Hindawi
Security and Communication Networks
Volume 2023, Article ID 9808670, 1 page
https://doi.org/10.1155/2023/9808670

Retraction

Retracted: A Low-Latency and High-Throughput Multipath Technique to Overcome Black Hole Attack in Mobile Ad Hoc Network (MTBD)

Security and Communication Networks

Received 26 December 2023; Accepted 26 December 2023; Published 29 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] D. Ramachandran, S. S, V. Rajeev Ratna et al., "A Low-Latency and High-Throughput Multipath Technique to Overcome Black Hole Attack in Mobile Ad Hoc Network (MTBD)," *Security and Communication Networks*, vol. 2022, Article ID 8067447, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8067447, 13 pages
https://doi.org/10.1155/2022/8067447

Research Article

A Low-Latency and High-Throughput Multipath Technique to Overcome Black Hole Attack in Mobile Ad Hoc Network (MTBD)

Dhanagopal Ramachandran,[1] **Sasikumar S**,[2] **Vallabhuni Rajeev Ratna**,[3] **Vijayprasath S**,[4] **Suresh Kumar R**,[1] **Vasanth Raj P T**,[1] **Ilhan Garip**,[5] **and Umamahesawari K**[6]

[1]*Centre for System Design, Chennai Institute of Technology, Kundrathur, Chennai, India*
[2]*Department of ECE, Hindustan Institute of Technology & Science, Kelambakkam, Tamil Nadu, India*
[3]*Application Developer, Bayview Asset Management, LLC, Coral Gables, FL, USA*
[4]*Department of Electronics and Communication Engineering, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India*
[5]*Department of Electrical and Electronics Engineering, Nisantasi University, Istanbul, Turkey*
[6]*Kebridehar University, Kebri Dehar, Ethiopia*

Correspondence should be addressed to Dhanagopal Ramachandran; dhanagopal.phd@gmail.com and Umamahesawari K; uma@kdu.edu.et

Received 2 June 2022; Revised 29 June 2022; Accepted 28 July 2022; Published 25 August 2022

Academic Editor: Tao Cui

Security in MANETs is a highly contentious topic in the field of network management. The availability and functionality of a MANET might be compromised by a variety of attacks. One of the most prevalent active attacks used to degrade network speed and reliability is the black hole attack, which leads the compromised agent to discard all data packets. The purpose of a black hole node is to trick other access points into thinking that they must use their node as their route to a certain destination. The black hole node in a cable network cannot be detected or eliminated in an AODV network. We improved AODV in this study by utilizing a lighter-weight technique based on timing and baiting for detecting and separating single and collaboration black hole attacks. MANETs have a dynamic topology, an open medium, and a lack of a highly centralized monitoring point, all of which offer security problems. Attacks on security are one of the sorts of attacks. In MANETs, it has no central administration, and mobile devices link to other devices wirelessly. Black holes, insider attacks, gray holes, parallel universes, faulty nodes, and packet drops are all threats that can cause considerable disruption in secure communication. Simulation findings demonstrate that the proposed method significantly outperforms previous techniques in terms of end-to-end delay, throughput, packet delivery ratio, and average energy. A multipath methodology is used in our proposed method to mitigate the black hole attack in MANET. The proposed technique is tested in a simulation reality to see how stable it is in the face of an attack. When the proposed method's results are compared to those of existing state-of-the-art approaches, it is discovered that the acquired results are satisfactory.

1. Introduction

MANET is a self-contained system in which nodes/stations connect with one another using wireless networks. The ability of nodes to connect to or leave the system is unfettered; hence, node connectors may depart at whim. MANET design is dynamic and may change fast with impact on the nodes' capacity to transmit freely and order them arbitrarily. Because of this attribute of the nodes, the MANETs are unpredictable in terms of durability and topology.

MANET is a Wi-Fi ad hoc network, wherein the nodes are permitted to move around at will and mobile nodes can send and receive data. Also, because wireless routers are multiple hop devices, wireless routers are operated by mobile nodes by forwarding traffic from other nearby nodes to the location node shown in Figure 1. MANET does not require wired

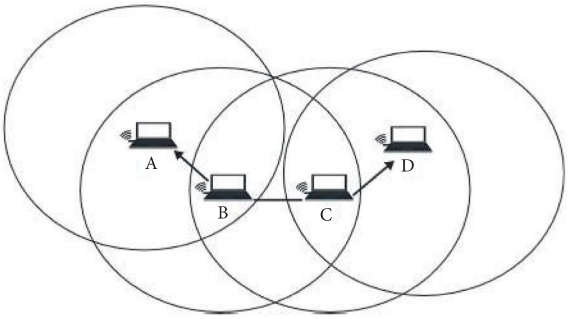

Figure 1: MANET.

facility platform channels. Network clients of Wi-Fi will connect mobile nodes with a self-organized network. Without any established infrastructure or central control, the mobile nodes instantaneously produce a network.

Wireless sensor networks (WSNs) are a major topic in communications research right now. Tiny-structured sensors with limited resources are getting easier to improve. In addition, they appear to be able to perceive the environment's parameters, gather important data, and communicate this knowledge to the user. When it comes to implementing the 4.0 industrial revolution, intensive research is needed to ensure that the Internet of Things (IoT) works properly [1]. Ad hoc networks do not have a central access point, but infrastructure-based networks have. Due to its wireless nature, a mobile ad hoc network (MANET) can be established as a multihop packet network with no fixed infrastructure [2]. The packet sizes, data rates, transmission ranges, and speeds of these nodes and devices might vary widely. Autonomous, multihop, and dynamic topology are just a few of the MANET's distinctive features. Other issues such as packet loss, security, and QoS are also present in these networks. The establishment of basic connection among distinct nodes necessitates the use of routing mechanisms.

Even if the attacker node does not truly have the quickest path to any targeted network node, all packets will still travel through it, giving the black hole node the ability to forward or reject packets while the data transmission is still in process. An active attack type is black hole attack. The black hole node takes advantage of the fact that every response from an ordinary node is taken for granted by acting as though it has a shorter path to any requests it gets. Nodes typically start the discovery phase to find a route to the end node of interest. Whenever a node receives a request from a source node, it checks to see if it has a new route to the destination node. As soon as the broadcaster requests this information, the black hole node responds by saying that it has the most recent and shortest route to the destination node. The source node accepts the response as fact since there is no way to determine if the request was sent by a regular node or a black hole node. To ensure that packets are sent to their intended destination, source servers begin sending them to the black hole node, which subsequently begins dropping the packets they received. Based on the number of attacker nodes, black hole attacks may be divided into single and cooperative attacks. A single attacker node is involved in a single black hole assault, as opposed to a cooperative black hole attack, which involves many attacker nodes cooperating to undermine network stability [3].

In addition to denial-of-service (DoS) attacks, which consume the most energy, the lack of an infrastructure exposes MANETs to a wide range of other threats [4–6]. Premature convergence increases the algorithm's capacity to discover the best value for the local minimum. Premature divergence can be ignored because it deems significant mutations to be normal, resulting in greater genetic variety among children. There was a significant improvement in energy efficiency and a consequent extension of network lifetime using QB's proposed algorithm over GA. The goal is to find a dominant collection of nodes by combining the weight matrices of table-driven and on-demand routing. Using the node's relative degree and the link expiration time, the LMANET was interconnected. We measured delay, total cluster head rounds, cluster head duration, overhead, and PDR to arrive at our conclusions. The proposed HCAL protocol outperforms in terms of performance. Clustering algorithms such as dynamic link duration, signal characteristic-based, dynamic Doppler velocity, and mobility-based algorithms are compared with each other. There is a well-defined organizational structure in place for these pieces, and it serves to emphasize their value by bringing attention to what was omitted and by posing important concerns that need additional investigation. After a thorough examination, specific observations are collected in order to assist in determining which risk reduction techniques are most suitable for a particular environment and then to communicate those strategies with the relevant parties [7].

Problem Statement: MANET security is critical in order to prevent many forms of attacks. An attack known as a "black hole" aims to break up all network connections and is one of the most widely used methods of doing so. In the event that two network nodes need to interact, the AODV routing protocol strives to find the shortest possible path between them. This attack cannot be detected or prevented by the AODV protocol because it does not include an algorithm for that. This research presents the method for identifying and differentiating between single and collaborative black hole attacks.

Contribution of the work is as follows:

(a) Taking care of low latency while maintaining high throughput is the contribution of this study.

(b) Above both are planned to achieve using new algorithm, which is called as multipath technique to overcome the black hole attack in mobile ad hoc (MTBD).

(c) The paper suggests a pseudo-code algorithm that is distributed randomly for energy-efficient time synchronization in two-way packet delivery scenarios, where the clock offset and the propagation delay are factors to consider when sending the packet beacon message to the destination vehicles.

The paper is organized as follows. Section 2 discusses related work. Section 3 introduces the existing mobile ad hoc network model and shows the role of the network identity. Section 4 presents the algorithms for formation/joining a network and how split and merge are managed. Sections 5 and 6 show the experimental setup and experimental results, respectively, and, finally, Section 6 concludes the paper.

2. Related Work

2.1. Black Hole Attack. DoS is a kind of black hole attack that is considered as one of the more attractive attacks. In MANETs, it is also referred as a full average packet attack. With changeable protocols and free communications in MANETs, a black hole component can easily and quietly move inside the network. Route discovery is the exact situation which is suitable for black hole creations. There is no valid path from the originating point to the destination at first. For route discovery, the source node sends a RREQ packet to the works by interfering. When a real sender moves an RREQ packet from a sender, it transfers it to the next node in the chain if it is not a cluster head; however, whenever a black hole node receives an RREQ, it transfers a fraudulent route reply with a high timestamp in order which is going to win the route request. The hash function is being utilized in assessing where frequently the route is updated, or how fresh it is. The black hole node manipulates the base station into thinking it has a legal, short, and refreshing route toward destination when it actually does not. The black hole node delivers a signal to the intermediate host and joins the program's route between both the initial point and the final node in this approach. The source node begins transmitting packets of data to the black hole nodes after the path has been created, and the black hole node gradually destroys all data packets before passing them on to the destination's node [8, 9]. Figure 2 shows black hole attack.

Each node in a MANET maintains a routing table, and each routing table maintains a sequence number, which is used to keep current routing information. The source node sends data packets to the destination node via neighbor nodes, which contain sequence numbers that are used to determine the proper path connection to the link. More update information equals a higher sequence number. The value of the sequence number is 216-1. It wraps around after the end of the sequence number value and returns to the original value. In a mobile ad hoc network, black hole nodes are mobile nodes that present more updated information by displaying a higher sequence number value (a higher sequence number indicates more updated information, whereas a lower sequence number indicates less updated information in the routing table). Because the sequence number of the black hole node is higher than the current flack sequence number, the node maintains its course through the black hole node. Neighbor nodes send data packets through the black hole, which the black hole node drops.

The method's strength comes in its ability to pinpoint optimal values for such variables as detection probability and throughput. This approach aids in both the detection and prevention of black hole attacks in MANET [10]. When malicious nodes misinterpret routing for dissemination, only the least diverted packets eventually make it to the target hub, and a route layer vulnerability known as a black hole assault is launched. Through simulations, [11] demonstrated that an NHBADI approach for identifying attackers in MANET reduced network inefficiency, PDR, and the normalized routing cost. Not only was the attack discovered, but the suggested method also isolated vulnerable nodes for black holes in the MANET. Proximity set method was developed by [12] to identify malicious nodes in MANET (PSM). Simulation findings show that the proposed AODV with PSM is superior to the current ad hoc on request distance vector direction methodology for discovering black holes. However, the E2E delay was subpar. The IDS method was proposed for black hole detection in [13]. Selecting the node with the greatest sequence number leads to improved QoS and, following analysis, a 60% boost in PDR. One potential drawback is that it is not very effective against intrusion attempts.

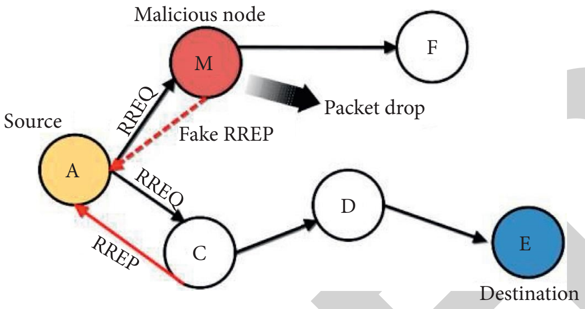

Figure 2: Black hole attack.

The benefit point of this approach is that a comparative approach for the protocols is helpful for the determination of black holes. IoT is a critical constituent of the industrial revolution 4.0, and its operation necessitates intensive study to guarantee that it functions properly [14]. AODV, DSR DSDV, reverse-AODV (RAODV), AOMDV, and temporally order routing algorithm (TORA) are some of the MANET protocols [14]. Packet networks are a type of packet network. Because of its mobility, it is a wireless system with a self-motivated topology [15]. Furthermore, with no permanent infrastructure, each node is operating as a bridge, source, or a destination in order to pass data packets to nodes outside the transmission range [16, 17]. This approach uses a digital signature-based IDS for identification of attacks on black holes.

3. Existing Work

3.1. FIDS. Handout of this approach lies in the smooth detection of black holes. It uses NS-2 simulators for better results. This approach is shown to be efficient than the normal AODV protocols. For AODV, [18] developed a mechanism for detecting black holes. Reference [19] presented a fuzzy-based genetic algorithm that uses beginning rules depending on fuzzy algorithm and final rules depending on GA. Reference [20] suggested a TCP/IP network based on genetic-based IDS. Reference [21] investigated RREQ flooding attacks and devised a new strategy based on next node monitoring to counter RREQ flooding attacks. Pitfall lies with its limitation of working with only one kind of attack along with low jitter values.

3.2. GABFO. Beneficence of this approach is that one can make a clear black hole attack analysis. This approach uses GA with a combination of BFO using which the black hole attacks are defended. The obstacle for this approach is that it is limited to few protocols and does not work in AODV protocol. MANETs are defined by their lack of housing, dynamical topology, and usage of the open wireless medium [22]. A black hole assault poses a significant threat to such networks. There are two purposes to this study. To begin, we will go through a comprehensive list of known black hole countermeasure methods. Reference [23] suggested a method for analyzing AODV's vulnerability to assaults, particularly the most prevalent network layer hazard, the black hole attack, and developing a conditional-based IDS using the GA method. The suggested arrangement uses a GA to assess each node's behavior and provide information about the attack. GAC is a collection of rules based on AODV's key features, such as request forwarding rate and reply receive rate.

3.3. NSABO. High packet delivery with minimum packet loss is one of the features of the proposed method. A proposed framework with the help of a simulator NS-2 works. Reference [24] presented a dynamic training method for anomaly detection where the supervised learning is restructured at regular intervals of time. Reference [25] proposed a technique in which the source verifies the reply a packet arriving from various nearby nodes, and then waits and checks the responses from all cluster heads to choose the finest and most protected route. The highlight of this approach lies in the detection of a secured receiver and senders' path; the pitfall of this approach is that it is limited to a few and general attacks. Reference [26] presented a system in which network nodes are divided into two categories: trustworthy nodes and regular nodes. Trusted nodes are nodes that are present in the network when it is created. Ordinary nodes are nodes which join the network at a later time. Ordinary nodes must demonstrate their reliability to be designated as trusted nodes.

3.4. SAODV. The plus point of this approach is that it is helpful in the discovery of black as well as gray hole attacks. Numerous DoS attacks have been launched. The black hole attack is the one where the attacker announces that it has the best path to the node whose packets it intends to discard or intercept using the routing protocol [27]. RREQ packets are broadcasted, whereas destination network receives data packets sent from source nodes which shows the black hole attack working nature. The black hole cluster with a higher sequence number and fewer hop counts, on the other hand, delivers RREP to the originating node right away [28]. This approach is helpful for the detection and prevention of malicious selfish nodes. The downfall of this approach is that it is limited to work with only one kind of protocol.

3.5. TBBTD. Contribution lies in isolating the detected black hole nodes. A timer-based baited technique is used. MANET practices a wireless link to attach nodes; therefore, throughput is considered a significant network feature. Wireless links have a substantially lower bandwidth than conventional lines. The signal of a wireless link can be harmed by noise, interfering from that other source, or fading [2]. According to [29], AODV has superior performance features than additional routing protocols underneath various performance statistics; The AODV protocol is superior to other routing protocols because it combines the principles of mutually DSR and DSDV and reaps both benefits [30]. They devised a method based on the CBDS. The three steps of CBDS′ black hole detection are bait, counter trace, and responsive defense. During the bait stage, the source node chooses one out of its neighbors at random and submits a bait request with that node's id. The RREP of the bait RREQ is used to construct a group of suspicious nodes in the reverse trace phase, after which the neighbor nodes translate to unrestrained mode to identify the presence of an assailant node within the path. A black hole alarm is broadcast to neighbor nodes for a piece black hole node found in the specific network. In reference [31], the proposed method relies on a specific type of node known as guard nodes, which aid in the detection of network black hole nodes. Guard nodes are promiscuous nodes that keep an eye on the activity of other devices in the system. The activity of the devices in the network is recorded in tables on guard nodes. Each network has a link quality that is calculated based on its network activity, and it drops because here the node is only the one which transmits no RREQ but only RREP. Few systems advanced to employ a trust-built methodology, in which apiece network device has trustworthiness that is established by the node's behavior. If the node's value is too less, it is classified as a node with black hole nature, as described in [32]. The disadvantage of this strategy is that the obtained parameter values are low and must be improved. The comparisons of existing methods are given in Table 1.

In [40], the authors suggested a trust-based multipath routing protocol called TBSMR to boost the MANET's overall performance. The key feature of the suggested protocol is that it incorporates numerous elements such as packet loss reduction, congestion management, secure data transfer, and malicious node identification to improve the MANET's QoS. The effectiveness of the suggested protocol is examined by the simulator in NS-2. Ensemble models based on machine learning were constructed [41]. While all of the attacks were labeled as anomalies and regular traffic, binary and multiclass classifications were performed on the KDD99 and NSLKDD datasets. Class designations included the five most common types of attacks: DoS probe, user-to-root, root-to-local, and normal. To predict the amount of vehicle crashes in a heavily trafficked challenging zone, researchers employ an artificial spider-monkey approach to probe sybil assault techniques on VANETs [42].

4. Proposed Approach

An MTBD algorithm is supposed to be transmitted to all CHs to tackle the sinkhole problem. However, before going into detail about the method, a variant of the routing protocols is provided to ensure disjoint routes: to ensure

Table 1: The comparison of existing methods.

Author	Contribution	Methodology	Advantage	Limitations
CBHDAP Vijayakumar and Somasundaram [33]	Sleuthing and circumventing black hole attacks in MANET	CBHDAP	Optimum results for throughput and detection probability	Does not work for security attacks
DSIDS Talukdar et al. [34]	BHAODV and DBHAODV protocols	IDS and digital signature	QoS, PDR, overhead is detected	Works well with a limited number of packets and nodes
FIDS Balan et al. [35]	Black hole node detection	NS-2 simulator	This approach is efficient than the normal AODV protocol	Limited to only one kind of attack, low jitter values
GABFO KanikaBawa [36]	Analysis of black hole attack	GA, BFO	Black hole attack effects are detected	Does not work with AODV protocols
NSABO Jaisankar et al. [37]	Finding a safe path between receiver and sender	Proposed framework with the NS-2 simulator	High packet delivery with less packet loss	Limited to two attacks
SAODV Dhende et al. [38]	Black, gray hole attack removal	SAODV, NS-2	Detection and prevention of malicious and selfish nodes	Works with only one protocol
TBBTD Yasin and Abu Zant [39]	Detection and isolation of black hole node	Timer-based baited technique	Throughput, PDR, and end-to-end delay are obtained	Throughput, PDR, and end-to-end delay need to be enhanced

discontinuous control message paths, AODV is changed as follows: after the source broadcasts the RREQ, each intermediary node that receives it adds its location to the requests and broadcasts it to its neighbors again. Until the author utilized the sink node, this procedure is repeated. As a response to the source node's request to deliver data over the selected paths, the sink node creates discontinuous paths.

The following is a description of the suggested attack recognition and protection system, MTBD:

Phase 1: the network is organized into clusters, with a CH for each cluster.

Phase 2: when the data Msg is available, the CH creates an RREQ as a cluster head. In the new version of the AODV protocol, the reply Msg comprises two distinct pathways to the sink node, as previously indicated. The CH transmits the data message over one of the receiving routes and generates the Ctrl message on the other. The sender ID, size, controlling route information, established written route, and checksum are all included in the Ctrl message.

Phase 3: after receiving the transmitted signal and both are said, the sink node begins comparing the control message to the received message. The sink node will determine if the highly considered has been altered or if it has not been changed by evaluating the control messages. Furthermore, if the sinkhole discards multiple emails, the sink node will notice when it receives control messages.

Phase 4: the sink node analyzes the histories of the same route to determine which CH is targeting the traffic because it records all of the routes.

Phase 5: if the sink node senses an incursion, it sends out an alarm to all of the CHs, warning them to stay away from the compromised one.

In Algorithm 1, there are supposed to be S nodes, a subset of a cluster head H, and one or more sink nodes SN. When a sensor sends the RREQ message to the CHj attached to it, it is prepared to submit its sensed data. Neighbor CHj transmits a message to its neighbors using the approach described in step 2 above. It sends an RREP message to si with an address to send after receiving the two disjoint pathways. CHj receives the message and sends the received message (data Msg) over one of the routes it received—send (Msg)—while also forming a Ctrl message to send through the other route send (Ctrl). Both data and control messages arrive at the sink node via distinct paths. The sink verifies the data it receives to the information in the Ctrl message. The sender ID, message size, packet information path, and checksum are all compared. The established written route is double-checked to ensure that it has not been tampered with and that the routes are disjoint. If the description in the Ctrl message does not match the data, the route and its history are reviewed. When a large amount of messages are sent to the same CH, it is referred to as a sinkhole node. The detailed flowchart for the proposed method is shown in Figure 3.

Following IDS′ disposal of status packets, all remaining nodes should receive them. A check should be done to determine whether packets have been dropped or not, and the right explanation for the dropped packets must be recognized. If a particular node drops whole packets, which is designated as a BH node, we must add it to the blacklist.

5. Experimental Setup

OPNET from Riverbed Technology is used to simulate the methods discussed in this work. OPNET supports state-of-the-art network simulation support with a huge stack of inbuilt network node types, protocols, and topologies. The

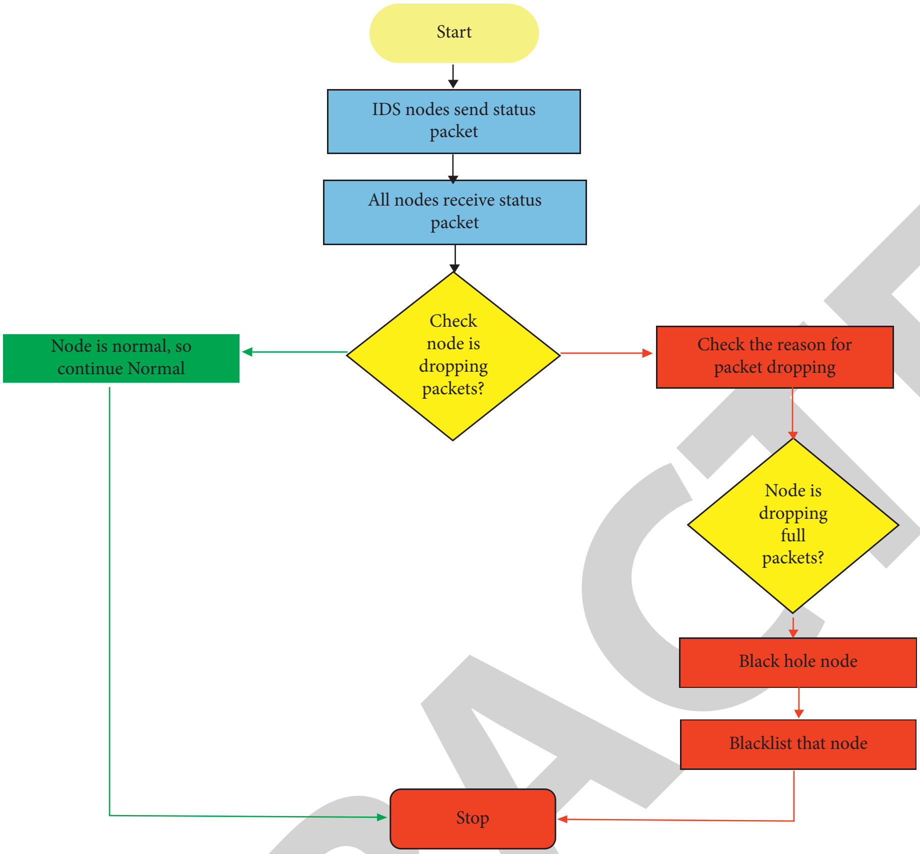
Start
IDS nodes send status packet
All nodes receive status packet
Check node is dropping packets?
Node is normal, so continue Normal
Check the reason for packet dropping
Node is dropping full packets?
Black hole node
Blacklist that node
Stop

Figure 3: Flowchart for the proposed method.

```
$s_1, s_{2,}, s_3, \ldots\ldots\ldots\ldots\ldots\ldots s_n \in S$
$sn_1, sn_{2,} sn_3, \ldots\ldots\ldots\ldots\ldots\ldots sn_n \in SN$
$CH_1, CH_2, CH_3, \ldots\ldots\ldots\ldots\ldots\ldots CH_1 \in H$
Repeat
   if ($CH_j$ ready to send)
sending device$_s$ $\longrightarrow^R$ $REQ$ Cluster Head$_j$
   ClusterHead$_j$ $\underset{RREQ}{\longrightarrow}^R$ $REQ$ Neighbour (Cluster Head$_j$)
   Cluster Head$_j$ $\leftarrow$ Neighbour (Cluster Head$_j$)
$S_i$ $\longrightarrow$ $^{\text{Pass information (Data)}}$ Cluster Head$_j$
      Send (message)
      Send (control)
   End if
$\forall Sn_i \in SN$
   Receive (Message (information))
   Receive (Message (Control))
      if ((compare (message (information), Message (control)) = true)
   Alert
   End if
   Until the transmission process is completed
End
```

Algorithm 1: Proposed MTBD algorithm.

freedom to design any kind of protocols and network architecture is provided by the scripting provision and graphical interface of OPNET. OPNET allows user to script user-defined network components, protocols, and architectures using C++. Visual Studio IDE is used to develop a dedicated user interface to load the input scripts to OPNET and to present results received from OPNET. Table 2 shows simulations parameters considered for study.

Table 2: Simulation parameters.

S. no.	Entity	Details
1	Frequency band	Mixed mode 2G, 3G, 4G, and VoLTE
2	RF range	Based on the type of 100 to 1000 meters
3	Network density	Typical real world
4	No. of nodes	100 to 1000 in steps of 100
5	No. of routers	Automatic selection
6	Node placement	Random distribution
7	Node types	Typical MANET nodes
8	Simulation area	10000 sq. meters
9	Simulation time	168 real-world hours

Table 3: Throughput.

	Parameter: throughput (kbps)						
Nodes	FIDS [34]	CBHDAP [32]	GABFO [35]	DSIDS [33]	TBBTBD [38]	NSABO [36]	MTBD [proposed method]
100	1200235	3498826	3996522	3149617	3660561	999622	3800366
200	1199316	3473081	3932599	3110567	3634051	974376	3792175
300	1198934	3441395	3859589	3068492	3606896	944088	3782606
400	1197893	3406603	3774152	3017808	3572176	908121	3769580
500	1197117	3366522	3678542	2962879	3534194	868428	3756476
600	1192534	3324746	3570724	2899399	3491403	821793	3742181
700	1192253	3274350	3451660	2826766	3446190	774666	3726018
800	1188402	3220755	3321135	2750391	3393795	719839	3708827
900	1185600	3161586	3178877	2669088	3339483	662409	3691235
1000	1181402	3096771	3024765	2577946	3280624	596816	3670213

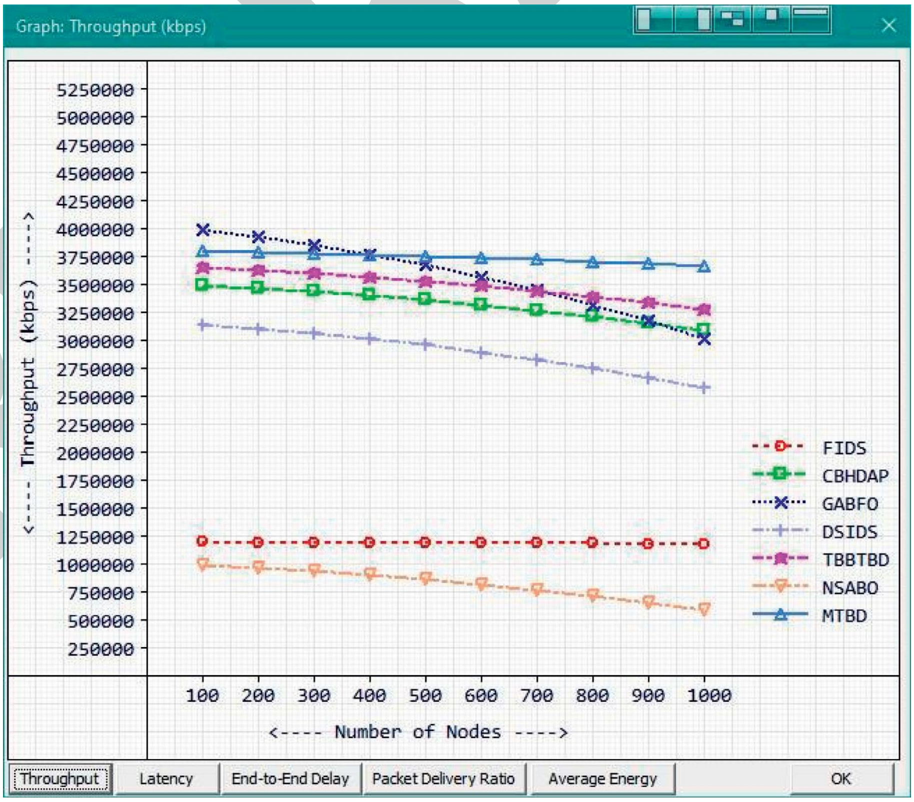

Figure 4: Throughput graph for various methods.

Table 4: Latency.

	Parameter: latency (ms)						
Nodes	FIDS [34]	CBHDAP [32]	GABFO [35]	DSIDS [33]	TBBTBD [38]	NSABO [36]	MTBD [proposed method]
100	250	222	171	230	220	202	190
200	250	221	178	233	221	205	194
300	252	223	186	235	223	205	196
400	253	225	193	234	222	207	196
500	253	223	199	236	223	209	196
600	254	224	209	238	226	213	201
700	254	227	216	237	226	213	202
800	257	225	221	241	227	217	201
900	255	227	231	240	226	219	203
1000	259	228	238	243	227	219	205

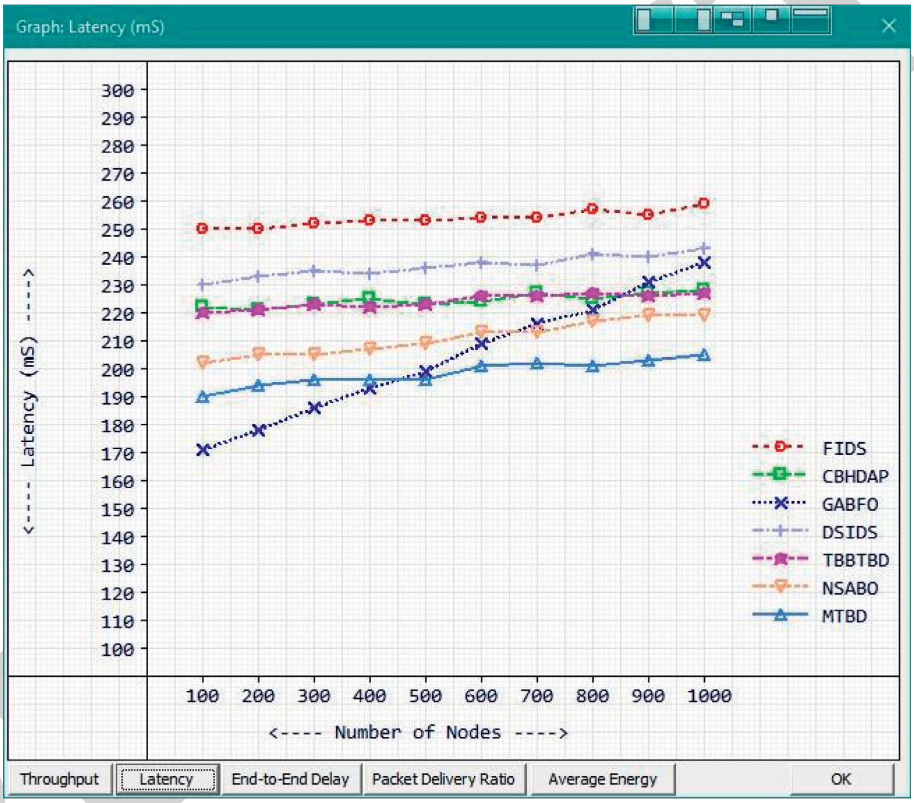

Figure 5: Latency.

6. Experiment Results

To show the importance of proposed method, the following parameters were considered as throughput, latency, packet delivery ratio, and average energy.

Throughput: the pace of data flow for a specific communication channel is referred to as throughput. During environmental monitoring, throughput is a critical aspect that necessitates constant data collecting. The higher the throughput quality, the greater the value of the network in question. The observed throughput values obtained from the regression results are presented in Table 3. The throughputs of different networks are shown in Figure 4.

Latency: it is a measure of reaction time; a shorter response time indicates better network quality. The latency numbers produced concerning different times for comparing techniques with simulation results are shown in Table 4 and Figure 5. Network performance is inversely proportional to latency. Milliseconds are used to measure it (ms).

End-to-End Delay: it is the sum of all latency issues, such as jitter, system postponement, and IP delay. It is taken into account how long it takes a data packet to move from source to destination. The worse the network traffic, the shorter the packet delay time. By established approach, Table 5 illustrates several end-to-end delay times. The end-to-end delays of different networks are shown in Table 5 and Figure 6.

Table 5: End-to-end delay.

	Parameter: E2ED (ms)						
Nodes	FIDS [34]	CBHDAP [32]	GABFO [35]	DSIDS [33]	TBBTBD [38]	NSABO [36]	MTBD [proposed method]
100	418	378	326	391	338	283	258
200	418	380	338	400	342	280	265
300	424	384	339	399	346	284	259
400	429	386	356	397	353	290	265
500	433	389	360	400	352	294	265
600	434	399	373	402	357	300	264
700	439	394	379	407	357	297	271
800	437	404	386	413	368	301	270
900	438	407	398	410	371	306	274
1000	442	408	406	417	373	304	276

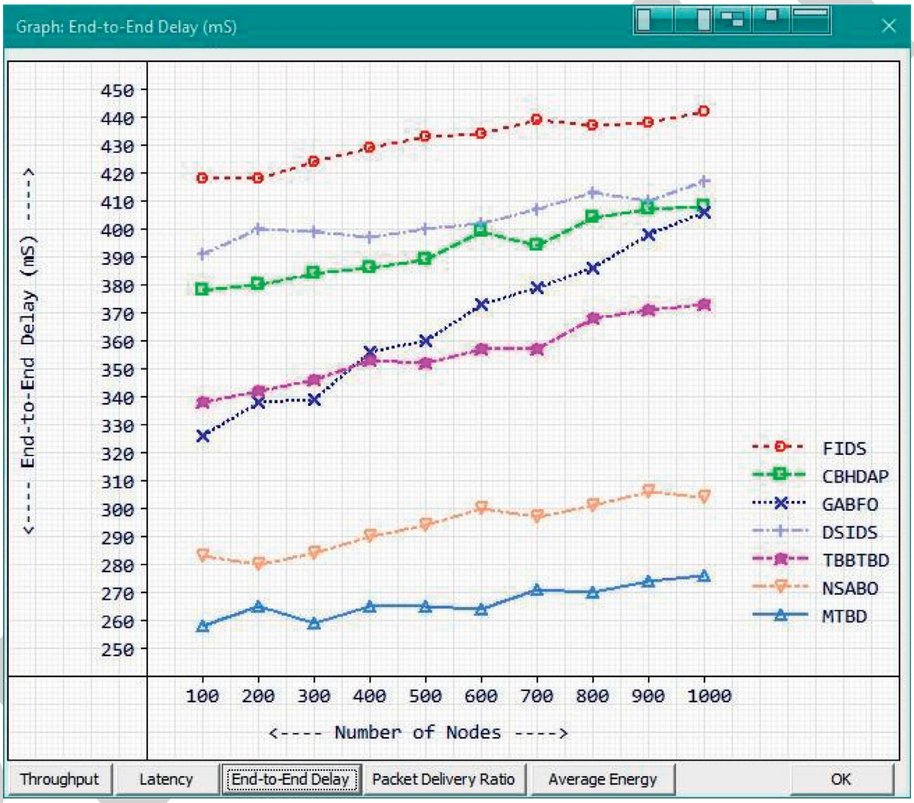

Figure 6: End-to-end delay graph.

Table 6: Packet delivery ratio.

	Parameter: PDR (%)						
Nodes	FIDS [34]	CBHDAP [32]	GABFO [35]	DSIDS [33]	TBBTBD [38]	NSABO [36]	MTBD [proposed method]
100	90	94	90	90	95	87	98
200	89	93	90	88	94	85	96
300	89	92	89	87	94	84	96
400	87	92	87	86	93	84	94
500	87	90	87	86	92	82	94
600	85	90	86	85	91	81	92
700	84	90	85	84	89	81	92
800	84	88	83	83	88	80	91
900	82	87	83	82	88	79	90
1000	82	86	82	81	87	78	89

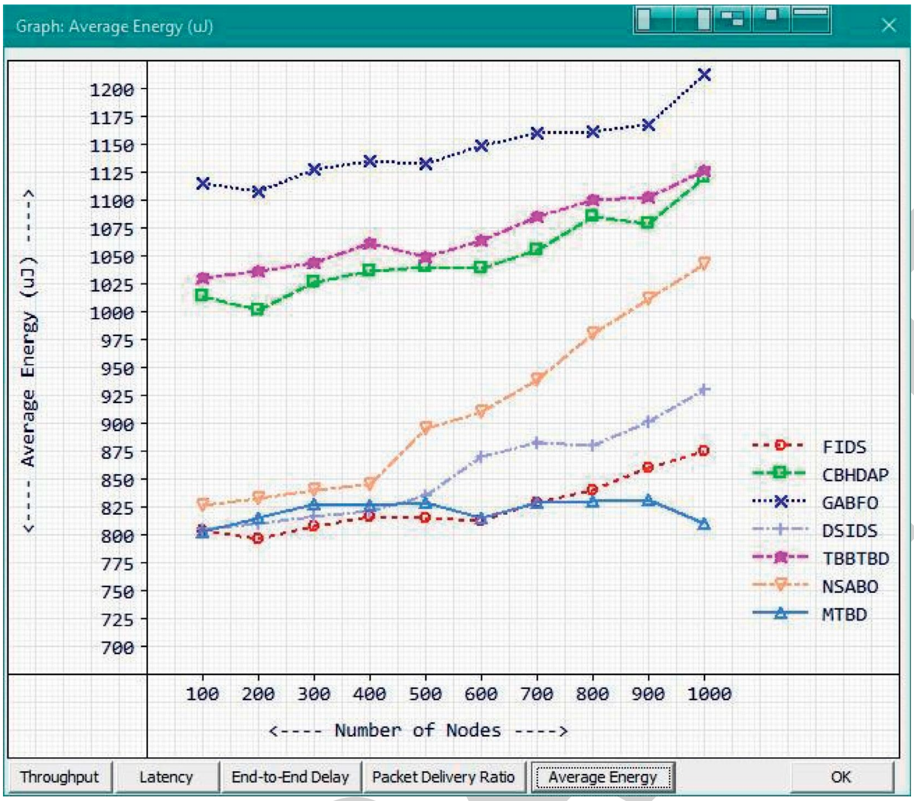

Figure 7: PDR.

Table 7: Average energy.

			Parameter: avg. energy (μJ)				
Nodes	FIDS [34]	CBHDAP [32]	GABFO [35]	DSIDS [33]	TBBTBD [38]	NSABO [36]	MTBD [proposed method]
100	804	1014	1116	806	1031	827	803
200	797	1002	1108	810	1037	833	815
300	808	1027	1128	817	1044	840	828
400	817	1037	1136	822	1062	845	827
500	816	1040	1133	835	1049	895	829
600	813	1039	1149	871	1064	910	815
700	829	1055	1160	883	1086	939	829
800	841	1086	1162	881	1101	981	830
900	860	1079	1168	902	1103	1012	832
1000	875	1120	1213	931	1127	1043	811

Packet Delivery Ration (PDR): it is measured as the sum of the mass of packets sent from the sources to the number of packets received at the destination; larger values indicate less data loss, implying a network design with a robust architecture. The packet delivery ratio values are presented in Table 6 and Figure 7.

Average Energy: it specifies how much energy the proposed method uses to get the outcomes in the

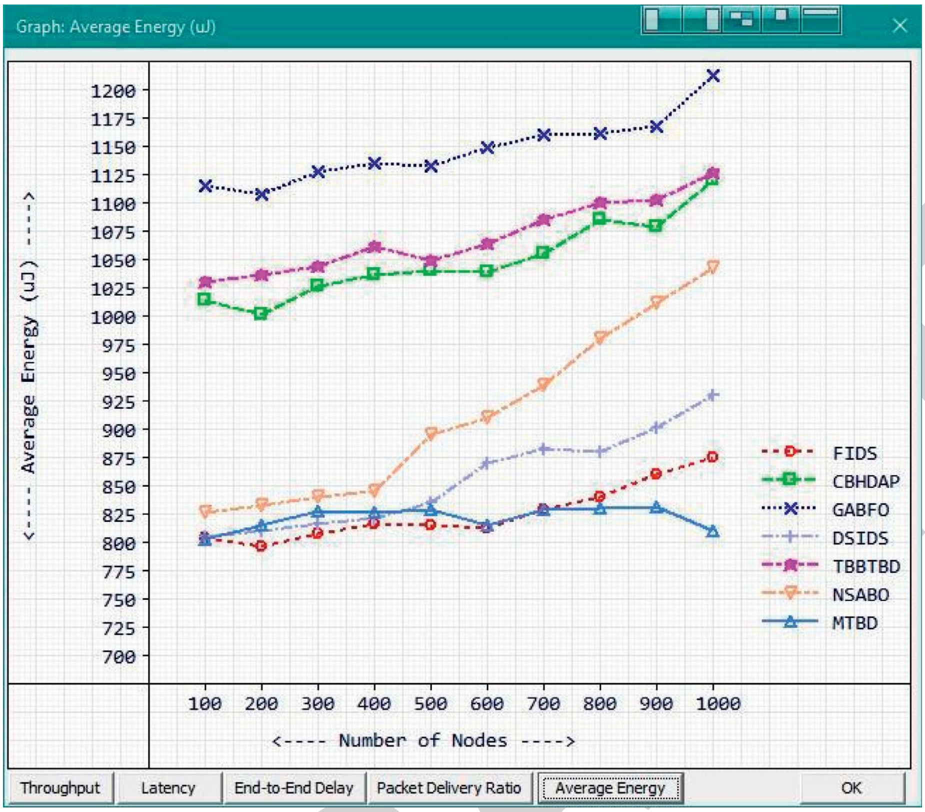

FIGURE 8: Average energy.

simulated environment. The system's effectiveness will increase as the amount of energy spent decreases. The average energy values are presented in Table 7 and Figure 8.

7. Conclusion

The black hole attack is regarded as one of the most dangerous threats to MANET's operations. Detecting and isolating any network black hole nodes is considered a critical task for preventing network collapse. We developed a smart black hole identification technique in this study, which should be taken into account while designing and emerging any black hole combat protocols or practices. Block-hole detection of the proposed method is improved. It is measured based on the parameters like throughput, end-to-end delay, latency, packet delivery ratio, and average energy. The proposed MTBT incorporates both timers and baiting approaches. The obtained average values of all the considered parameters are throughput (3743967.7 kbs), end-to-end delay (266.7 ms), latency (198.4 ms), packet delivery ratio (93.2%), and average energy (821.9 μJ). The suggested technique's simulation results show that the end-to-end delay, throughput, PDR, and average energy are far better than existing state-of-the-art approaches. In the future, we intend to develop the proposed model to enhance throughput and packet delivery ratio while reducing end-to-end delay and average energy consumption.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication.

References

[1] S. Mirza and S. Z. Bakshi, "Introduction to MANET," *International Research Journal of Engineering and Technology*, vol. 5, no. 1, pp. 17–20, 2018.

[2] V. Goyal and G. Arora, "Review paper on security issues in mobile Adhoc networks," *International Research Journal of Advanced Engineering and Science*, vol. 2, no. 1, pp. 203–207, 2017.

[3] X. Lai, J. Xia, L. Fan, T. Q. Duong, and A. Nallanathan, "Outdated Access Point Selection for Mobile Edge Computing with Cochannel Interference," *IEEE Transactions on Vehicular Technology*, vol. 71, pp. 7445–7455, 2022.

[4] J. Lu, L. Chen, J. Xia et al., "Analytical offloading design for mobile edge computing-based smart internet of vehicle," *EURASIP Journal on Applied Signal Processing*, vol. 2022, no. 1, 44 pages, 2022.

[5] L. Zhang, W. Zhou, J. Xia et al., "DQN-based mobile edge computing for smart Internet of vehicle," *EURASIP Journal on Applied Signal Processing*, vol. 45, no. 1, 2022.

[6] L. Chen, R. Zhao, K. He, Z. Zhao, and L. Fan, "Intelligent Ubiquitous Computing for Future UAV-Enabled MEC Network Systems," *Cluster Comput*, vol. 25, pp. 2417–2427, 2021.

[7] S. Singh, A. Bhasin, and A. Kalia, "Capitulation of mitigation techniques of packet drop attacks in MANET to foreground nuances and ascertain trends," *International Journal of Communication Systems*, vol. 34, no. 10, Article ID e4822, 2021.

[8] D. Singh and A. Singh, "Enhanced secure trusted AODV (ESTA) protocol to mitigate blackhole attack in MobileAdHoc networks," *Future Internet*, vol. 7, no. 3, pp. 342–362.

[9] P. R. Dumne and A. Manjaramkar, "Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs," in *Proceedings of the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 486–490, Noida, India, September 2016.

[10] K. Vijaya Kumar and K. Somasundaram, "Study on reliable and secure routing protocols on manet," *Indian Journal of Science and Technology*, vol. 9, no. 14, pp. 1–10, 2016.

[11] M. Rajesh Babu and G. Usha, "A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET," *Wireless Personal Communications*, vol. 90, no. 2, pp. 831–845, 2016.

[12] K. Vijaya Kumar and K. Somasundaram, "Detection of black hole attacks in MANETs by using proximity set method," *International Journal of Computer Science and Information Security*, vol. 14, no. 3, pp. 136–145, 2016.

[13] S. K. Arora, S. Vijan, and G. S. Gaba, "Detection and analysis of black hole attack using IDS," *Indian Journal of Science and Technology*, vol. 9, no. 20, pp. 1–5, 2016.

[14] M. Z. Ibrahim and R. Hassan, "The implementation of Internet of Things using testbed in the UKMnet environment," *Asia-Pacific Journal of Information Technology & Multimedia*, vol. 08, no. 02, pp. 1–17, 2019.

[15] 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.

[16] 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.

[17] M. Singh, C. Kumar, and P. Nath, "Challenges and protocols for P2P applications in multi-hop wireless networks," in *Proceedings of the 2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 310–316, IEEE, February 2018.

[18] S. Kurosawa and A. Jamalipour, "Detecting blackhole attack on AODV- based mobile ad hoc networks by dynamic learning method," *International Journal on Network Security*, vol. 5, 2007.

[19] Yu Wang, "Using Fuzzy Expert System Based on Genetic Algorithm for Intrusion Detection System," in *Proceedings of the 2009 International Forum on Information Technology and Applications*, Chengdu, China, April 2009.

[20] G. Xiaopeng and C. Wei, "A novel gray hole attack detection scheme for mobile ad hoc networks," in *Proceedings of IFIP International Conference on Network & Parallel Computing*, Dalian, China, September 2007.

[21] Y. Hu, Y. Perrig, and B. Johnson, "Rushing attack and defences in wireless Ad hoc networks routing protocols," in *Proceeding of the 2nd ACM workshop on Wireless Security*, New York, NY, USA, 2003.

[22] S. Ahmed and M.E. A. Shoukry, "A novel taxonomy of blackhole attack detection techniques in mobile ad-hoc network (MANET)," in *Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering*, pp. 346–352, IEEE, Sydney, Australia, December 2013.

[23] S. Sujatha, V. Dharmar, and R. S. Bhuvaneswaran, "Design of genetic algorithm-based IDS for MANET," in *Proceedings of the 2012 International Conference on Recent Trends in Information Technology*, pp. 28–33, IEEE, Chennai, India, April 2012.

[24] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," *International Journal on Network Security*, vol. 5, no. 3, pp. 338–346, 2007.

[25] V. Sankaranarayanan and L. Tamilselvan, "Prevention of blackhole attack in MANET," in *Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, IEEE, 2007.

[26] A. Tcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile Ad Hoc networks," in *Proceedings of the Radio and Wireless Conference: AWCON'03 Proceedings*, IEEE, Boston, MA, USA, August 2003.

[27] V. Mohan, "Pawar and J. Anuradha, "Network security and types of attacks in network," *Procedia Computer Science*, vol. 48, pp. 503–506, 2015.

[28] SapnaGambhir and S. Sharma, "PPN: prime product number based malicious node detection scheme for MANETs," in *Proceedings of the 3rd International Advance Computing Conference (IACC)*, IEEE, 2013.

[29] A. K. S. Ali and U. V. Kulkarni, "Comparing and analyzing reactive routing protocols (aodv, dsr and tora) in QoS of manet," *IACC*, in *Proceedings of the 7th IEEE International Advanced Computing Conference*, pp. 345–348, Hyderabad, India, 2017.

[30] M. Sathya and M. Priyadharshini, "Detection and removal of black hole attack in mobile ad-hoc networks using cooperative bait detection method scheme," *International Journal of Scientifc& Engineering Research*, vol. 7, no. 3, pp. 81–85, 2016.

[31] A. R. Rajeswari, K. Kulothungan, and A. Kannan, "GNBAODV: guard node based –aodv to mitigate black hole attack in MANET," *International Journal of Scientifc Research in Science, Engineering and Technology*, vol. 2, no. 6, pp. 671–677, 2016.

[32] A. Jain, U. Prajapati, and P. Chouhan, "Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario," in *Proceedings of the 2016 Symposium on Colossal Data Analysis and Networking*, CDAN 2016, Indore, India, March 2016.

[33] K. Vijayakumar and K. Somasundaram, "An effective CBHDAP protocol for black hole attack detection in manet," *Indian Journal of Science and Technology*, vol. 9, no. 36, 2016.

[34] M. I. Talukdar, R. Hassan, M. S. Hossen, K. Ahmad, F. Qamar, and A. S. Ahmed, "Performance improvements of AODV by black hole attack detection using IDS and digital signature," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6693316, 13 pages, 2021.

[35] E. V. Balan, M. K. Priyan, C. Gokulnath, and G. U. Devi, "Fuzzy based intrusion detection systems in MANET," *Procedia Computer Science*, vol. 50, pp. 109–114, 2015.

[36] Kanikabawa, “Prevention of black hole attack in MANET using addition of genetic algorithm to bacterial foraging optimization,” *International Journal of Current Engineering and Technology*, vol. 5, no. No.4 (Aug-2015, pp. 2406–2411.

[37] N. Jaisankar, R. Saravanan, and K. D. Swamy, “A novel security approach for detecting black hole attack in MANET,” in *Proceedings of the International Conference on Business Administration and Information Processing*, pp. 217–223, Springer, Trivandrum, India, March 2010.

[38] S. Dhende, S. Musale, S. Shirbahadurkar, and A. Najan, “SAODV: Black hole and gray hole attack detection protocol in MANETs. 2017 international conference on wireless Communications,” in *Proceeding of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 2391–2394, IEEE, Chennai, India, March 2017.

[39] A. Yasin and M. Abu Zant, “Detecting and isolating blackhole attacks in MANET using timer based baited technique,” *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9812135, 10 pages, 2018.

[40] M. Sirajuddin, Ch. Rupa, C. Iwendi, and CresantusBiamba, *TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network, Security and Communication Networks*, vol. 2021, Article ID 5521713, 9 pages, 2021.

[41] C. Iwendi, S. Khan, J. H. Anajemba, M. Mittal, M. Alenezi, and M. Alazab, “The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems,” *Sensors*, vol. 20, no. 9, p. 2559, 2020.

[42] C. Iwendi, M. Uddin, J. A. Ansere, P. Nkurunziza, J. H. Anajemba, and A. K. Bashir, “On detection of Sybil attack in large-scale VANETs using spider-monkey technique,” *IEEE Access*, vol. 6, pp. 47258–47267, 2018.