)$ is represented as the time taken for transmission.

$$E = \frac{1.2}{11.6} = 0.1J \tag{11}$$

Consequently, the proposed approach provides 0.1 J lower energy for transmitting neighboring 25 mobile nodes, which is represented in Eq. (11). Hence, the proposed strategy utilized to provide secure transmission between the mobile nodes that creates lower energy and a high-quality path for message transmission. Also, the proposed HBPR routing protocol provides less throughput ratio, low PDR, and low delay.

5.2 Performance Analysis

The proposed approach measured the QoS parameters such as end-to-end delay, throughput, and PDR. Here, the comparison is performed between the proposed routing protocol and various existing routing approaches. The simulation time of the proposed protocol is very low compared with the execution time of various parameters. Also, the results of the proposed approach parameters like delay, PDR, throughput, and energy consumption are compared with existing schemes. Some of the existing approaches are EE-RA [26], FIS [27], DVSM [28], QoSTRP [29], EED-M [30] and LEACH-DT [31].

5.2.1 End-to-End Delay

The mean period interval between the creation of a packet from a source node and an effective transmission of the packet is measured at the target node. It calculates every probable delay that can happen in the source and all middle nodes, together with queue period, packet broadcast and dissemination, and rebroadcasting at the network layer. The proposed approach transmits the message with a lower delay compared with existing methods, which are shown in Fig. 6.

Also, the queue period can be developed by network obstruction or inaccessibility of suitable routes. The end-to-end delay of the proposed network is very low compared with other approaches that values are shown in Table 1.

5.2.2 Packet Delivery Ratio (PDR)

PDR is the fraction of the quantity of data packets effectively distributed to every destination node and the measurement of information packets produced by the entire source nodes. The calculation for the PDR is mentioned in Eq. (12).

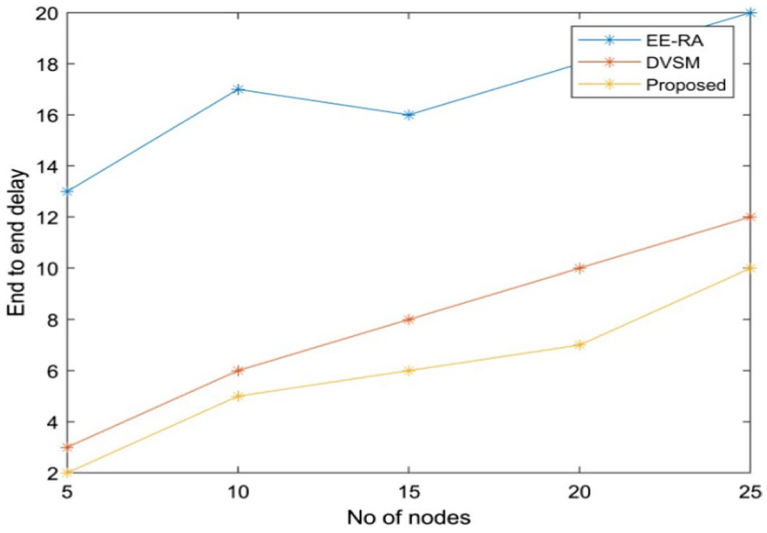

Fig. 6 Network size versus end-to-end delay

Table 1 End-to end delay

End-end-delay (s)			
No. of nodes	EE RA	DVSM	HBPR-SHPO (proposed)
5	13	3	2
10	17	6	5
15	16	8	6
20	18	10	7
25	20	12	10

$$PDR\% = \frac{Number\_of\_packet\_received}{Number\_of\_packet\_sent} \times 100 \tag{12}$$

In this simulation, the parameters of packet size were examined while determining the packet delivery ratio. The PDR of the proposed scheme has improved when the pause time enlarges is shown in Fig. 7. It illustrates that the proposed HBPR routing scheme has sustained a superior packet delivery ratio of about 90% while differing the pause time.

An exhaustive performance assessment shows that the proposed scheme has enhanced the potential of discovering the best possible route with the assist of the HBPR scheme. The packet delivery ratio of the proposed HBPR-SHPO approach is compared with existing methods, which values are given in Table 2.

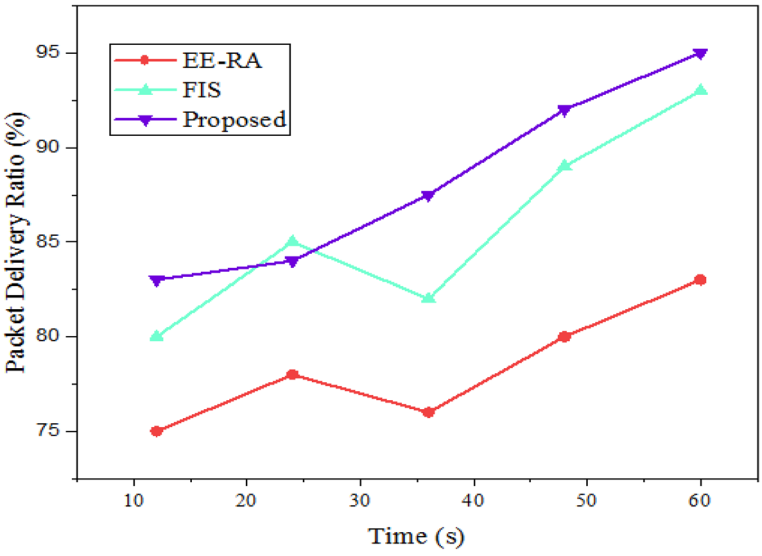

Fig. 7 Packet delivery ratio

Table 2 Packet delivery ratio

Time (s)	Packet delivery ratio (%)		
	EE RA	FIS	HBPR-SHPO (proposed)
12	75	80	83
24	78	85	84
36	76	82	87.5
48	80	89	92
60	83	93	95

5.2.3 Harmful Node Detection

The node activity is sometimes monitored and captured by some un-trusted party. The activity for predicting this behavior is called harmful node detection. In the proposed methodology, only 1% of harmful nodes are predicted out of 25 nodes.

In this simulation, the amount of harmful nodes is obtained with the total quantity of nodes present in the network. The proposed method is having the fewer number of harmful nodes than node predicted in the existing technique. The harmful nodes are predicted by SHPO from the total number of nodes, which are given in Fig. 8. The proposed approach has less number of harmful nodes when compared to the existing scheme like QoSTRP and EED-M scheme is given in Table 3.

5.2.4 Throughput

It is the quantity of packets (bytes) that are received successfully in a unit period (packet transmission period) is called throughput, and it is represented in kbps. The packet

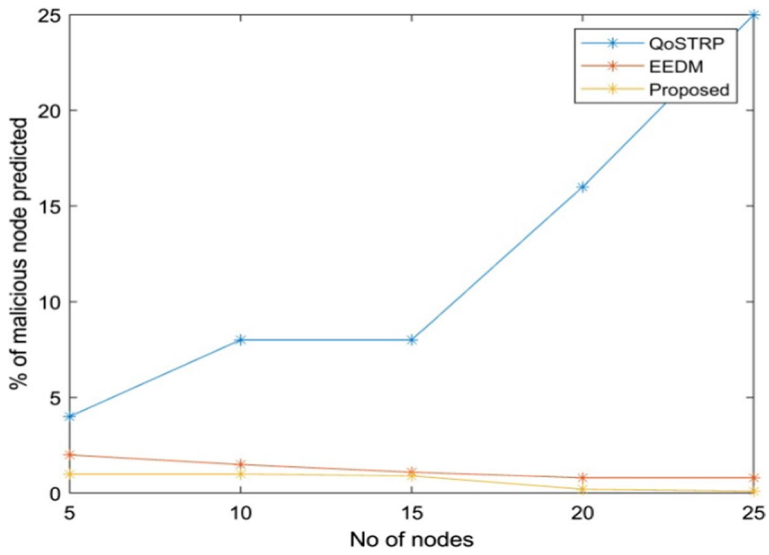

Fig. 8 Number of nodes versus % of harmful node detection

Table 3 Prediction of harmful nodes

Number of nodes	Malicious node prediction		
	QoSTRP	EED-M	HBPR-SHPO (proposed)
5	4	2	1%
10	8	1.5	1%
15	8	1.1	0.9%
20	16	0.8	0.2%
25	25	0.8	0.1%

transmission line is calculated by subtracting the start period from the stop period. The equation for the throughput is mentioned in Eq. (13).

$$Throughput(kbps) = \frac{\text{Re}ceived\_packet(bytes) * 8}{1024 * (stoptime - starttime)} \times 100 \tag{13}$$

In this simulation, the parameter of pause time (transmission time) was examined while determining the throughput. The evaluation is based on the measurement of throughput with various existing schemes like EE-RA and FIS that is shown in Table 4. The proposed HBPR achieves higher throughput when compared to EE-RA and FIS are shown in Fig. 9.

5.2.5 Energy Consumption

The amount of energy required for data transmission is called the power consumption of the nodes in the network. The proposed methodology requires less energy because of OSPF-LLFR generate the shortest path for data transmission.

In the proposed scheme, the energy consumed in the network is very low when compared to the existing scheme like LEACH-DT and QoSTRP. The graphical illustration of the energy consumption of nodes with a linear increase in the number of nodes is represented in Fig. 10. The proposed approach gets less energy consumption when compared to the existing schemes given in Table 5.

Table 4 Comparison for throughput

Pause time	Throughput (Kbps)		
	EE_RA	FIS	HBPR-SHPO (proposed)
12	80	700	710
24	90	680	682
36	100	660	650
48	130	640	650
60	150	600	620

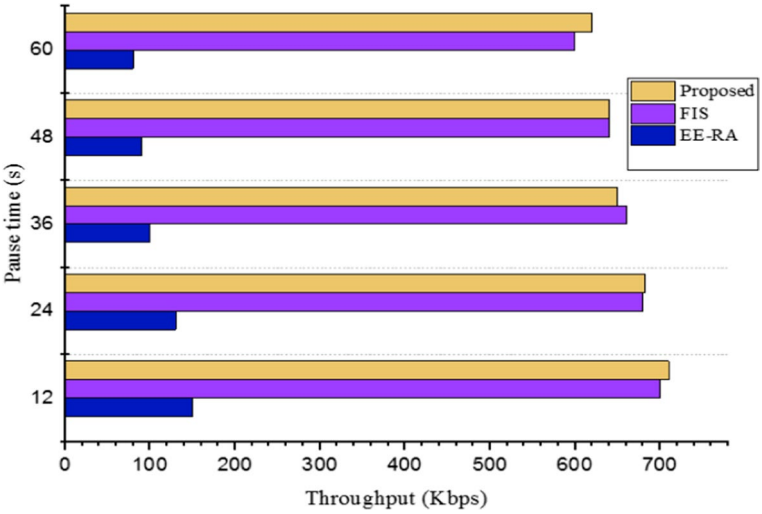

Fig. 9 Pause time versus throughput

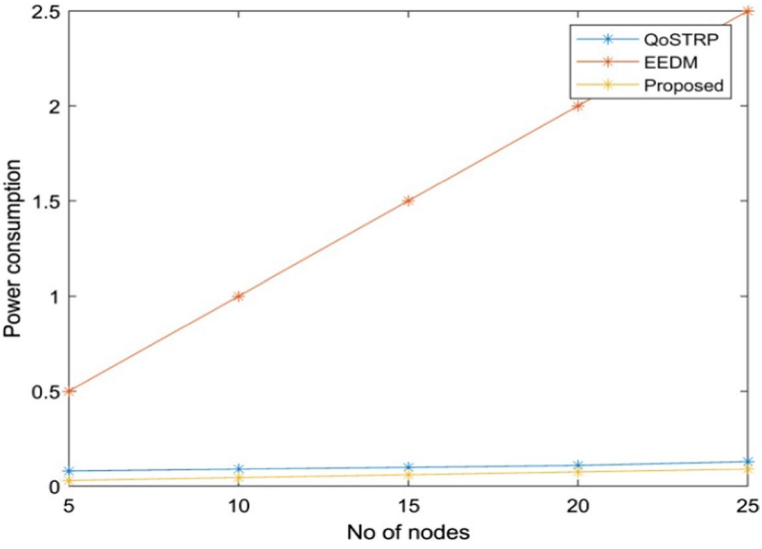

Fig. 10 Number of nodes versus energy consumption

5.2.6 Pause Time Versus End-to-End Delay

In this simulation, the impact of the number of node increases obtained delay is measured based on node pause time (transmission time) in seconds. The evaluation of the proposed approach is based on the measurement of delay, which is shown in Table 6.

The delay obtained in the network with various existing schemes like EE-RA and FIS is exposed in Fig. 11. This graph shows that the proposed HBPR has a low delay when

Table 5 Comparison for energy consumption

Number of nodes	Energy consumption (J)		
	LEACH- DT	QoSTRP	HBPR-SHPO (proposed)
5	0.08	0.5	0.03
10	0.09	1	0.07
15	0.1	1.5	0.08
20	0.11	2	0.05
25	0.13	2.5	0.1

Table 6 Comparison of delay based on pause time

pause time	End-to-end delay(s)		
	EE-RA	FIS	HBPR-SHPO (proposed)
12	4	30	2.9
24	2	22	2
36	4	28	3
48	4.5	24	5
60	5	20	4

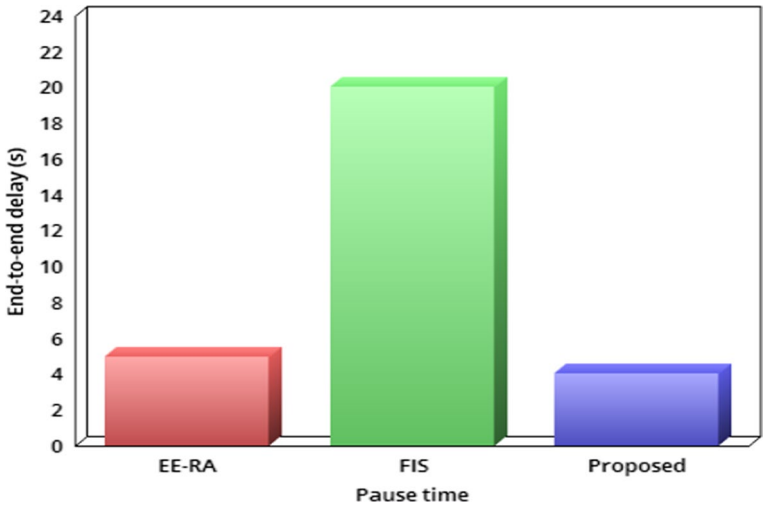

Fig. 11 Pause time versus end-to-end delay

compared with EE-RA and FIS. Also, the presence of end-to-end delay depends on the node pause time and the total number of nodes.

Finally, the proposed HBPR-SHPO approach predicts the harmful nodes and creates an alternate path for data transmission. Thus, the proposed technique achieves better

output in QoS parameters like throughput, end-to-end delay, packet delivery ratio, and energy consumption using a variety of network sizes and pause period.

6 Conclusion

In MANET, security maintenance is a complicated task because of the existing routing schemes is created more energy and more delay for data transmission when the link fails in the network. So, this paper proposed an HBPR routing protocol for reducing the delay and energy consumption of nodes in the network. Here, HBPR predicted the crashes and generates the alternate path when the node/link failures occurred in the network. Moreover, the node security is improved by SHPO that is helped to transmit the data optimally and securely. This approach reduced the PDR as 95%, the delay time is 10 s and 0.03 J lower energy and it improved QoS parameters while comparing to the existing techniques.

Acknowledgement None.

Compliance with Ethical Standards

Conflict of interest The authors declare that they have no potential conflict of interest.

Human and Animal Rights All applicable institutional and/or national guidelines for the care and use of animals were followed.

Informed Consent For this type of study formal consent is not required.

References

1. Sra, P., & Chand, S. (2019). QoS in mobile ad-hoc networks. *Wireless Personal Communications, 105*(4), 1599–1616. https://doi.org/10.1007/s11277-019-06162-y.
2. Kumar, H., et al. (2020). Study and design of route repairing mechanism in MANET. *Design Frameworks for Wireless Networks*. https://doi.org/10.1007/978-981-13-9574-1_6.
3. Banerjee, A., & Ghosh, S. (2019). WEEP: Weight based energy efficient priority scheduling of data packets in mobile ad-hoc networks. *International Journal of Information Technology, 11*(3), 435–443. https://doi.org/10.1007/s41870-018-0246-5.
4. Poongodi, T., Khan, M. S., Patan, R., Gandomi, A. H., et al. (2019). Robust defense scheme against selective drop attack in wireless ad hoc networks. *IEEE Access, 7,* 18409–18419. https://doi.org/10.1109/ACCESS.2019.2896001.
5. Ahmad, M., Hameed, A., Ikram, A. A., & Wahid, I. (2019). State-of-the-art clustering schemes in mobile ad hoc networks: Objectives, challenges, and future directions. *IEEE Access, 7,* 17067–17081. https://doi.org/10.1109/ACCESS.2018.2885120.
6. Ramya, P., & Gopalakrishnan, V. (2019). Proficient algorithms for enhancing topology control for dynamic clusters in MANET. *Cluster Computing, 22*(4), 9715–9726. https://doi.org/10.1007/s10586-017-1410-6.
7. Anand, M., & Sasikala, T. (2019). Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol. *Cluster Computing, 22*(5), 12681–12687. https://doi.org/10.1007/s10586-018-1721-2.
8. Pu, C., Lim, S., Chae, J., & Jung, B. (2019). Active detection in mitigating routing misbehavior for MANETs. *Wireless Networks, 25*(4), 1669–1683. https://doi.org/10.1007/s11276-017-1621-z.
9. Manolopoulos, I., Kontovasilis, K., & Stavrakakis, I. (2020). Methodologies for calculating decision-related event occurrence times, with applications to effective routing in diverse MANET environments. *Ad Hoc Networks, 99,* 102068. https://doi.org/10.1016/j.adhoc.2019.102068.

10. Howser, G. (2020). Open shortest path first. *Computer Networks and the Internet*. https://doi.org/10.1007/978-3-030-34496-2_17.
11. Nafarieh, A., Fazili, Y., Raza, M., & Robertson, W. (2016). Greenness link state advertisement extension for WDM networks. *Procedia Computer Science, 94,* 310–317. https://doi.org/10.1016/j.procs.2016.08.046.
12. Al-Musawi, B., Branch, P., Hassan, M. F., & Pokhrel, S. R. (2020). Identifying OSPF LSA falsification attacks through non-linear analysis. *Computer Networks, 167,* 107031. https://doi.org/10.1016/j.comnet.2019.107031.
13. Khudayer, B. H., Anbar, M., Hanshi, S. M., & Wan, T. C. (2020). Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks. *IEEE Access, 8,* 24019–24032. https://doi.org/10.1109/ACCESS.2020.2970279.
14. Kumar, S. S. (2019). Minimizing link failure in mobile ad hoc networks through QOS routing. *Innovations in Computer Science and Engineering*. https://doi.org/10.1007/978-981-10-8201-6_27.
15. Rahul, M. S., Arun, E., Shameem, P. M., & Rajeesh, J. (2017). An augmented routing algorithm for trusted detection of link failures in MANETs. *Wireless Personal Communications, 96*(4), 5185–5201. https://doi.org/10.1007/s11277-016-3735-5.
16. Jain, R., & Kashyap, I. (2019). An QoS aware link defined OLSR (LD-OLSR) routing protocol for MANETS. *Wireless Personal Communications, 108*(3), 1745–1758. https://doi.org/10.1007/s11277-019-06494-9.
17. Bai, X., Wei, X., & Bai, S. (2020). Efficient receiver-based flooding in mobile ad hoc networks. *Wireless Networks, 26*(1), 17–31. https://doi.org/10.1007/s11276-018-1779-z.
18. Zhang, D., Gao, J., Liu, X., Zhang, T., & Zhao, D. (2019). Novel approach of distributed and adaptive trust metrics for MANET. *Wireless Networks, 25*(6), 3587–3603. https://doi.org/10.1007/s11276-019-01955-2.
19. Yang, B., Wu, Z., Shen, Y., & Jiang, X. (2019). Packet delivery ratio and energy consumption in multicast delay tolerant MANETs with power control. *Computer Networks, 161,* 150–161. https://doi.org/10.1016/j.comnet.2019.06.003.
20. Malathi, M., & Jayashri, S. (2018). Robust against route failure using power proficient reliable routing in MANET. *Alexandria Engineering Journal, 57*(1), 11–21. https://doi.org/10.1016/j.aej.2016.10.004.
21. Soni, M., & Joshi, B. K. (2019). Security assessment of SAODV protocols in mobile ad hoc networks. *Data Science and Big Data Analytics*. https://doi.org/10.1007/978-981-10-7641-1_30.
22. Merlin, R. T., & Ravi, R. (2019). Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET. *Wireless Personal Communications, 104*(4), 1599–1636. https://doi.org/10.1007/s11277-019-06120-8.
23. Liu, S., Zhang, D. G., Liu, X. H., Zhang, T., Gao, J. X., & Cui, Y. Y. (2019). Dynamic analysis for the average shortest path length of mobile ad hoc networks under random failure scenarios. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.2896699.
24. Prabha, S., & Yadav, R. (2019). Trusted-differential evolution algorithm for mobile ad hoc networks. *Recent Trends in Communication, Computing, and Electronics*. https://doi.org/10.1007/978-981-13-2685-1_19.
25. Femila, L., & Beno, M. M. (2019). Optimizing transmission power and energy efficient routing protocol in MANETs. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-019-06202-7.
26. Bisen, D., & Sharma, S. (2018). An energy-efficient routing approach for performance enhancement of MANET through adaptive neuro-fuzzy inference system. *International Journal of Fuzzy Systems, 20*(8), 2693–2708. https://doi.org/10.1007/s40815-018-0529-9.
27. Bisen, D., & Sharma, S. (2018). Fuzzy based hybrid energy control technique to optimize hello interval of reactive routing in MANET. *National Academy science Letters, 41*(4), 211–214. https://doi.org/10.1007/s40009-018-0650-1.
28. Usman, M., Jan, M. A., He, X., & Alam, M. (2018). Performance evaluation of high definition video streaming over mobile ad hoc networks. *Signal Processing, 148,* 303–313. https://doi.org/10.1016/j.sigpro.2018.02.030.
29. Raja, R., & Ganeshkumar, P. (2018). QoSTRP: A trusted clustering based routing protocol for mobile ad-hoc networks. *Programming and Computer Software, 44*(6), 407–416. https://doi.org/10.1134/S0361768818060099.
30. Zhang, W., Zhu, S., Tang, J., & Xiong, N. (2018). A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks. *The Journal of Supercomputing, 74*(4), 1779–1801. https://doi.org/10.1007/s11227-017-2150-3.
31. Kavidha, V., & Ananthakumaran, S. (2018). Novel energy-efficient secure routing protocol for wireless sensor networks with mobile sink. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-018-0688-3.

Sunil Kumar received his MCA from Dr B.R. Ambedkar University, Agra and M.Tech in Computer Science and Engineering from A.P.J. Abdul Kalam Technical University, Lucknow in India. Presently pursuing Ph.D in Computer Science and Engineering from Department of Computer Science, IIMT University, Meerut Uttar Pradesh in India. He has published papers in International/National Journals.