A Dynamic Threshold And Mac Address Based Technique To Detect Black Hole Nodes In Manets

Zulfiqar Ali Zardar[1], Imtiaz Ali Brohi[1], Yasir Ali Panhwar[1], Murk Chohan[1] , Najma Imtiaz Ali[2]

***Abstract*—A distributed wireless network of mobile nodes is a mobile ad-hoc network (MANET). To exchange the information between nodes each node receives and forwards the data packets. Appropriate communication depends on cooperation between the nodes. But some nodes become malicious and misbehave during the communication. Therefore, MANET is vulnerable from those malicious nodes. The black hole node is treated as a malevolent node in MANET. Thus, the malicious node manipulates the source node's false routing information and hence, drops every data packets without routing them to the destination point. The protection from the black hole attack, we have proposed a prominent prevention technique depend on the dynamic threshold, hop count and MAC address. In the proposed novel technique, it is verified by the legitimate device that the route reply packet (RREP) is either sent by the genuine or malicious node. In RREP packets, the node is suspicious. If the target sequence number is determined to be greater than the dynamic threshold of the corresponding node. Furthermore, the node is declared as the malicious node, when the hop count of the suspicious node one and MAC address flag is "DOWN". Comparatively the proposed technique not only provides better in detection rate but also provide overall better performance in other metrics. A lightweight novel technique that detects the malicious node attack using MAC address and threshold value. the-art face recognition techniques.**

***Keywords—*: MANET, Defense mechanism, Black hole node, dynamic threshold, MAC address, Hop count.**

INTRODUCTION

The rapid rise of handheld devices and the exponential increase in the use of wireless networking technology have shifted the focus of the current period toward mobile ad-hoc networks (MANETs) [1, 2]. The primary characteristic of a MANET network is its rapid setup at a low cost and in a short period of time. It can be formed at any time and in any location with the use of wireless nodes. Additionally, the network lacks a backbone structure, allowing nodes to move freely, self-configure, and join and exit the network arbitrarily [3, 4]. The wireless nodes can function as a host or a router, performing route finding and maintenance as well as packet forwarding. The topology of a MANET evolves dynamically as a result of the nodes' movement [5]. MANET facilitates communication in a multi-hop mode, i.e. via intermediary nodes. The intermediary nodes act as a link between the sending and receiving nodes, as well as a relay for data packets [6]. If intermediary nodes cooperate and behave properly, they are considered legitimate nodes; otherwise, they are considered malevolent nodes. Additionally, the network contains numerous other nodes, such as selfish nodes, defective and liar nodes, and so on [7, 8]. Nodes typically have limited battery capacity, memory, bandwidth, and computing capabilities. However, due to the node's limited power, it is unable to communicate across a long distance. MANET can be used for a variety of purposes, including military activities, rescue operations, disaster zones, mountainous locations, and forestry areas. [9]. The communication between two vehicles for the purpose of driver assistance and safety, as well as in locations where wired infrastructure is impractical to build [10, 11]. Such communication between mobile nodes should be extremely secure, as it is directly related to the user's safety and security. Though MANET is more susceptible to attack than typical wire infrastructure due to its unique characteristics, such as dynamic topology. Due to the mobility of nodes, the common means of communication, and the lack of central control, a malicious node can simply exploit a forged response to the source node in order to gain access and begin dropping data packets in the network [12-14].

A) Black hole attack

In MANET, a black hole attack is a continuous assault referred to as a full-packet drop attack [15, 16]. The rogue node in the network suppresses all data packets flowing through it by delivering a bogus route response packet (RREP) to the originating device. The terminology are defined in Table-1, whereas Fig.1 demonstrates that the sending node (SN) did not have a route to the destination node, and hence sent the path request packet (RREQ) to the network infrastructure for route discovery. When the RREQ packet is received from the destination node, the intermediate node sends the route reply (RREP) packet. Meanwhile, the intermediary nodes forward RREQ packets to the neighboring node for processing. Subsequently, the black-hole node assumes the role of the hostile entity, promptly responding with a forged RREP packet [17]. The RREP contains the greatest sequence number and one hop count to catch the source node's attention. The sequence number is useful for determining the route's freshness. When a source node receives a large sequence number from a malicious entity, it establishes a false route

[1]Department of Information and Communication Technologies, the Begum Nusrat Bhutto Women University, Sukkuri
[2]Institute of Mathematics and Computer Science, University of Sindh, Jamshoro
Email: zulfiqar.ali@bnbwu.edu.pk

with it because the source node recognizes that it has a valid route to the receiver node and begins transmitting payload to it. The malicious entity in the network provides bogus routing information and demonstrates to the target node that it has a new and valid path to it [18]. After receiving a fraudulent route reply (RREP) packet from the malicious node, the source node determines optimal path to take in order to reach the target. Unbeknownst to the destination node, a black hole forms between the source and destination paths and consumes all traffic during the payload transmission phase. Such attacks result in Denial of Service (DoS) attacks in MANETs, drastically reducing network performance [19, 20].

Table I. Notations

Notations	Significance
SN	Source Node
IP	Internet protocol
IN	Intermediate node
DN	Destination Node
BN	Black hole Node
SSN	Source Sequence Number
DSN	Destination Sequence Number
RREQ	Route Request
RREP	Route Reply
SSN	Source Sequence number
DSN	Destination Sequence number

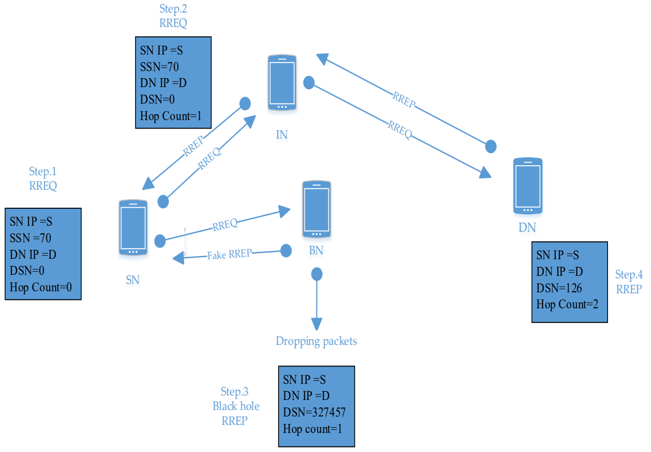

Figure.1 Blackhole attack

Figure-1 shows the illustrations of the attack of the malicious node with a bogus reply in the MANET infrastructure. The source node is represented by the SN, while IN is intermediate node. The destination node is represented by DN and black-hole node is by BN. RREQ packet is accepted by the BN from the sending entity and it immediately forwards a fake RREP with one hop count and high sequence number as to pretend that it has a shortest and fresh path. When sending entity accepts fake Route REP packet then, it creates a path which passes through the malicious node. Thus, based on fake RREP packet the sending entity starts communication by sending the payload packets. However, black hole node drops all payloads without forwarding to the destination node [21-23].

In this research, we offer a technique for detecting and preventing black hole node attacks in the AODV routing protocol. Using a dynamic threshold value, MAC address, and hop count, this technique determines if a node is a valid node or a black hole node. The destination Request REP packet's sequence number is compared to the dynamic threshold value in our suggested technique. When the destination sequence number exceeds the dynamic threshold value, the node is considered malicious. Additionally, if its hop count is one and it does not provide the MAC address, it proves that it is a malicious black-hole node. As a result, all nodes in the MANET will discard connection with the malicious node and add it to their blacklist of nodes to communicate with in the future. Additionally, the suggested strategy provides a secure and optimum route to normal entities by avoiding blacklisted nodes.

The main contribution of the paper are summarized as under:
The suggested technique discovers and eliminates black hole nodes in MANET by continuously updating the dynamic threshold value, MAC address, and hop count. The suggested technique has the advantage of detecting black hole nodes in a dynamic environment.
The suggested technique is distinct from a number of existing techniques discussed in previous work, which have a low detection rate for black hole nodes.
Complete investigational results demonstrate the proposed technique is a viable and productive method used for identifying black hole nodes and also mitigates the harm caused by black hole nodes.
Rest of the paper presents in the following sections:

B) Related Work

Numerous strategies for detecting and preventing black-hole attacks in MANET infrastructure have been proposed. However, present methods have the following limitations/ disadvantages, which are detailed chronologically in Table.2.

Table.II shows the list of existing techniques and their demerits.

.S.No	Author & year	Technique Used	Limitations
01	Su, M. Y. (2011) [24]	Special IDS nodes	Extra nodes are required, and unable can't detect malicious node due to improper deployment of IDS nodes
02	Baadache et al. (2012) [25]	Acknowledgement Based	Usage of extra acknowledgment control packets .in term of overhead
03	Katal et al.2013 [26]	Clustering based	Increases delay in data packet routing
04	K.S.Dhanalakshmi et al. 2014 [27]	Cryptography based	Instantly the nodes consume more battery power as new key are generated
05	Chang et al. 2015[28]	Bait Detection	.Additional routing overhead due to bait packets
06	Vadhana. K et al. 2015 [29]	Trust-based	High routing overhead
07	Nachiket. K et al. (2016) [30]	MAC layer based detection engine	High routing overhead because of RTS and CTS
08	S. Gopinath 2018[31]	Detection based on location	Ample hardware requirements
09	V.S. Venu (2018)[32]	Frame-checking Sequence	computational complexity

After analysing the existing solutions and their advantages and disadvantages, our proposed solution is a prominent prevention technique within MANET infrastructure.

The proposed technique is different from existing techniques because of the following reasons:

- The proposed technique detects the black hole nodes under the highly dynamic environment.
- The proposed technique didn't use any extra computations, extra packets, spam request, or special nodes.
- The proposed technique only checks the RREP packet from the corresponding node to avoid routing overhead and computations. Additionally, proposed technique did not disturb the remaining routing process except RREP packet.

PROPOSED METHODOLOGY

This section explains on the proposed technique. We avoid adding additional nodes or assigning privileges to a particular node using the proposed technique due to the high routing overhead and energy consumption. The proposed technique detects the black hole node by utilizing a dynamic threshold value, MAC address, and hop count. In MANET infrastructure, a dynamic threshold is critical for detecting black-hole nodes. It is critical to identify and avoid black-hole nodes in a dynamic environment due to the topological changes associated with dynamically changing MANET infrastructure node positions.

A) Description of Flowchart

As illustrated in Figure-2, AODV routing protocol plays a critical role from source to destination node. The source node can send packets whenever it wishes using RREQ and RREP packets. AODV uses the DSN of the RREP packet to determine the fresh path. When the current packet's destination sequence number is greater than the previously stored destination sequence number in the data routing information table, the normal node's routing information is updated.

When a legitimate node receives a route reply (RREP) packet from the corresponding node, it verifies that the packet originated from a legitimate node rather than a malicious node. It first checks the blacklist to see if it is already present, and then discards the RREP packet. If it is not discovered, proceed with the normal procedure. For malicious node detection, it compares the destination sequence number to a threshold value; if it is greater than the node, it is suspicious; otherwise, the node continues normally with the second phase's hop count and mac address checks. If the hop count of the corresponding node is zero and the mac address is missing, the legitimate node declares the node to be a black hole node. As a result, the legitimate node immediately broadcasts a message to the MANET infrastructure indicating that the node is a black hole node. All communication with that node will be discarded and added to the blacklist.

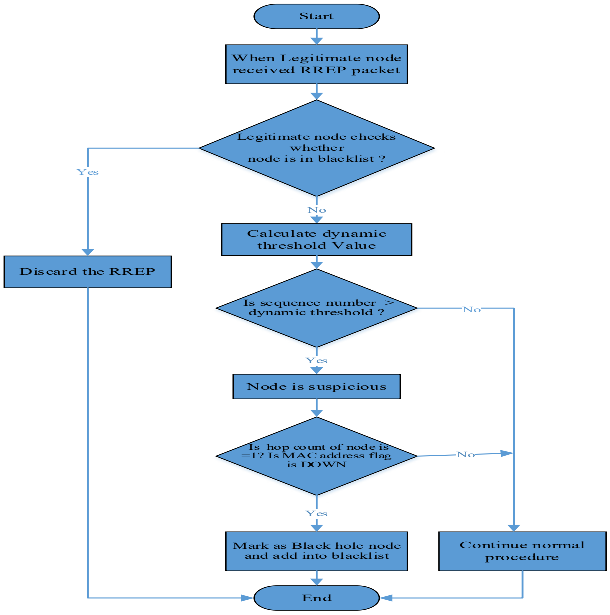
Start
When Legitimate node received RREP packet
Legitimate node checks whether node is in blacklist ?
Yes
No
Discard the RREP
Calculate dynamic threshold Value
Is sequence number > dynamic threshold ?
No
Yes
Node is suspicious
Is hop count of node is =1? Is MAC address flag is DOWN
No
Yes
Mark as Black hole node and add into blacklist
Continue normal procedure
End

Figure.1 Flowchart of the proposed technique

B) Calculation of dynamic threshold value

Each node calculates the dynamic threshold value in our suggested technique. The threshold value is calculated using the total number of active nodes in the network infrastructure, the current time, and the destination node's last sequence number. The number of destination sequences in a network is almost proportional to the time interval and the number of active nodes in the network. We defined the following dynamic threshold equation based on this insight.

Known Threshold = (n+) t + LSDN (1)

The number of nodes in this case is denoted by n. and are positive constants indicating the growth of the target node's sequence number. Here, t denotes the passage of time; the amount of time that has transpired after identifies the final sequence number. LSDN denotes the latest sequence number of the destination node that the calculating node is aware of. When a node, whether genuine or malicious, joins the network, the total number of nodes increases as well. Each node in our proposed technique calculates the threshold value using only n and t. While n increases as new nodes join, the threshold value is also changed.

C) MAC address and Hop count of black hole node

Each genuine node includes the appropriate parameters and maintains the destination flag "UP" in the RREP packet. The destination flag verifies that the node's destination is valid. In the AODV routing protocol's trace file, the source MAC address is 0 and the destination MAC address is down. It did not display its destination flag "UP" during the black hole attack. It just responds with a hop count and conceals the target node's mac address. This means that black hole nodes will blindly transmit such messages back to the source node. The suggested technique checks the mac address of the associated node's destination flag in the RREP packet for confirmation of the black hole node if the mac address of the corresponding node's destination flag is "DOWN" in the RREP packet, indicating that the node is malicious. The hop count indicates the number of hops between the transmitting and receiving entities. The malicious attack always transmits a single (one) hop count in the RREP packet to the source node, and the source node thinks the black hole node to be close to the destination node due to the single hop count.

D) The detection method of black node

In the first phase, the network has both malicious and benign nodes. As a result, determining whether a node is a legal node or a black-hole node is rather challenging. Each legitimate node keeps a blacklist table that contains information about the network infrastructure's black hole nodes. To combat if a node is a black hole or not, the proposed technique examines three conditions contained in the RREP packet. The destination sequence number is checked first, followed by the hop count and last mac address of the corresponding node, and the sending node broadcasts the RREQ packet for path discovery in the network. The RREQ packet is then forwarded by the intermediate node to the subsequent node if it is not the destination node. The black hole node, on the other hand, responds swiftly to the RREQ packet by delivering a false RREP packet. The RREP packet contains a large sequence number and a small hop count, i.e. 1. By sending these false values, it asserts that it has the valid and shortest path to the destination entity in the network infrastructure, and then the source node establishes a route advertised by the black hole node to send the data packets, and once established, the black hole node drops all incoming payloads without forwarding them to the destination node.

Each node in the network calculates the dynamic threshold value in order to detect the black hole node. A legal node is one that matches the dynamic threshold value with the accompanying node's destination sequence number. When the destination sequence number of the node's payload exceeds the threshold value, the node considered suspect. To confirm that the node is not a black hole node, the hop count value and mac address of the connected node are also checked. If the hop count is one and the RREP packet contains no mac address, it is confirmed that the node is a black hole node. The reason for this is that the black hole node chose not to display its destination node. Because it lacks a genuine destination node, immediately upon confirmation of the black hole node, each node rejects any traffic from the black hole node and adds it to the blacklist. If none of these three conditions are met by the RREP packet, the remainder of the operation is identical to the traditional AODV protocol as illustrated in the proposed technique's Fig.1 flowchart.

Tables 3 and 4 illustrate the node's behavior as a function of several settings. When the appropriate node gives the greatest sequence number, hop count, and destination, the mac address flag in the RREP packet remains "DOWN." Then the associated node is referred to as a malevolent node.

Table.III Performance of the mobile node

The destination sequence number of RREP packet	Hop count	flag of Mac Destination	Type of attack
Normal number	1	UP	No attack
Normal number	0	UP	No attack
Normal number	1	UP	No attack
Highest number	1	DOWN	Black hole attack

Table.IV Simulation parameters

Parameters	Value
(Network Simulator	(NS-2.35
Network area	800 800 m
Normal nodes	140
(Protocol	(AODV
Mobility model	Random Walk mobility
Simulation time	800 sec
(Traffic type	Constant bitrate (CBR
Traffic Agent	UDP
Packet size	512 bytes
Mobility	0.5-0.1 m/s
Pause time	5-20 s
(Network density	50,70,90,140 (nodes

RESULTS AND ANALYSIS

Network simulations are performed using the network simulator (NS-2.35). Two hundred nodes are randomly distributed across a network simulation area of 800 800 m. The simulation is conducted for 800 seconds with 512-byte packets. The nodes' mobility ranges from 5 to 35 m/s, and the network simulation is done using the AODV routing protocol.

A)Packet delivery ratio (PDR)

The PDR comparison of native-ADOV with a black hole, AODV without a black hole, and the proposed approach is shown in Figure 3. demonstrates unequivocally that the proposed technique has a greater PDR than techniques. The reason for this is that it detects black hole nodes far more quickly than others. It increases by 96.48 percent when compared to the normal AODV and ADOV.

Table.V Simulation parameters

No. of Nodes	Normal-AODV	ADOV with Attack	Proposed technique
50	93.29	73.13	88.12
70	93.61	66.81	89.57
90	95.25	62.23	90.11
120	93.99	60.94	90.16
140	**96.48**	**57.89**	**90.26**

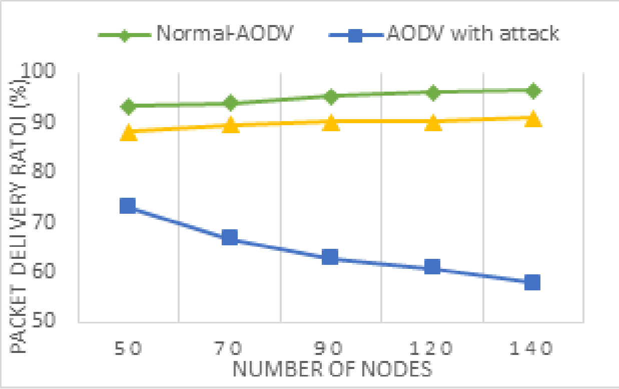

Figure.2 Packet delivery ratio

B) Throughput (kbps)

The performance of native AODV with a black hole, AODV without a black hole, and the suggested approach are depicted in Fig.4.the AODV achieves improved result than black hole nodes, but with black hole nodes, performance decreases because black hole nodes continuously disrupt communications by dropping data packets, whereas the proposed technique provides secure route nodes to transfer data packets due to the detection and isolation of black hole nodes on time.

Table.VI Simulation parameters

No. of Nodes	Normal AODV	ADOV with Attack	Proposed Techniques
50	69.26	36.17	66.39
70	70.21	33.64	66.97
90	71.86	31.70	67.82
120	72.64	29.54	68.67
140	**73.35**	**26.92**	**69.41**

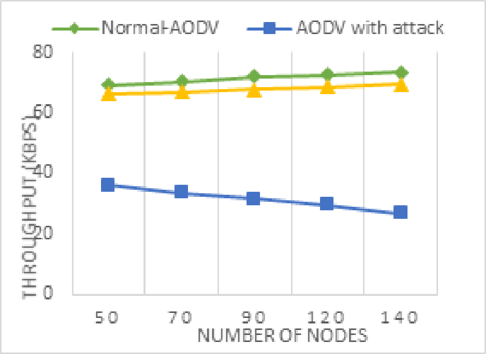

Figure.3 Throughput

C) Average delay

Figure.4 illustrates the suggested technique's average latency with both normal AODV and AODV under assault. It is obvious that ADOV without attack has a shorter delay than standard AODV and the proposed approach.

Table.VII Simulation parameters

No of Nodes	Nor-mal-AODV	ADOV with attack	Proposed technique
50	1.339	0.934	1.024
70	1.899	0.926	1.034
90	2.279	1.049	1.185
120	2.692	1.362	1.492
140	**3.197**	**1.783**	**1.917**

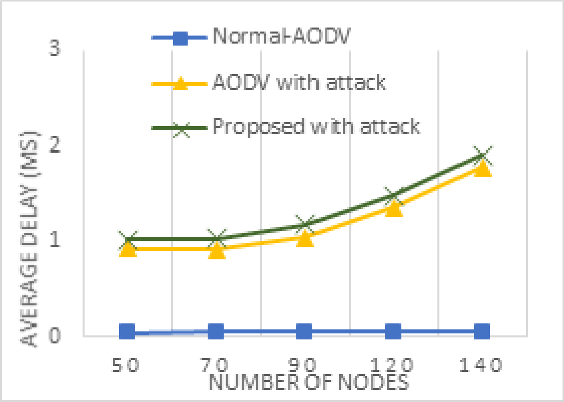

Figure.4 Average delay

CONCLUSION

All nodes in a MANET operate as routers during communication, which introduces security risks into the network routing protocol. Additionally, a black hole is a well-known security vulnerability in the MANET architecture, and as such, we have developed a detection and prevention technique. The suggested technique locates the black hole node using the threshold value, the mac address, and the hop count. When the destination sequence number of the corresponding node exceeds the dynamic threshold value in the RREP packet, the node is considered suspicious. If the hop count is one and flag is "DOWN," which confirms the black hole node. The suggested technique has the advantage that the estimated threshold value is dynamically updated as the network get dense. The value of the threshold is dependent on the number of active nodes, the passage of time, and the value of and. According to simulations, our suggested technique detects all malicious nodes and improves throughput and payload delivery performance. In future study, the network can be tested using a variety of scenarios involving varying network sizes, mobility, and node counts.

REFERENCES

[1] M S Pathan, (2018) "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs", Future Internet, Vol. 10, No. 2, pp. 16–16.

[2] Ali Zardari and Z, (2019) "A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs", Future Internet, Vol. 11, No. 3, pp. 61–61.

[3] M Umar, A Sabo, and A A Tata, (2018) "Modified Cooperative Bait Detection Scheme for Detecting and Preventing Cooperative Blackhole and Eavesdropping Attacks in MANET", in 2018 International Conference on Networking and Network Applications.

[4] A M Desai and R H Jhaveri, (2019) "Secure routing in mobile Ad hoc networks: a predictive approach", International Journal of Information Technology, Vol. 11, No. 2, pp. 345–356.

[5] Q M Yaseen and M Aldwairi, (2018) "An Enhanced AODV Protocol for Avoiding Black Holes in MANET", Procedia Computer Science, Vol. 134, pp. 371–376.

[6] M Sathish, (2016) "Detection of single and collaborative black hole attack in MANET", 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).

[7] A Lupia and F D Rango, (2016) "A probabilistic energy-efficient approach for monitor- ing and detecting malicious/selfish nodes in mobile ad-hoc networks", 2016 IEEE Wireless Communications and Networking Conference.

[8] N Ramya and S Rathi, (2016) "Detection of selfish Nodes in MANET - a survey", 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS).

[9] R Jain and I Kashyap, (2018) "Survey of Energy Aware Link Stable Routing Protocols in MANETS", 2018 2nd

International Conference on Trends in Electronics and Informatics (ICOEI).

[10] A A Chavan, D S Kurule, and P U Dere, (2016) "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack", Pro- cedia Computer Science, Vol. 79, pp. 835–844.

[11] S Sarika, (2016) "Security Issues in Mobile Ad Hoc Networks", Procedia Computer Science, Vol. 92, pp. 329–335.

[12] M Peng, (2016) "Black hole search in computer networks: State-of-the-art, challenges and future directions", Journal of Parallel and Distributed Computing, Vol. 88, pp. 1–15.

[13] A Tripathi and A K Mohapatra, (2016) "Mitigation of Blackhole attack in MANET", 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN).

[14] N Nissar, N Naja, and A Jamali, (2017) "Lightweight authentication-based scheme for AODV in ad-hoc networks", 2017 International Conference on Wireless Technologies, Em- bedded and Intelligent Systems (WITS).

[15] D Khan and M, (2017) "Study of detecting and overcoming black hole attacks in MANET: A review", 2017 International Symposium on Wireless Systems and Networks (ISWSN).

[16] Gurung, S., & Chauhan, S. (2019). Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. Wireless Networks, 25(3), 975-988.

[17] I Nurcahyani and H Hartadi, (2018) "Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET)", 2018 International Symposium on Electronics and Smart Devices (ISESD).

[18] M Mistry, P Tandel, and V Reshamwala, (2017) "Mitigating techniques of black hole at- tack in MANET: A review", 2017 International Conference on Trends in Electronics and Informatics (ICEI).

[19] Gurung, S., & Chauhan, S. (2019). A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. Wireless Networks, 25(4), 1685-1695.

[20] A Nabou, M D Laanaoui, and M Ouzzif, (2018) "Evaluation of MANET Routing Proto- cols under Black Hole Attack Using AODV and OLSR in NS3", 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM).

[21] M R Hasan, (2017) "Enhanced AODV: Detection and Avoidance of Black Hole Attack in Smart Meter Network", 2017 26th International Conference on Computer Communication and Networks (ICCCN.

[21] Yang, H., Zhou, Y., Hu, Y. H., Wang, B., & Kung, S. Y. (2018, May). Cross-layer design for network lifetime maximization in underwater wireless sensor networks. In 2018 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[22] A T Kolade, (2017) "Performance analysis of black hole attack in MANET", Proceedings of the 11th International Conference on Ubiquitous Information Management and Commu- nication.

[23] M. Y Su, (2011) "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications, Vol. 34, No. 1, pp. 107– 117.

[24] A Baadache and A Belmehdi, (2012) "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks", Journal of Network and Computer Applications, Vol. 35, No. 3, pp. 1130–1139.

[25] A Katal, (2013) "A cluster based detection and prevention mechanism against novel data- gram chunk dropping attack in MANET multimedia transmission", 2013 IEEE Conference on Information & Communication Technologies.

[26] K S Dhanalakshmi, B Kannapiran, and A Divya, (2014) "Enhancing manet security using hybrid techniques in key generation mechanism", 2014 International Conference on Elec- tronics and Communication Systems (ICECS).

[27] J Chang, (2015) "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE Systems Journal, Vol. 9, No. 1, pp. 65–75.

[28] S V Kumari and B Paramasivan, (2015) "Ant based Defense Mechanism for Selective For- warding Attack in MANET", 31st IEEE International Conference on Data Engineering Workshops.

[29] N Kshatriya, K Mallawat, and A S Biswas, (2016) “Security in MANET using Detection En- gine”, 2016 International Conference on Computing, Analytics and Security Trends (CAST).

[30] Sandhya Venu, V, and D Avula, (2018) “Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks”, International Journal of Communication Systems, Vol. 31, No. 6, pp. 3518–3518.

[31] K Ragunathan and T Kathiravelu, (2016) “A hop-count and time based MANET routing protocol”, 2016 IEEE International Conference on Advanced Networks and Telecommuni- cations Systems (ANTS).

[32] H Bayulu, (2017) “Preventing goodput collapse for multi-hop routing in IEEE 802.11 based ad-hoc networks by adjusting residual hop count”, 2017 25th Signal Processing and Com- munications Applications Conference (SIU.