Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.027719
Article

Tech Science Press

Timer Entrenched Baited Scheme to Locate and Remove Attacks in MANET

S. Padmapriya[1], R. Shankar[2], R. Thiagarajan[1,*], N. Partheeban[3], A. Daniel[3] and S. Arun[4]

[1]Department of Computing Science and Engineering, Prathyusha Engineering College, Thiruvallur, 602025, India
[2]Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engg. College, 500097, Telangana, India
[3]School of Computing Science and Engineering, Galgotias University, Greater Noida, 203201, India
[4]Department of Electronics and Communication Engineering, Prathyusha Engineering College, Thiruvallur, 602025, India
*Corresponding Author: R. Thiagarajan. Email: thiagarajanpit@gmail.com

Received: 24 January 2022; Accepted: 01 March 2022

Abstract: The Mobile Ad-hoc Network (MANET) is a dynamic topology that provides a variety of executions in various disciplines. The most sticky topic in organizational fields was MANET protection. MANET is helpless against various threats that affect its usability and accessibility. The dark opening assault is considered one of the most far-reaching dynamic assaults that deteriorate the organization's execution and reliability by dropping all approaching packages via the noxious node. The Dark Opening Node aims to deceive any node in the company that wishes to connect to another node by pretending to get the most delicate ability to support the target node. Ad-hoc On-demand Distance Vector (AODV) is a responsive steering convention with no corporate techniques to locate and destroy the dark opening center. We improved AODV by incorporating a novel compact method for detecting and isolating lonely and collaborative black-hole threats that utilize clocks and baits. The recommended method allows MANET nodes to discover and segregate black-hole network nodes over dynamic changes in the network topology. We implement the suggested method's performance with the help of Network Simulator (NS)-3 simulation models. Furthermore, the proposed approach comes exceptionally near to the original AODV, absent black holes in terms of bandwidth, end-to-end latency, error rate, and delivery ratio.

Keywords: Mobile ad-hoc network (MANET); wireless ad hoc network; ADOV; attacks; denial of service

1 Introduction

Remote correspondence organization can confine by a focal framework that controls correspondence between nodes or a simple framework known as Ad-hoc Networks. The MANET is a wireless ad hoc network variation that links portable nodes. Nodes in a MANET do not depend on a single point to facilitate communication or flow between them; instead, they work together to communicate information among nodes that cannot contact each other directly. Overall, nodes can bridge the originator and the collector node whenever the sender and beneficiary do not share the same inclusion. Because of the nodes' adaptability, the organization's geography evolves uniquely.

The MANET guiding conventions are structured to be flexible for any specific shifts in geography [1–4]. Energy from MANET is also the main network factor. Every node in the organization has a limited sum of energy; accordingly, we should use appropriate components and conventions that evade excessive energy utilization. MANET connects nodes via a distant connection, and data transfer capacity is a vital network characteristic. Remote connections have a substantially lower data transfer capability than connected connections. A clamor, obstruction from another sign, or blurring can influence a remote connections sign [5]. Because MANET lacks a central framework to manage node-to-node communication, nodes must rely on one another to provide data to the target node. As a result, a hostile aggressor node can break the association connection or ignore the information transmitted.

Because nodes in MANET may link and disconnect fast, the channel's topology is unpredictable. This channel's dynamic architecture makes it vulnerable to a variety of threats. As a result, building such a system and improving path stability will be extremely difficult. MANET is always undertaking a variety of vicious assaults, but we focus on black hole attacks. Medical organizations require round-the-clock monitoring, including routine upgrades and emergency information streaming through the channel. However, the primary concern discovered within those locations is the malicious nodes occurring, causing unnecessary waits and perhaps hazardous outcomes. In addition, it contributes to the occurrence of congestion and communication delays. In a black hole attack, the malicious nodes pose as if they know the fastest path to the end node. In this strategy, a fake path creates through the suspect's node and diverts all traffic to that suspect's node.

Consequently, although messages to the identified address, complete payloads are occupied in the meanwhile, potentially slipping it through malicious nodes. The Timer Based Baited Technique (TBBT) employs both clocks and a bait mechanism to discover and disconnect black hole nodes in a MANET. This technique increases black-hole exposing capability. The strategy of fake identity bait is used in this method to find black-hole network nodes. On the other hand, this method dramatically improves latency while reducing performance. The Counter and Timer-based Baited Method (CTBM) for Isolating Black Hole Threats in MANET are present to deal with these issues. This method has three operations: bait message, quasi reply, and timer. All three factors distinguish the channel's Blackhole node.

In MANET, assaults classify as either dynamic or inactive. In dynamic assaults, assailant nodes influence MANET activity by excluding changing association joins, conveying information, and depleting the nodes. The attacking nodes only snoop between nodes in uninvolved assaults that influence the associate operation [6]. This article coordinates in the following sequence: Segment 2 gives a foundation of the AODV directing convention and dark opening assault in MANET, Segment 3 looks at the connected efforts, Segment 4 introduces the suggested framework, and Segment 5 portrays the philosophy to test the suggested system. Segment 6 shows the consequences of the suggested system and correlation with some other suggested systems and the summarized outline in Segment 7.

2 Background

2.1 AODV

The authors picked AODV pointing pact in the given examination because it has a superior presentation quality than responsive directing conventions. Under various execution measurements as indicated by [7], AODV is superior to other responsive steering conventions. Because it consolidates the methods of both Dynamic Source Routing (DSR), steering convention and Destination Sequenced Distance Vector (DSDV) obtains the two focal points. Two kinds of control packages, called route require (RREQ) and route response (RREP), is required to communicate between two nodes using AODV. RREQ is communicated to nearby nodes to approach them for a course to the wanted node; nodes continue sending RREQ until the objective node reaches. After accepting an RREP, the objective node receives the bundles sent by the source node. In [8], the receptive directing convention is present under various assaults.

2.2 Black-Hole Attack

The functioning assault class the aggressor node asserts has a short course regardless of whether it does not. Consequently, all bundles will go through it, enabling the dark opening node to advance. Typical nodes accept counter to solicitations, and dark opening node acquires an advantage by responding to any request and claiming to have the shortest path to the ideal node. In most cases, nodes begin the revelation step to locate the ultimate node. When the originating node makes a query towards the goal node, each node that receives it checks to see if it has a new path to the goal node. The source node begins sending parcels to the dark opening node to deliver the parcels to the goal node; however, the dark opening node leaves out the supplied bundles. The dark opening assaults will classify into two types: single and pleasant dark opening assaults.

A solitary dark opening is a single attacker node, but an agreeable dark opening assault has a group of assailant nodes collaborating [9–12] to corrupt the organization's unwavering quality. Furthermore, the black-hole attack node discards every delivered packet, preventing interaction between the source and the target node.

2.3 Problem Description

To avoid the harm that can cause by various threats, the protection of MANET is crucial. The dark opening assault is the famous assault that hurt the organization and expects to forestall any association. The AODV steering convention seeks to identify the quickest route between these two nodes, which must be communicated in the organization when the way is needed. Unfortunately, the AODV convention does not provide a calculation that makes a difference in distinguishing and forestalling the dark opening assault. This article intends to improve the AODV directing convention with a compact method to distinguish the dark opening assault and forestall its damage to the organization.

3 Related Work

In this segment, we will portray the created methods, particularly teasing procedures against dark opening assaults in receptive directing convention, the restrictions of each method, and how brilliant dark opening assault may defeat the created method. Regarding savvy dark opening assault, we imply that the aggressor node knows the pre-owned method, and it can utilize the entirety of its highlights against the other MANET nodes. Khan et al. [10] discuss using the Ant Colony Optimization (ACO) Method and Repetitive Routing Setup utilizing Reactive Routing in MANETs to prevent Black Hole Attacks. The above analysis revealed that employing ACO alongside Reactive Routing Protocol resulted in increased effective performance and improved protection of Black Hole Attacks, with a 10% increase overall performance and a 27% reduction in network congestion over Minimal Cost Route System.

In [13], the created teasing procedure relies on the lead to individual node id. The discovery of a dark opening node embarks on broadcasting a trap solicitation to each adjacent node. The snare request includes the source sequence number (SSN) and the source id. When a response has a higher destination sequence number (DSN), the source node scans. After the location of the organization's dark opening node, the source node communicates a dark opening caution to all adjacent nodes to inform them. The limits of this process are that a brilliant dark opening node can check if those acquired RREQ requests have a path to an equivalent wellspring of such RREQ, and if they do, it simply does not answer that need. Dark opening nodes can also use the dark opening warning to issue fraudulent dark opening alerts.

They developed a [14–16] that relies on the Cooperative Bait Detection Technique method. First, an overview of the dubious nodes from the RREP of the snare RREQ in the Reverse Trace stage; at that point, the neighboring nodes join the wanton mode to identify an aggressor node in the way. Next, a dark opening caution transmits to neighboring nodes for each dark opening node identified in the organization.

Finally, the source node in the Reactive Defense stage scans to see if Packet Delivery Ratio (PDR) seems weaker than a chosen edge. If so, it restarts the Bait stage.

In [17], the created conspire utilizes a fake id to trap a dark opening node. Owing to its regular manner that reacts to every RREQ in the organization, soothing it has the best itinerary, the dark opening node will respond to that trap RREQ. In DSR, the generated conspire executes the RREQ RREP header changes. Source node continues checking if there are abatement; it begins the baiting once more. The obstacles to this plan would be that it creates the shape of systems packages (RREQ and RREP), which causes the overhead to rise in expansion to the dark opening cautions that disconnect nodes in the organization by a shrewd dark opening.

In [18], the suggested framework begins by overflowing the organization with a bogus demand. Such a node response is a dubious node by verifying whether the dubious node is transferring parcels to the target. As this system can use in the military, the suggested framework has a restriction framework that provides the dark opening node situation. The limitation of this system is that it feeds a false request to the network, which can prompt clogging in the organization. In [19], the suggested framework relies upon an uncommon kind of nodes called monitor nodes, which help distinguish dark opening nodes in the organization. Gatekeeper nodes check the behavior of nodes in the organization. Each node appears to have a level of confidence reflected through its behavior within the organization, and when the node only transmits RREP, its level of confidence drops, and it does not send RREQ. If a node's trust assessment falls below a certain threshold, it is obstructed or separated at that time. When a dark opening node is recognized, gatekeeper nodes broadcast a caution to all nearby nodes.

It was agreed in this system [20] that the assailant node is unaware of the chomped legitimacy that must send after transferring the RREP. This system impedes the irrational assumption that any assailant node required to assault an organization would also utilize a related convention and evaluate before the assaulting. The suggested system recognizes black-hole and dim opening nodes dependent on the adjacent node's feeling. The Statistical AODV nodes include dual neighbor list (NL) tables containing neighbor nodes ids and reaction lists (RL) used to describe nodes that rely on their organization exercises. When the source node receives an answer, it sends an appraisal message to neighbors. This node is a dark opening node at that point, on the off chance that all nodes reacted with NO message, assuming that some nodes replied YES and the residue with a NO. Disclosing the warning messages to the firm when identifying a dark node. Exchanged messages in the reserved room for RL tables and overhead in the assessment, the constraints of this method are high overhead; even though brilliant dark opening nodes will give a bogus feeling when they list for what enables them to disconnect ordinary nodes.

In [21], the recommended framework utilizes produced requesting to recognize dull opening centers in the association. Source starts by communicating a made requesting in the association; any center response to the spurred interest considers a dim opening center point. Source center point stores the typical DSN found solutions of the spurred interest. In this framework, the source center imparts a sale to the ideal center point. The target center considered is a dim opening center point; regardless, the center is customary. We will, in like manner, contrast our framework and the suggested framework in [22].

A few frameworks and fragments execute in AODV and DSR, which utilizes to perceive, furthermore, disengage the faint opening community in MANET [23]. Sections of the executed system rely on neighbor communities to pick the direction of various focuses, called Watchdog methods. In this method, focus focuses are in an unbridled mode. They begin to tune in and guarantee that diverse focus focuses are sending packs; consequently, focuses can pick whether there is a faint opening place point that does not propel groups to various neighbors as in [24]. Likewise, a segment of the used systems uses a false package as bait to perceive dull opening centers in the association. In batting methodology, centers send a sale for a non-existing center point in the association and hold on for a response. Since dim opening center point constantly responds in due order regarding any request, vague opening center point answers for the sales of the fake center. After scrutinizing and seeing the upsetting methods used in MANET to recognize the dim opening center in the association, we shut three prodding methodologies that differ from other methods [25].

4 System Model

The proposed method limits impressive dark opening assaults by employing tickers and encouraging messaging, as shown in Fig. 1. Subordinate to the typical lead of a faint opening community, once it draws the request for a course, it answers by certifying it would have the effective techniques if not available. Whenever the soft opening draws the snare demand, it responds towards the origin place point, confirming that it does have a course. When the origin community comes up with a solution, It evaluates the center point right away that reacted as a soft opening and adds it to the faint opening outline because it declared to have a course to a phony community point.

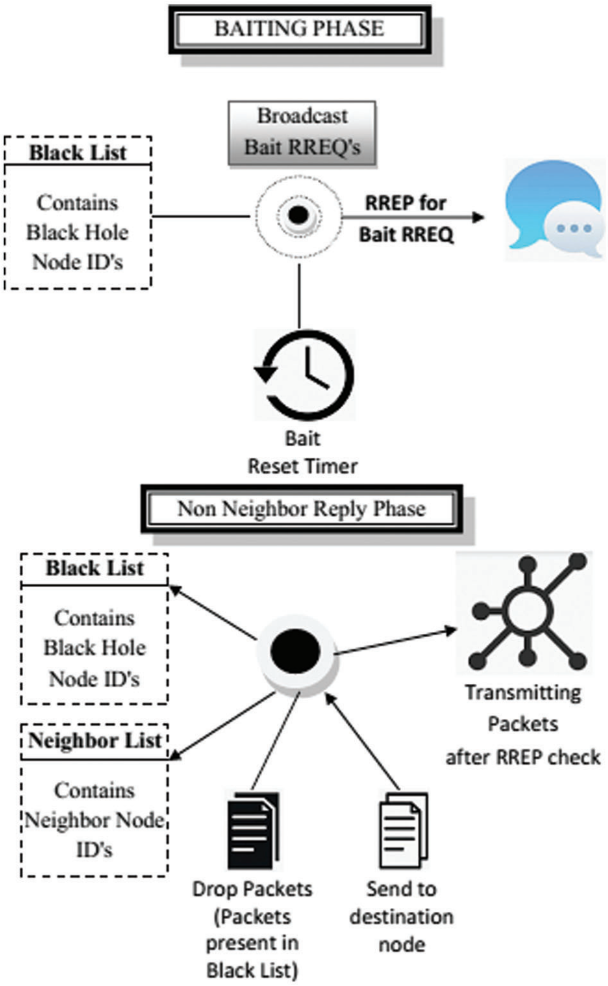
BAITING PHASE
Broadcast Bait RREQ's
Black List
Contains Black Hole Node ID's
RREP for Bait RREQ
Bait Reset Timer
Non Neighbor Reply Phase
Black List
Contains Black Hole Node ID's
Neighbor List
Contains Neighbor Node ID's
Transmitting Packets after RREP check
Drop Packets (Packets present in Black List)
Send to destination node

Figure 1: System model

The Time-To-Live (TTL) assessment is to help people take the essential steps to avoid destroying the association with counterfeit transactions in the catch interest. In the non-neighbor answer stage, each center knows its proximity to focus by the righteousness of the welcome message broadcasting measure. Discovering a clueless opening rundown the source community validates its identity of such node with the lightest path (NWLP). If NWLP is not a neighboring location, its origin place point ignores the reaction to prevent possible correlation between dim focuses. Our approach assigns a self-ID and segment to every dull opening point, enabling openness between MANET focal points. The recommended approach is not to use the dull opening alarm to prevent any uncommon faint opening point from employing this section by sending false alerts. To avoid blocking any connection with requests and responses, we set the snare interest's TTL to one. This mediation across both fake id and catch clock would keep the boring opening community detecting all manual counters along the road. Not utilizing the overhead and one-of-a-kind gatherings makes it a lightweight strategy course. When the source center point discovers the solution, it instantly considers the center point, which answers as a dim opening and adds it to the dim opening overview since it requires a route to a fake.

As seen in Fig. 2, each center point sends a hello message to its neighboring center points. Each center point in the Baiting stage creates a catch interest with a TTL and self-assertive fake id close to 1. It then distributes sales to all of its contiguous centers; the bait would pique the interest of the uninteresting opening centers BH1 and BH2. Adding the uninteresting opening would get center point BH1 if Nodes (N) N4, N6, and N7. Since center point BH1 reacted in due order to each bait from N4, N6, and N7 based on the usual direction of the dark opening center point, it responds to each request whether or not it has a current path for the ideal center point. Centre points N2, N3, N8, and N10 will include BH2 in their dim opening once-over since center BH2 answered in appropriate sequence to each trap request that originated from N2, N3, N8, and N10. All centers reset the drawing clock with an abnormally Bait (B) sec, and when Source (Sr) asks to interact alongside Destination (Dt) at the center, it sends RREQ. Center N4 sends RREP to ensure it would have the optimal route; center Sr checks to see whether center N4 is in its neighbor list or not. If center N4 is in center S's consideration, center N4 is in the neighbor neglects, and Data is transferred from center Sr to Dt via N4. Algorithms 1 and 2 illustrate the counts of the recommended strategies, respectively.

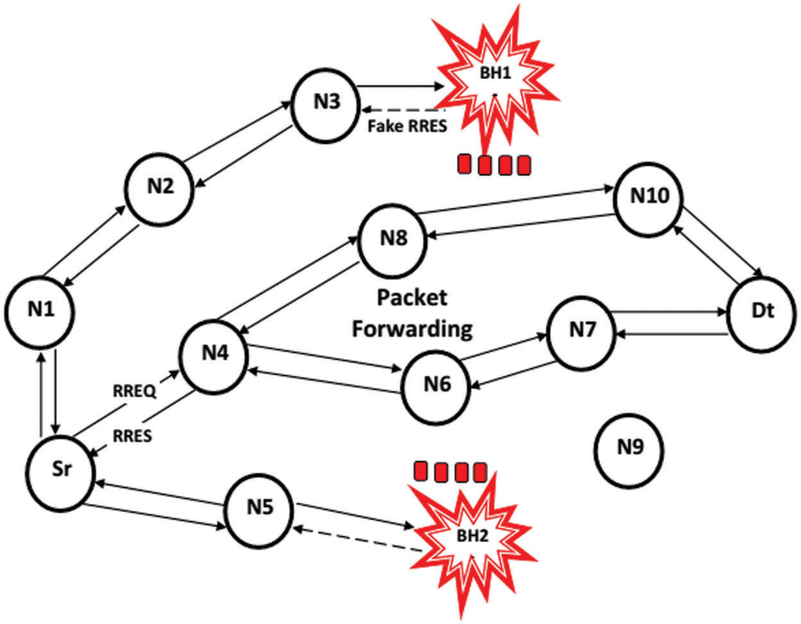

Figure 2: Outline of baiting request and black-holes (BH)

5 Procedure Followed

The reconstruction process uses the NS-3 evaluation method to validate the correctness of the proposed procedure Timer Entrenched Baited Scheme (TEBS). We used the CMU tool to generate the circumstances, using the CMU instrument to make the activities and location of centers self-assertive. We put the personal circumstances of both the source and goal centers. The dull opening center point was the initial position in the organization. We set the 1000x1000 meter association coordination. Center transmission reaches 150, group size to 512 bytes, center points maximum speed to 15 meters per second, entertainment time to 200 s, implying that center points will travel between 0 and 15 at average speed, and defer time to 5 s. Finally, we do everything possible to avoid using Transmission Control Protocol (TCP) as a vehicle display. TCP contains figures that attempt to preserve a crucial good route out of the association obstacle. They may impact the introduction estimations outcomes as we try to execute our demonstration, not the group streams in the association. We provide information regarding the atmosphere's limits. We divided the introduction of neighborhood AODV and TEBS-AODV under dim opening assault into three execution figures, Throughput, Packet Transmission Proportion, and End-to-End Delay, which are the most impacted limits in AODV under dim opening attack, as demonstrated by [26]. We used AWK substance to examine the follow-up record. Throughput shows the proportion of data collected from the source center at the target center point over the maximum transmission time [27–30].

Algorithm 1: Baiting Phase Methodology

```
Source Node
If CT==BT then
    Create B.request;
    Create a unique ID and save it in B.request;
    Set B.request's TTL to I;
    Broadcast B.request;
    Reset BT to a RT;
    End if
For each B.request response received do
In BH list L, save NWLP ID
End for
```

It uses the unit kilobits (kbps) to measure the Throughput. Therefore, it implies using the Eq. (1).

$$T = \frac{P_r}{C_t} * \frac{8}{1024} \tag{1}$$

In which T belongs to Throughput. Pr is the place point. Ct is the time difference seen among sending and receiving communities. Common End-to-End (E2E) Delay represents moving from the originating location to the target community. Using millisecond units to calculate the End-to-End Delay [31]. It will, by and large, be a delight utilizing condition (2).

$$D_{E2E} = \sum_{i-1}^{k} Rt_i - \frac{St_i}{k} \tag{2}$$

In which D_{E2E} denotes regular E2E Delay. Rt_i defines the getting period of the gatherings at focus point I. St_i denotes the send time of packs at focus point I. n denotes the amount of focus in the affiliation. Bundle conveyance Ratio shows the degree of packs that effectively gets the objective place to bunch sent from the starting community point [32]. It will, as a rule, is readied utilizing condition (3).

$$PDR = \frac{P_r}{P_s} \tag{3}$$

where P_r denotes the number of bundles received at the target node, P_s denotes the total number of bundles transmitted from the source node. PDR stands for Packet Delivery Ratio.

Algorithm 2: Non-neighbour reply phase

```
Source Node
Broadcast a native AODV req. to the Dest. node;
for each response to the req. for a dest. node do
  if NWLP has been added to the B.list then
  Abandon reply;
  End if
  if NWLP not from Destination node && not in neighbor list then
  Abandon reply;
  else
  Carry on as a local AODV and begin sending packets to the D.N;
End if
End for
```

6 Results

The overall outcome of Throughput within neighborhood AODV indicates that there is no dim opening center point inside the organization was perhaps the most elevated. On the other hand, while watching the observations of TEBS, it was discovered that if there is a dull opening center point in the association, the performance gets higher than the neighboring AODV, but lower than the neighboring AODV as there is no dim opening center point.

The proposed TEBS's throughput improvement is due to rejecting every answer by obscure nodes that claim to provide a constrained path towards the goal node, resulting from a decrease in throughput, as illustrated in Fig. 3. The location of the dark opening node is essential since it can only locate in the most limited method between the source and the aim [33]. When there is a dim opening center point in the association, the outcome of End-to-End Delay inside neighborhood AODV was the most important, as illustrated in Fig. 4. Because of the AODV's duty in selecting the most straightforward technique, the outcome of Final Latency in nearby AODV was the most minimal. When there is no dull opening center point, the results of the TEBS study revealed a minor change in Final Delay. Outcomes were distinguishable from neighborhood AODV. An after effect of the way assurance segment in TEBS settles as before as in neighborhood AODV.

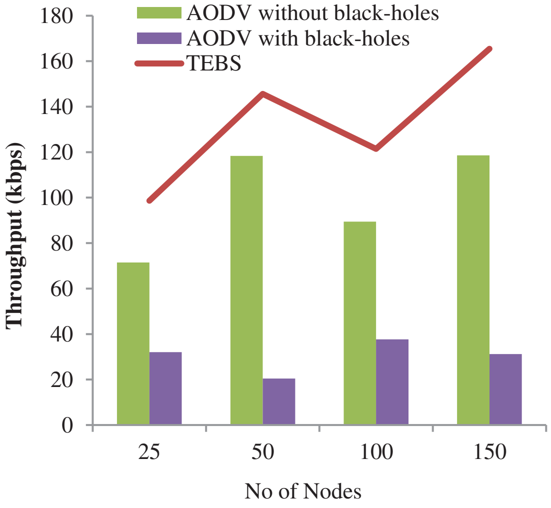

Figure 3: Number of nodes *vs.* throughput results

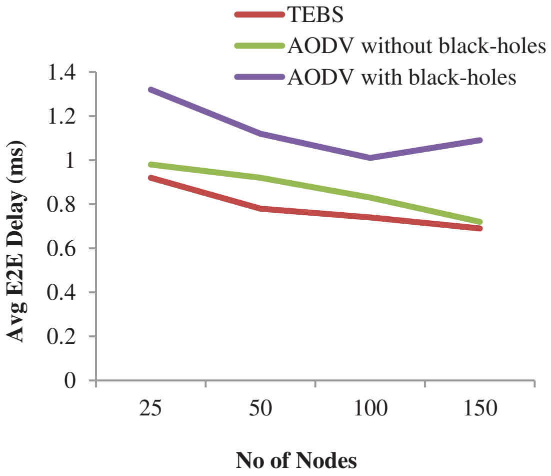

Figure 4: Average number of nodes *vs.* end-to-end delay results

The delayed result of PDR in the neighborhood AODV occurs, as shown in Fig. 5. A dull opening center point within the association is shallow, nearly zero because a dim opening center consistently intends to cut the relationship between any two center points that endeavor to confer within the association and endeavor to hold all packages between both of them. Depicting the outcome of energy consumption in Fig. 6. based on that. We can see that the current approach consumes significantly less energy.

The result of PDR in close AODV while the absence of dark opening center point in the relationship is the most critical. If we look at the results, we can see that TEBS has a higher PDR than neighboring AODV when the opening center point is dim. It is lower than neighborhood AODV as there is no dull opening center point in the association. The PDR upgrade of suggested TEBS excludes any answer from such an obscure node, which reduces PDR. The dark opening node's position is significant. The direct distance between the source node S and the destination Dt. Tab. 1 depicts the effects of E2E Delay, PDR, Throughput, and Energy utilization as the number of nodes grows. We then simulate the above result in the NS-3 tool, based on the outcomes of various parameters are plotted in graphs as seen above.

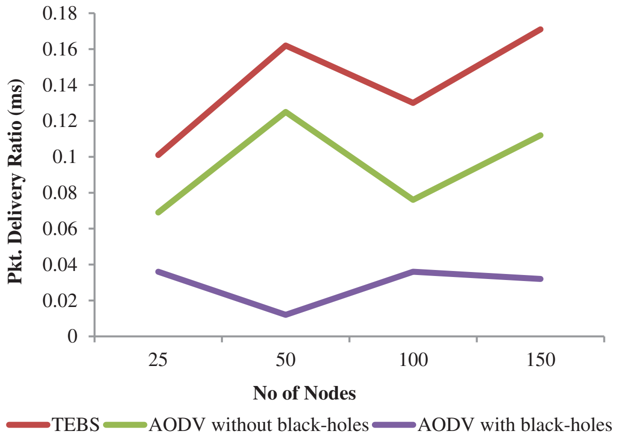

Figure 5: Packet delivery ratio (PDR) *vs.* no. of nodes results

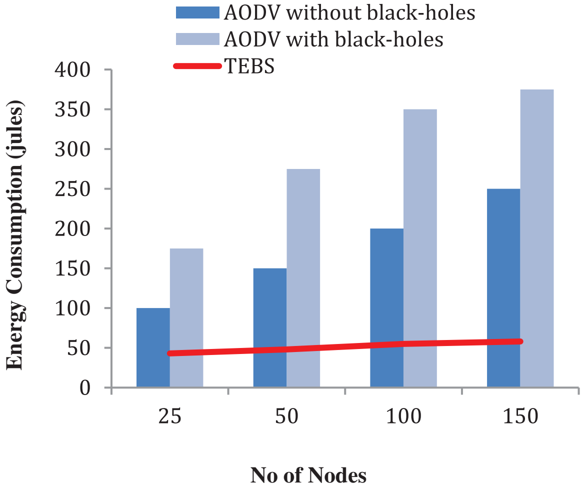

Figure 6: Energy consumption *vs.* no. of nodes results

Cooperative Black-Hole Nodes-the outcome of local AODV *vs.* helpful dark opening nodes demonstrated a zero Throughput. Expanding the number of dark opening nodes in the organization would undoubtedly hinder the linkage between the beginning and goal node, as illustrated in Fig. 7. Although TEBS removes any response from hidden nodes, this is because of the positioning of the dark aperture. Removing the response may be a position between the source and the objective node. Tab. 2 shows the simulation findings for cooperative black holes.

As shown in Fig. 8, when there are only two dark opening nodes within the organization, the terminal latency side effect in local AODV is the highest. Similarly, the relationship between source and target centers warned when the number of dark open centers rose, and end-to-end latency neared infinitely. Comparing TEBS AODV to local AODV, there is a minor change in end-to-end latency findings when the number of dark opening nodes is increased on the basis that the device still equals local AODV in route selection.

Table 1: Single black hole simulation results

No. of nodes	TEBS	AODV without black-holes Throughput (kpbs)	AODV with black-holes
25	98.635	71.488	32.032
50	145.623	118.327	20.443
100	121.448	89.442	37.671
150	165.456	118.6	31.234
Average of E2E delay (ms)			
25	0.92	0.98	1.32
50	0.78	0.92	1.12
100	0.74	0.83	1.01
150	0.69	0.72	1.09
Packet delivery ratio (ms)			
25	0.101	0.069	0.036
50	0.162	0.125	0.012
100	0.13	0.076	0.036
150	0.171	0.112	0.032
Energy consumption (jules)			
25	43	100	175
50	48	150	275
100	55	200	350
150	58	250	375

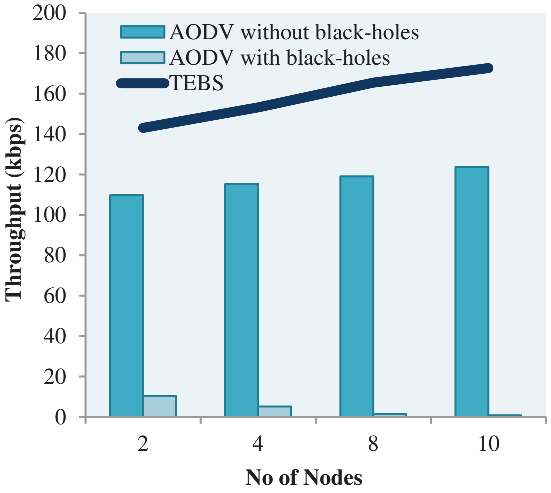

Figure 7: Comparative analysis over throughput *vs.* the number of BH nodes and its results

Table 2: Cooperative black hole simulation results

No. of nodes	TEBS	AODV without black-holes	AODV with black-holes
		Throughput (kbps)	
2	143.04	109.72	10.351
4	153.17	115.26	5.2
8	165.43	119.06	1.5
10	172.65	123.78	0.798
Average of E2E delay (ms)			
2	0.91	1.1	1.32
4	0.94	1.25	∞
8	0.97	1.74	∞
10	1.02	2.33	∞
Packet delivery ratio (ms)			
2	0.15	0.1078	0.01
4	0.15	0.073	0
8	0.15	0.069	0
10	0.15	0.051	0
Energy consumption (jules)			
2	11	20	44
4	25	50	128
8	30	78	249
10	33	100	321

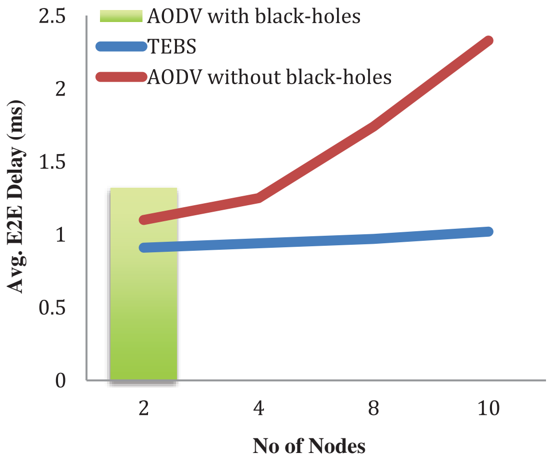

Figure 8: Comparative analysis over avg. E2E delay *vs.* No. of BH nodes and its results

The local AODV against acceptable dark opening nodes has a zero PDR, as shown in Fig. 9. When the amount of dark opening grows, they will defend the whole organization, undoubtedly cutting any communication between two nodes of any sort in the organization as shown in Fig. 10. Tab. 2 shows the numerical implications of increasing the number of dark opening nodes on E2E delay, throughput, and packet delivery ratio.

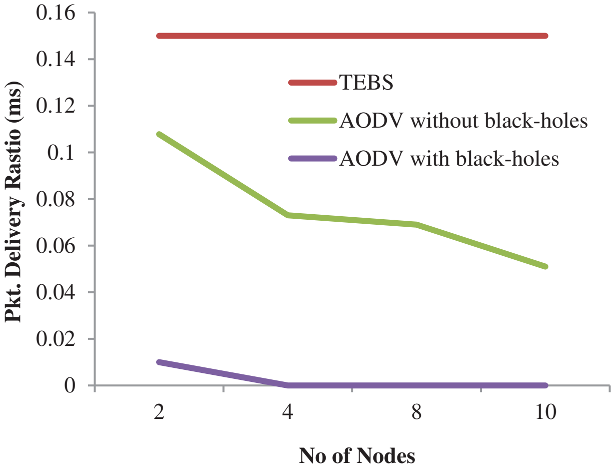

Figure 9: PDR findings *vs.* no. of BH nodes

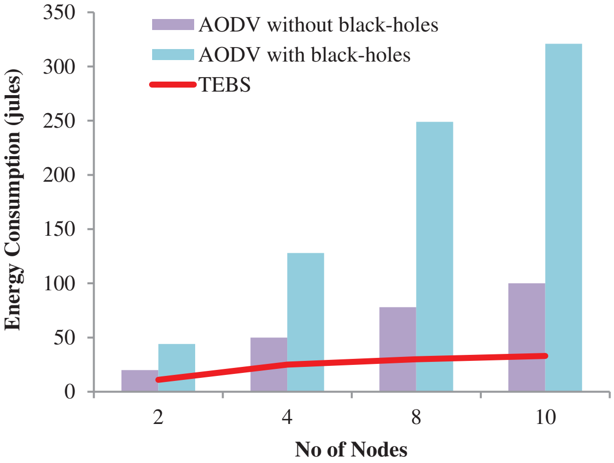

Figure 10: Energy consumption *vs.* no. of BH nodes

7 Conclusion

One of the most significant threats against MANET's operation is the dark opening attack. Detecting and isolating all dark aperture nodes in the network is vital for preventing the network from collapsing. This examination provided an intelligent dark opening recognition and detachment technique in this research, which might consider while developing and refining any dark opening combat norms or methods. As a consequence of the simulation of the technique, the E2E latency, throughput, and PTR are comparable to the local AODV.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Sharma, "Performance examination of black hole and gray hole attacks in MANETs," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2S6, pp. 980–982, 2019.

[2] S. Gurung and S. Chauhan, "A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability," *Wireless Network*, vol. 26, pp. 1981–2011, 2020.

[3] M. Goswami, P. Sharma and A. Bhargava, "Black hole attack detection in MANETs using trust based technique," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 4, pp. 1446–1451, 2020.

[4] J. Kaur, "Black hole attack in MANETs: Defending and detecting techniques," *International Journal of Information Security Science*, vol. 8, no. 4, pp. 65–76, 2019.

[5] S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," in *Int. Conf. on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, pp. 2391–2394, March 2017.

[6] M. Sathish, K. Arumugam, S. N. Pari and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in *IEEE Int. Conf. on Wireless Communications, Signal Processing and Networking, WiSPNET*, Chennai, India, pp. 2040–2044, March 2016.

[7] H. Kaur and K. Mangat, "Black hole attack in mobile ad hoc networks: A review," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 3, no. 2, pp. 189–191, 2017.

[8] K. Kumar and T. S. Aulakh, "Black hole attack in MANETs preventions and advancements: A review," *International Journal of Computer Applications International Conference on Advances in Emerging Technology*, vol. 12, pp. 4–9, 2016.

[9] 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.

[10] D. M. Khan, T. Aslam, N. Akhtar, S. Qadri and N. A. Khan, "Black hole attack prevention in mobile ad-hoc network (MANET) using ant colony optimization technique," *Information Technology and Control*, vol. 49, no. 3, pp. 308–319, 2020.

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

[12] R. Thiagarajan and M. Moorthi, "Energy consumption and network connectivity based on novel-LEACH-POS protocol networks," *Computer Communications*, Elsevier, vol. 149, pp. 90–98, November 2019.

[13] 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.

[14] M. M. Alani, "MANET security: A survey," in *IEEE Int. Conf. on Control System, Computing and Engineering (ICCSCE)*, Penang, Malaysia, pp. 559–564, November 2014.

[15] A. Joshi, "A review paper on black hole attack in MANET," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 4, no. 5, pp. 16–21, 2016.

[16] A. K. S. Ali and U. V. Kulkarni, "Comparing and analyzing reactive routing protocols (AODV, DSR and TORA) in QoS of MANET," in *IEEE Int. Advanced Computing Conf., IACC 2017*, Hyderabad, India, pp. 345–348, January 2017.

[17] K. Sudharson and V. Parthipan, "A Survey on ATTACK –anti terrorism technique for adhoc using clustering and knowledge extraction," in *Advances in Computer Science and Information Technology. Computer Science and Engineering. CCSIT 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Berlin, Heidelberg: Springer, vol. 85, pp. 508–514, 2012. https://doi.org/10.1007/978-3-642-27308-7_54.

[18] R. Thiagarajan and M. Moorthi, "Efficient routing protocols for mobile Ad Hoc networks," in *Int. Conference on AEEICB (978-1-5090-5434-3)*, IEEE SJR, Chennai, India, August 2017.

[19] L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs," in *5th Int. Conf. on Reliability, Infocom Technologies and Optimization*, Noida, India, pp. 405–408, September 2016.

[20] H. Moudni, M. Er-Rouidi, H. Mouncif and B. El Hadadi, “Performance analysis of AODV routing protocol in MANET under the influence of routing attacks,” in *2nd Int. Conf. on Electrical and Information Technologies, ICEIT 2016*, Tangiers, Morocco, pp. 536–542, May 2016.

[21] N. Kalia and H. Sharma, “Detection of multiple black hole nodes attack in MANET by modifying AODV protocol,” *International Journal on Computer Science and Engineering*, vol. 8, no. 5, pp. 160–174, 2016.

[22] P. L. Chelani and S. T. Bagde, “Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme,” in *Int. Conf. on Communication and Electronics Systems, ICCES 2016*, Coimbatore, India, October 2016.

[23] 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 Scientific& Engineering Research*, vol. 7, no. 3, pp. 81–85, 2016.

[24] S. Arun and K. Sudharson, “DEFECT: Discover and eradicate fool around node in emergency network using combinatorial techniques,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, 2020. https://doi.org/10.1007/s12652-020-02606-7.

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

[26] J. A. Shanny and K. Sudharson, “User preferred data enquiry system using mobile communications,” in *Int. Conf. on Information Communication and Embedded Systems (ICICES2014)*, Chennai, India, pp. 1–5, 2014. https://doi.org/10.1109/ICICES.2014.7033943.

[27] J. A. Jasmine, V. N. Jenipher, J. S. R. Jimreeves, K. Ravindran and D. Dhinakaran, “A traceability set up using digitalization of data and accessibility,” in *3rd Int. Conf. on Intelligent Sustainable Systems (ICISS), 2020*, Coimbatore, India, pp. 907–910, 2020. https://doi.org/10.1109/ICISS49785.2020.9315938.

[28] R. Thiagarajan, R. Ganesan, V. Anbarasu, M. Baskar, K. Arthi *et al.,* “Optimised with secure approach in detecting and isolation of malicious nodes in MANET,” *Wireless Personal Communications*, vol. 119, pp. 21–35, 2021. https://doi.org/10.1007/s11277-021-08092-0.

[29] M. Baskar, J. Ramkumar and C. Karthikeyan, “Low-rate DDoS mitigation using real-time multi threshold traffic monitoring system,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–9, 2021. https://doi.org/10.1007/s12652-020-02744-y.

[30] D. Dhinakaran and P. M. Joe Prathap, “Ensuring privacy of data and mined results of data possessor in collaborative ARM,” in *Pervasive Computing and Social Networking. Lecture Notes in Networks and Systems*, vol. 317. Singapore: Springer, 2022. https://doi.org/10.1007/978-981-16-5640-8_34.

[31] M. Baskar, R. Renuka Devi and J. Ramkumar, “Region centric minutiae propagation measure orient forgery detection with finger print analysis in health care systems,” *Neural Processing Letters*, 2021. Springer, pp. 1–13, January 2021. https://doi.org/10.1007/s11063-020-10407-4.

[32] K. Sudharson and V. Parthipan, “SOPE: Self-organized protocol for evaluating trust in MANET using eigen trust algorithm,” in *2011 3rd Int. Conf. on Electronics Computer Technology*, Kanyakumari, India, pp. 155–159, 2011. https://doi.org/10.1109/ICECTECH.2011.5941675.

[33] J. Ramkumar, M. Baskar, M. Viswak and M. D. Ashish, “Smart shopping with integrated secure system based on IoT,” *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 301–312, ISSN: 2005–4238, April 2020.