International Journal of Emerging Science and Engineering (IJESE)
ISSN: 2319–6378 (Online), Volume-13 Issue-9, August 2025

Detecting and Predicting Malicious Nodes in Mobile Ad-Hoc Networks using a Secure Technique

Imran Khan, Pratik Gite

Abstract: *Mobile Ad Hoc Networking (MANET) is a rapidly growing area of interest in the realm of communication frameworks. Because the MANET lacks a basis, it exhibits the dynamic character of a self-assertive network architecture. Security concerns are critical in these networks. Nodes in MANETs may launch a variety of attacks or become conspicuously self-centred to maintain their advantage. These nodes may be considered malicious. Identification of such malicious nodes is critical for the successful operation of MANETs. A collection of networks has been presented, but each one has its own set of constraints. The scope of this proposal is to conduct research on black hole, wormhole, collaborative malevolent, and flooding attacks, and to establish a network of counteractive measures using responsive directing conventions. For execution analysis and replication, an AODV, NS-2 organised test network is used. To prevent black hole, wormhole, malevolent, and flooding attacks, a countermeasure is employed that calculates the Trust value based on the route request, route response, and information packet. Following the count, place stock in values ranging from 0 to 1. If the trust esteem is more than 0.5, the node is solid and permits access to the network as a whole. The suggested convention, secure Ad hoc On-demand Distance Vector (SAODV), is evaluated in terms of network performance. When compared to the standard AODV convention, the results reveal a notable difference in execution. By increasing the duration of a dip in throughput, SAODV achieves a throughput superior to that of the joint malicious assault AODV and the current protocol. SAODV's packet delivery ratio is superior to that of the joint malicious attack AODV and the established AODV protocol. SAODV's end-to-end delay is superior to the joint malicious attack AODV and the current AODV protocol.*

Keywords: *Mobile Ad Hoc Networking, AODV, SAODV, NS2, End-to-End Delay, Packet Delivery Ratio, Throughput*

Abbreviations:
TCP: Transmission Control Protocol
QB: Queen-Bee
QOS: Quality of Service
IDS: Intrusion Detection Systems
PANs: Personal Area Networks
CBR: Constant Bit Rate
SAODV: Secure Ad hoc On-demand Distance Vector

Manuscript received on 24 May 2025 | First Revised Manuscript received on 15 June 2025 | Second Revised Manuscript received on 01 August 2025 | Manuscript Accepted on 15 August 2025 | Manuscript published on 30 August 2025.
*Correspondence Author(s)
Imran Khan*, Scholar, Department of Computer Science Engineering, IES IPS Academy, Indore (M.P.), India. Email ID: Imran.khanikik@gmail.com
Pratik Gite, Assistant Professor, Department of Computer Science Engineering, IES IPS Academy, Indore (M.P.), India. Email ID: pratikgite@ipsacademy.org

I. INTRODUCTION

Multi-hop network pathways can be established in a Mobile Ad Hoc Network (MANET), where each node acts as a router, eliminating the need for a telecommunications backbone.

When a wireless network is used in place of a wired network, it is ideal for military and emergency rescue operations, as well as for short-term classroom or conference events. The security of such a network must be given high importance. The openness of the wireless medium allows outsiders to observe and interfere with network activity, as a consequence of its use by criminals.

Such considerations may expose sensors to a broad variety of assaults [1] because of their implementation. These malicious nodes are capable of launching both passive and aggressive assaults on the network from their positions. On the other hand, active assaults may require the rogue node to spoof or reject real messages in addition to just listening in on them. Wormhole attacks are a common type of active security attack that has the potential to cause significant harm. An attacker collects packets from one site in a network and delivers them to another malicious node, which then repeats the packets in its network, thereby causing the network to crash. This active assault poses a threat to wireless security systems and routing protocols, as well as aggregated and clustered data storage systems. The active attack may also be initiated even if no cryptographic keys have been given.

MANET is a wirelessly linked network of mobile nodes that may operate independently of one another and communicate with one another. It is not founded on any solid basis. The router function is performed by each node in the centre of the network in this scenario. When a node moves from one location to another, MANET ensures that the device remains available and that it can adapt to the new environment. Routing packets from the source node to an adjacent node allows them to be routed until they reach their ultimate destination. A lack of constant wireless connections between mobile nodes in an ad hoc network poses a problem for communication participants due to insufficient energy, which prevents the nodes in the network from moving freely. Another stumbling block is the topology of the dynamic network itself. Nodes in MANETs can join or leave the network at any moment, as well as travel independently of one another. MANETs do not have a predefined topology because of the nature of the network type. If nodes are not physically safeguarded,

they have the potential to become malevolent and cause network performance to suffer. These networks are especially vulnerable to malicious attacks due to their key characteristics, which include dynamic topology, wireless medium, and bandwidth limitations [3].

Reactive, proactive, or a mix of the three [4] types of MANET protocols can be found. MANET routing technology focuses on establishing routes between mobile nodes that are both energy-efficient and meet quality of service requirements, such as bandwidth and end-to-end latency, which are crucial to the technology's operation. In MANET protocols, you can use AODV, DSR, RAODV, AOMDV, and TORA, among other methods, to quickly transfer information from one location to another (TORA). AODV is superior to other reactive routing protocols in terms of important quality of service (QoS) criteria, particularly in modelling black holes [5]. [6] People use the AODV and DSR protocols the most when they use a MANET. Integration of DSR and DSDV routing protocols is also part of the package. This gives you the best of both worlds.

When using the AODV protocol, there must be ways to find and manage routes to avoid routing loops. Denial-of-service (DoS) attacks are the most common type of attack on MANETs [7]. They use the most electricity. Using another strategy [8], developed a wireless sensor network cluster algorithm based on the Queen-Bee (QB) algorithm, which they then utilised to construct the algorithm. Its ability to determine the best value for the local minimum is enhanced by the method's rapid convergence, which makes it a more efficient algorithm. Normal and severe mutations are thought to make future generations more diverse and able to ignore early differences. The results show that the proposed QB algorithm is more energy efficient than the genetic algorithm (GA), which means the network will last longer in the long run.

According to [9], they developed a hierarchical clustering algorithm (HCAL) and a protocol for massively parallel mobile ad hoc networks (MANETs). When table-based and on-demand routing weight matrices are combined, a collection of the network's most important nodes is obtained. The LMANET network was constructed using the node count and timeout values for each connection. Additionally, it was determined how long it took to run, the time required to complete the task, the necessary amount of overhead, and the amount of PDR required. The new HCAL protocol outperforms its predecessors in terms of functionality. Dynamic Doppler velocity clustering is compared to clustering based on signal characteristics, dynamic link duration, dynamic mobility, and other factors.

Section 2 is called "Literature Work." The rest of the paper is organised as follows: Section 3 proposes a method, Section 4 describes the implementation and results, and Section 5 summarises our paper.

II. LITRACTURE WORK

Personal area networks (PANs) and Bluetooth are examples of ad hoc wireless communication networks. Ad hoc networks are also used in other types of wireless communication, such as wireless LANs. When it comes to providing reliable communication between nodes, especially under demanding settings, there is an increasing need to investigate MANETs. These networks, on the other hand, contain several security weaknesses that must be addressed. Over the past few years, numerous researchers have proposed a wide range of solutions to enhance MANET security, including, but not limited to, cryptographic approaches, protocol enhancements, and intrusion detection systems (IDS). Their solution for MANET IDS is based on a neuro-fuzzy approach, which they discuss in full in [11]. For intruder detection and identification, it was a pioneer in the use of a fuzzy method, which is still in use today. It was recommended that an enhanced trust detection technique be used to detect and block malicious attackers in MANETs, which enhanced the effectiveness of the strategy.

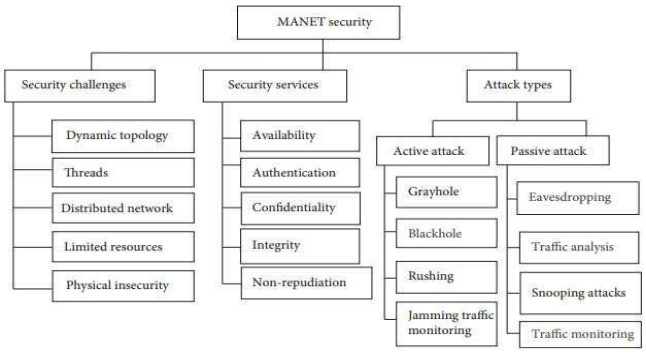
Using this technique, malicious nodes are avoided in MANETs, network performance is increased, packet loss is minimised, and power consumption is reduced when harmful malicious nodes are present. Another possibility mentioned in [10] is the use of detection algorithms that have a low network overhead. This method has the potential to enhance the density of dense networks by 45.6% while increasing the sparsity of sparse networks by 41%. Furthermore, it reduces the number of lost packets by 75% in dense networks and by 63% in sparse networks when used in conjunction with other techniques.

A honeypot-based security solution is provided to enable improved packet delivery with fewer packet losses, as well as reduced end-to-end latency and network strain from one end to the other. The authors of this study propose a dynamic destination sequence number threshold value that identifies and disables malicious nodes, outperforming both malicious assaults and malicious attacks [2]. Another research group has developed mathematical approaches for recognising and avoiding malicious nodes in MANETs, which they believe may be helpful in the future. Furthermore, various methods have been designed to address the security flaws of MANETs.

It is challenging to maintain network security in a MANET since there are no defined boundaries, adversaries within the network continue to operate uninterrupted, and there is no centralised management. As a result, MANETs are vulnerable to a wide range of different types of assaults. This includes, but is not limited to, attacks such as the black hole, eavesdropping, and man-in-the-middle attacks, as well as wormholes, impersonation, and other similar techniques. These assailants might be violent or calm in their approach. It was discovered that the malicious assault was one of the most lethal attacks carried out by these perpetrators. Attacks on MANETs may be prevented in one of two ways: either by being proactive or by reacting to an attack. However, once an assault has been launched, there are several options for responding to it. Many approaches may be taken to prevent an attack from being launched in the first place. It is necessary to utilise both detection and prevention techniques, as well as a response component, to create a comprehensive security solution. Several mitigating

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

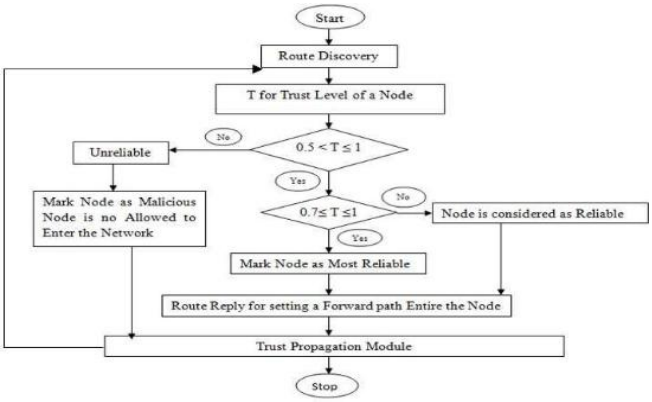
and preventive security measures can be implemented to ensure secure routing. Figure 1 illustrates the potential security vulnerabilities that may arise in MANET systems.



[Fig.1: Attacks in MANET]

III. PROPOSED METHOD

A. Proposed Architecture of Secure AODV



[Fig.2: Flow Chart for Secure AODV Model]

Secure AODV, a secure routing system based on trust display, may be implemented in mobile ad-hoc networks. Secure AODV has a broad range of key characteristics, including the following: Secure routing protocols are often deployed by nodes based on their connections with other nodes and the level of trust they have in one another. After a while, a malicious node will be found and removed from the network as a precaution. Each route node has the potential to contribute to improved network processes.

B. The Degree to Which a Node is Secure

The AODV routing protocol, along with the trust function, is implemented in this work. It is only via the cooperation and trust of their neighbours that nodes in a mobile ad-hoc network may become members. There are many sorts of nodes that may be classified based on their neighbour trust and threshold levels:

"Unreliable" is the term used to describe a node that is not trustworthy. A node with a low degree of trust is seen as being untrustworthy by the other nodes. When a node initially enters the network, it does not have any trust linkages with its neighbours, and as a result, it is tagged as unreliable by the network.

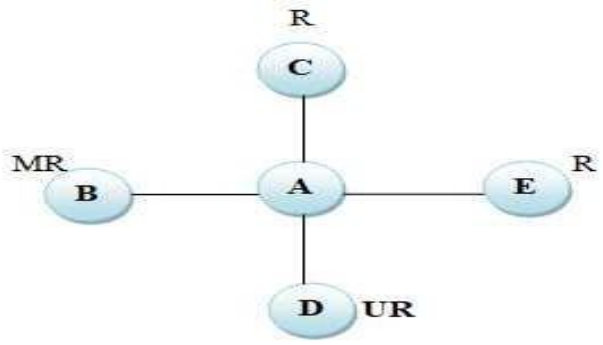
These are the nodes that have a trust rating that is in the centre of the range between "most trustworthy" and "least dependable." In the case of receiving two or three packets from a neighbouring node, it decides that the neighbouring node is trustworthy.

The term "most reliable" refers to the nodes that are the most trustworthy, or those with the highest degree of confidence. When a node's trust level is high, it is more probable that other nodes in the network have successfully accepted or exchanged packets with that particular node.

While the route discovery phase is in progress, AODV Routing keeps track of the trust values of each node's neighbouring nodes. All of your neighbours are evaluated as either Most Reliable, Reliable, or Undependable by the trust evaluation technique after the process is complete.

Because each node in this system maintains a copy of the Trust table, it is possible to monitor for suspicious activity. To keep track of a node's relationships with other nodes, it is necessary to utilise the Trust table. The Trust table consists of two components. The name of the node that surrounds an individual node, as well as the relationship status, which might be Most Reliable, Reliable, or Unreliable. Alternatively. Each time a packet is received, it is removed from this table and placed elsewhere.

For starters, every new node is seen as untrustworthy by the system as a whole. Unreliable has a high danger of being attacked, while Most Reliable has a low chance of being attacked.



[Fig.3: Trusts for Node]

Table-I: Trust for Node A

Neighbouring Nodes	Trust Status
B	Most Reliable
C	Reliable
D	Unreliable
E	Reliable

As seen in Fig. 3, node B is the most trustworthy, followed by nodes C and E, and finally node D, which is the least reliable. We choose a path for each node that begins at B, the node with the highest level of dependability. If there is

Since there is no node with the Most Reliable status, we feed the requirement to Reliable nodes, but never allow an Unreliable node to establish a route under these circumstances.

c) The Threshold Value of a Node: Neighbours vary in their reliability; some are more trustworthy than others, and some are more unreliable than others. There are three levels of reliability: unreliable, reliable, and most reliable. Each level has a threshold value of Tmr, Tr, and Tur.

We provide a Trust estimate job that can be used to calculate trust value.

$$T = \tanh(R1 + R2)$$

Where,

Tanh is a hyperbolic tan function, which has a

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

value.

$$Tanh\ X = (e^{x} - e^{-x})/(e^{x} + e^{-x})$$

T = Trust value

R1 Ratio between the number of packets sent and the number of packets to be sent.

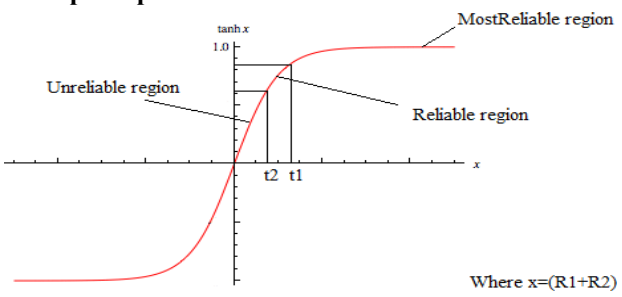
R2 = Ratio of the number of packets received from a node; however, it started from another to signify the number of packets received from it.

C. Trust Status Updating of a Node

It is only after receiving an RREP from each neighbour that the source node can identify which route is the most efficient. We send out a large number of erroneous packets to re-establish trust. The stock statuses of nodes are computed and, if necessary, updated as part of the packet-processing process. A node must first achieve the threshold trust level of Tr before it can be considered visibly Reliable to its neighbour. It is necessary for a node to first accomplish the dependability level of Tr before attempting to attain the threshold trust level of tmr. The Trusts will be referred to as such for the time being.

A (node x → node y) = Most Reliable when T≥ tl
A (node x → node y) = Reliable when t2 <T<tl
A (node x → node y) = Unreliable when 0<T ≥t2
Where,
A= Trust
T= Threshold
And t1 and t2 are the threshold values which will be decided in the implementation part.

D. Graph Representation of Trust Values of a Node:



[Fig.4: Representations of Trust Values of a Node]

In the above graph, the value of x is always greater than 0, because R1 and R2 will always remain positive, so T belongs to the interval (0, 1).

IV. SIMULATION TOOLS AND RESULTS

A. Simulation Parameters

The researchers tested the MANET protocols in this work using a simulator named NS2. The researchers developed this simulator. A software called "cbrgen" can be used to detect random traffic between nodes connected through a Transmission Control Protocol (TCP) or a Constant Bit Rate (CBR) connection. It is located in the "ns/independent-utils/cmu-scene-gen" directory. The "setdest" command may also be used to create node traces by randomly shifting nodes according to their speed to any unfixed location within the wireless range. The "ns" directory contains a file named "setdest." Additionally, it may be found in the directory "ns/independent-utils/CMU-Scen-Gen/SetDest". A small network may be constructed manually by randomly dispersing the network's nodes at each waypoint. Then, traffic connections and node mobility may be accomplished manually. Moving nodes are employed to create the wireless network environment that you see today.

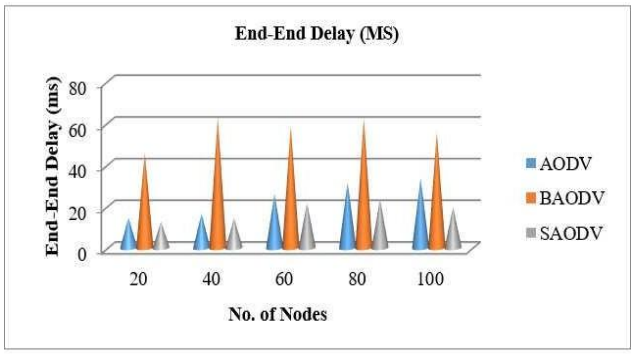
Table-II: Simulation Parameters

Simulation Parameters	Value
Number of Nodes	20,40,60,80,100
Network Size	1200m*1200m
Simulation Duration	100(Sec)
Primary Energy	100 joules
Txpowers	0.9/sec.
Repowers	0.8/sec.
Idle Power	0
Sense Power	0.0175
Source Node	5
Destination Node	5
Intermediate Nodes	15
Malicious Node	5,10,15,20,25
Packet Size	1024byte

B. Result

End-to-End Delay: This is Also Known as the End-to-End Delay. When there are more malicious nodes, the time it takes for AODV to complete its operation increases. The SAODV's end-to-end delay increases by an extra step, but it remains as safe as that of AODV.

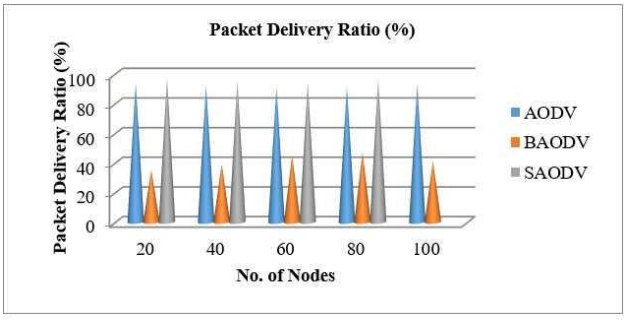
EED = Total EED / No. of Packets Sent



[Fig.5: End-to-End Delay]

Packet Delivery Ratio: "application layer" Constant Bit Rate source and Constant Bit Rate source receive less than one packet at a time during their last goal.

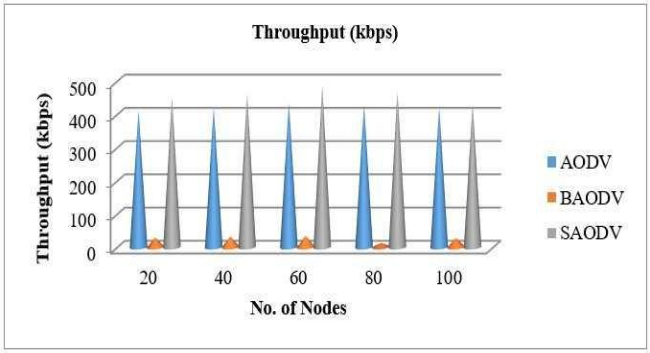
PDR = Packets Delivered / Packets Sent



[Fig.6: Packet Delivery Ratio]

Throughputs: The usual rate of successful packet transmission through a communication channel is referred to as throughput.

Throughput = Number of Packets Sent / Time Taken



[Fig.7: Packet Delivery Ratio]

V. CONCLUSION

Slowing down the system's execution by keeping a critical separation will be the primary objective of this evaluation, which will begin by alternately maintaining the combined assault and then proceeding from there. SAODV's participation in the AODV meeting is a notable highlight in our evaluation. More than one person is attacking MANET, as this incident demonstrates. An assault requires the use of NS-2 simulations to establish the parameters. To meet the criteria, both community-oriented and collaborative harmful attacks must be included. SAODV's throughput is better than that of AODV and the current protocol because it increases the length of time a drop in throughput influences the overall throughput. SAODV's packet delivery ratio is much greater than that of AODV and the current AODV protocol. The present AODV protocol and the collaborative malicious attack AODV protocol, SAODV's end-to-end latency is superior to both of them.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCE

1. I. Mohd Zaki and H. Rosilah, "The implementation of Internet of Things using test bed in the UK Mnet environment," Asia Pacific Journal of Information Technology and Multimedia, vol. 8, no. 2, pp. 1–17, 2019. DOI: http://dx.doi.org/10.17576/apjitm-2019-0802-01
2. K. L. Arega, G. Raga, and R. Bareto, "Survey on performance analysis of AODV, DSR and DSDV in MANET," Computer Engineering and Intelligent Systems, vol. 11, no. 3, pp. 23–32, 2020. DOI: http://doi.org/10.14445/22315381/IJETT-V69I8P225
3. T. Salam and M. S. Hossen, "Performance analysis on homogeneous LEACH and EAMMH protocols in wireless sensor network," Wireless Personal Communications, vol. 113, no. 1, pp. 189–222, 2020. DOI: https://doi.org/10.1007/s11277-020-07185-6
4. M. S. Hossen, "DTN routing protocols on two distinct geographical regions in an opportunistic network: an analysis," Wireless Personal Communications, vol. 108, no. 2, pp. 839– 851, 2019. DOI: https://doi.org/10.1007/s11277-019-06431-w
5. N. Khanna and M. Sachdeva, ''BEST: Battery, efficiency and stability based trust mechanism using enhanced AODV for mitigation of blackhole attack and its variants in MANETs,'' Adhoc Sensor Wireless Netw., vol. 46, nos. 3–4, pp. 215–264, 2020. https://dl.acm.org/toc/ijirr-igi/2022/12/3
6. R. Fotohi, E. Nazemi, and F. S. Aliee, ''An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks,'' Veh. Commun., vol. 26, Dec. 2020, Art. no. 100267. DOI: https://doi.org/10.1016/j.vehcom.2020.100267
7. A. Nabou, M. D. Laanaoui, and M. Ouzzif, ''New MPR computation for securing OLSR routing protocol against single malicious attack,'' Wireless Pers. Commun., vol. 115, pp. 1–20, Nov. 2020. DOI: https://doi.org/10.1007/s11277-020-07881-3
8. N. C. Singh and A. Sharma, ''Resilience of mobile ad hoc networks to security attacks and optimization of routing process,'' Mater. Today, Proc., 2020. DOI: https://doi.org/10.5120/ijca2022921988
9. M. Faraji-Biregani and R. Fotohi, ''Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles,'' J. Supercomput., vol. 76, pp. 1–28, Nov. 2020. DOI: https://doi.org/10.1007/s11227-020-03462-0
10. H. M. Haglan, S. A. Mostafa, N. Z. M. Safar et al., "Analyzing the impact of the number of nodes on the performance of the routing protocols in MANET environment," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 1, pp. 434–440, 2020. DOI: https://doi.org/10.1007/978-981-16-1866-6_23
11. R.-R. Yin, N. Zhao, and Y.-H. Xu, ''A selective forwarding attack considered routing protocol for scale-free network,'' in Proc. 12th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP), Jul. 2020, pp. 1–6. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9336623

AUTHORS PROFILE

Imran Khan received a B.E. (C.S.E.) from the Jawaharlal Institute of Technology, Borawan, Khargone, in 2019, and an M.E. (C.S.E.) from IES, IPS Academy, Indore, in 2022. His areas of interest are Mobile Ad-hoc Networks, Software Testing, Software Engineering, and Computer Networks. He has published two papers in various international and national conferences.

Dr. Pratik Gite has completed his B.E. and M.E. from RGPV University, Bhopal (M.P.). He holds a PhD in Wireless Mobile Ad-hoc Networks from Pacific Academy of Higher Education & Research University, Udaipur, Rajasthan. He began his academic studies at LKCT Indore (MP).