A blackhole attack mitigation algorithm in MANET based on standard deviation outlier detection

BEATRICE CLEMENCE [1], ZHAO CHENG XUAN [1] AND AYESHA YOUNIS [2]
Department of Computer Science[1]; Department of Signaling and Information Processing[2]
Tianjin University of Technology and Education
Tianjin 300222
CHINA
beatrice.mushy@yahoo.com; xuanzc@tute.edu.cn; ayesha@tute.edu.cn

Abstract: - A mobile ad hoc network (MANET) performs a routing and data forwarding obligations in a trustless environment where mobile nodes are not controlled and administered by third parties, it usually suffers from multiple attacks such as the blackhole attacks. This blackhole attacks cause two extreme effects on the network if the malicious nodes are not eliminated. Firstly, it deliberately alters the original data route sequence with an injection of false routing information comprises of the counterfeit destination sequence number and smallest hop count. Secondly, it becomes too greedy to send data to other nodes after receiving from a genuine node. Therefore, this may delay the data transmission process in the act of data dropping. To protect the routing discovery process of an ad hoc on-demand distance vector (AODV) protocol from the blackhole attack, we present a mitigation algorithm based on standard deviation outlier detection to determine a threshold value for validating the route reply (RREP) destination sequence number before route establishment. The simulation shows that the algorithm can detect the malicious nodes and performs better than AODV in a blackhole attack environment.

Key-Words: - MANET; Blackhole Attack; AODV; Malicious Node; Standard Deviation; Routing Discovery.

Received: October 24, 2019. Revised: February 23, 2020. Accepted: March 10, 2020. Published: April 3, 2020.

1 Introduction

The MANET is an improvise dynamic wireless ad hoc network with a random collection of self-configure and self-healing mobile devices temporarily communicate wirelessly to serve onsite emergency. It manages network activities in an environment where it is difficult to establish a centralized system and install a fixed cable network or base station. Mobile devices in MANET act both as host and router, they regulate routing and data forwarding process with an assist of three protocols, namely reactive, proactive and hybrid. It serves military operation, business conference meetings, environment monitoring operations, emergency relief operations, and inventory management operations. These sorts of applications certainly require highly secure communication between mobile nodes as they handle vital information concerning human life and safety[1].

Compared to conventional wired networks, MANETs have unique peculiarities that make them extremely defenseless to various attacks such as blackhole, wormhole, and a grayhole. [2]–[5] analyze how the blackhole nodes degrade the performance of AODV protocol using mobility, pause time and nodes as main assessment parameters. Simulation results show that the AODV has very poor performance under the deployment of the blackhole attack. To handle the situation, therefore, various mitigation methods have been suggested. Jain and Khuteta[6] proposed the deployment of a base node (BN) on the network suspected to have abnormal behavior. The BN tracking node responds to the dummy RREP and broadcasts a block message in the network so that real nodes can use it to isolate black hole nodes. Noguchi and Yamamoto[7] proposed a dynamic threshold-based method with the support route request (RREQ) dummy approach to maximize the true detection rate and minimize the false detection rate of blackhole attack. The threshold value identifies a black hole node, and the RREQ dummy prejudges the black hole node in advance before permanently deleting it from the blacklist table. Mishra, Samvatsar, and Singh[8] proposed a node discharge method with black hole attack traits. This method successfully improves the packet transmission rate than the improved AODV with an attacking attribute. Devi, Saraswathi, and Yogesh [9] proposed a cooperative multilayer defensive mechanism to eliminate a distributed denial of service (DDoS) attack in which it was successfully.

MANET is severely affected with multiple blackhole attack, as therefore require mitigation

methods that cope with its special dynamic feature.[1], [6], [10], [11] proposed methods varied in implementations to detect and prevent blackhole attacks. Here we give an alternative method for the detection of the multiple blackhole node. The proposed work uses the standard deviation outlier detection to determine the threshold value with the provision of the destination sequence number dataset of RREP stored in the local memory of each node accepting the RREP packet. The threshold value verifies the destination sequence number to eliminate a node with the fake routing information.
The remaining work of this paper is arranged as follows. The illustrations of the AODV protocol and blackhole attack are given in section 2. Section 3 details the blackhole attack mitigation algorithm. The proposed algorithm is evaluated in section 4. The conclusion and future work are explained in the final section.

2 Illustration of AODV and blackhole attack

AODV is a unicast on-demand routing protocol that adapting the distance-vector algorithm to manage mobile devices operates in MANET. The protocol only processes a route discovery when there is no active communication link to a new destination. Otherwise, the source shares the data with the destination using an active route presented in the routing table. MANET faces the challenge of frequent disconnection of links due to the network instability, therefore AODV is a suitable protocol since it offers a fast convergence, and enables mobile devices affected by the link failure to notify each other so that all routes with the broken links become invalid[12]. This protocol is the most useful because it prevents routing loops by relying on each node to maintain its destination sequence number. It operates into two phases where mobile nodes cooperatively discover and maintain routes by sharing RREQ, Route Reply, Route Errors and HELLO control messages[13], [14]. Figure 1 is constructed with seven nodes to demonstrate the route discovery process of AODV in steps.

1) A Source S has data to share with destination D, but no route has found in S' routing table, therefore, S initiates the process of route discovering by broadcasting RREQ to neighbors in a range which are 2, 3 and 5. Initially, a hop count field of the RREQ packet is set to zero and updated on each hop.

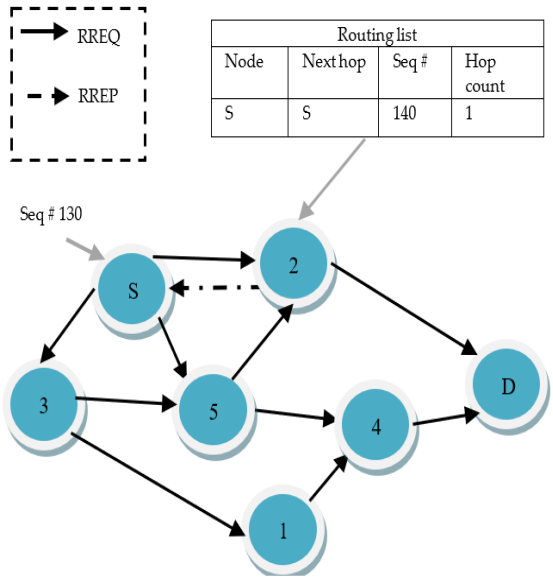

Fig 1 AODV discovery process

2) Node 2, 3 and 5 receive the RREQ packet, they make a temporary memo (reverse route) of returning to S in their routing table by fetching data from originator RREQ fields. Each node maintains the same sequence number to avoid rebroadcast of RREQ.
Reverse route list:
   - Node 2: destination = S, next-hop = S, Sequence number = 130, hop count = 1
   - Node 3: destination = S, next-hop = S, Sequence number = 130, hop count = 1
   - Node 5: destination = S, next-hop = S, Sequence number = 130, hop count = 1
   - Node 1: destination = S, next-hop = 3, Sequence number = 130, hop count = 2
   - Node 4: destination = S, next-hop = 5, Sequence number = 130, hop count = 2
3) The same process in stage 2 continues until the source node receives RREP with a fresh route obtained from either an intermediate node or a destination node. Notably, during the broadcast of RREQ, there is a high probability that the intermediate or destination node receives more than one RREQ packet of the same source address and Request ID. Node 5, for example, has received the same control message from 3, will not process it since it has already set a reverse path of the same message
4) In the case based on Figure 1, node 2 realizes it has a route to the destination; no update will be conducted in the routing table since the sequence number is fresh to reach the destination. It is fresh because the sequence number is larger than that of RREQ. Therefore,

node 2 will not broadcast RREQ to D instead it unicast RREP packet back to S using a reverse path "destination = S, next-hop = S, Sequence number = 130, hop count = 1". If node 2 has a smaller sequence number, then broadcast of RREQ to D could have been taken place.

5) The Source node S establishes a forward path using reverse path details after receiving the RREP message from neighbor 2 and update its routing table details.
6) Forward route:
   - Node S: destination = D, next-hop = 2, Sequence number = 140, hop count = 1
   - Node 2: destination = D, next-hop = D, Sequence number = 140, hop count = 1
7) The node in MANET does not operate in a fixed location, if it happens, node 2 is out of range and node 5 has acknowledged that link to 2 has broken, then node 5 will deliver the error message RRER to node S to delete the route.

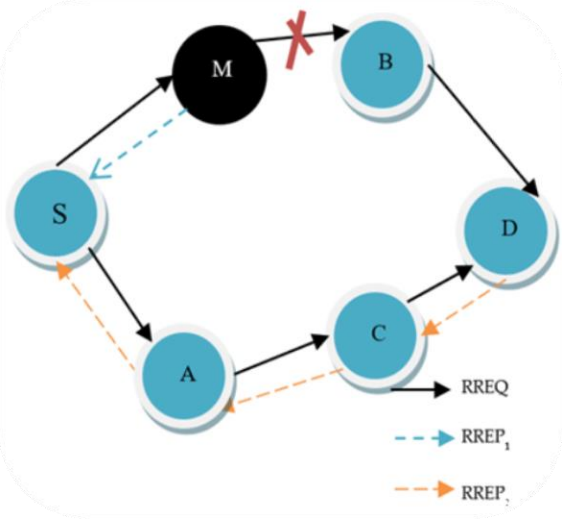

Fig 2 Blackhole attack

Despite having good characteristics than some of the other protocols, it's routing discovery process is vulnerable to blackhole attack. The blackhole attack is a denial service attack on the network layer where the blackhole node denies to forward data to the neighbors or destination node. In Figure 2 Source node (S) sends the RREQ packet to both the destination node (D) and blackhole node (M). D sends $RREP_2$ packet contains actual destination sequence number back to S. On the other hand, M sends a fake $RREP_1$ having a highest destination sequence number and lowest hop count back to node S. S receives both fake $RREP_1$ and reliable $RREP_2$, but it will select the path via M as a next-hop to communicate D and ignores $RREP_2$ because AODV protocol accepts any route with a high destination sequence number and lowest hop count as the best route towards the defined destination node. M drops all the packets it receives from S.

3 The blackhole attack mitigation algorithm

3.1 Problem statement

Attackers recognize MANET's security vulnerability on AODV, therefore burglary all the information it receives from the network. They usually decrease the number of packets to be received at the destination node, decrease throughput, increase routing overhead and increase the delay in data transmission. Our proposed scheme intends to improve these metrics.

3.2 Adversary Attack Model

Consider the fact that origin AODV does not contain blackhole nodes initially, we decide to set up a blackhole attack environment. In the procedure, we allow nodes to send each other Hello packet to collect all available nodes in the network. After 15 seconds, 10% of the total nodes collected are assigned as the compromised nodes. These nodes will participate in attacking the route discovery process of the AODV protocol without being noticed. And when a compromised node is in range of the current communication, it receives the RREQ and on the spot responds with RREP with no extra work of checking the routing table. The responded RREP has a compromise routing information (forged destination sequence number and small hop count) to convince the source to accept and trust the path as the best route for communicating with the target node. The source is reacting to the compromised node with data transmission, but unfortunately, the data never reaches the destination since the attacker drops the entire data packets.

3.3 Proposed Scheme

We have elaborated our proposed mitigation algorithm in two phases

3.3.1 Standard deviation outlier detection

An outlier is a data object that extremely diverges from the majority of data objects as if it were generated by a different mechanism[15]. To get meaningful data, outlier must be removed from the

dataset. Outlier detection like standard deviation removes all data objects that act differently from the expectation. In MANET, blackhole nodes manipulate two RREP fields; destination sequence number with extremely maximum value and hop count with the lowest value, therefore we treat these values as network outlier. Moreover, in our work, we considered a univariate dataset since we only deal with the destination sequence number. We apply an outlier detection on the dataset to obtain threshold as a control limit value that differentiates a real and bogus data. Each node contains the destination sequence number dataset of the RREPs it has received. The node before saving the RREP's destination sequence number, it firstly compare the current threshold value with the currently RREP destination sequence number, and if the threshold value is highest then the node will save the destination sequence number and compute the algorithm to acquire a new threshold for the next communication round, otherwise will detect the RREP as counterfeit, tumbling it and prevent the node to further participate in the network communication.

3.3.2 Controlling Attacking environment

To control the attacking situation a node that detected a blackhole node saves attackers id and advertises the id to the neighbors. Meanwhile, the neighbors will also save the attacker's id and share the attacker's information until the source node becomes aware of the attacker. The source node will re-broadcast RREQ to find another route for the same target node. Moreover, a node advertises attacker id if it is a new attacker, otherwise, ignore the RREP for the knowing attacker, and concentrate on other RREP packet. This helps to limit the massive generation of control packet that causes routing overhead and reduces data transmission delay. And if the RREP is genuine then data will be forwarded to the target node

Table 1 Blackhole attack mitigation algorithm in manet based on standard outlier detection

Notations
Th: Threshold value
DSQ: Destination sequence number
RREQ: Route Request Packet
RREP: Route Reply Packet

//Network free from attack within 15 seconds
1.Source node Broadcast RREQ packet to all neighboring nodes
2. Fetch and save DSQ from (RREP)
3. Perform Standard deviation on collected DSQ
4. Determine Threshold value using

$$Th = X_m + 3 \times SD$$

Where $SD = \sqrt{(\Sigma^{n}_{i=0}(x_i - x_m)^2 / n)}$

X - set of sequence number received in previous communication
X_m - mean value of a set of the destination sequence numbers
n - total number of the destination sequence number
SD - Standard deviation

//Network compromised after 15 seconds
7. The source node broadcasts the RREQ packet to all neighboring nodes
8. A node receiving RREP packet
If (DSQ>Th) {
Remove blackhole attacker and return to step 7
}
Else {
Unicast RREP packet to the source node
}
9. Forward data through the path
10.End

4 Performance evaluation

This section details the success of the mitigation algorithm we have suggested to thwart the blackhole nodes that have a serious negative impact on the network. We have examined the algorithm by comparing and analyzing it along with the AODV and AODV under the blackhole environment. Our work has been successful with the support of a network simulation tool NS-2.35[16]. Nodes are assigned with an initial position in the dimension of (1000x1000) meters, with maximum mobility speed of 5m/s and packet transmission rate of 10packet/second. Table 2 lists the simulation parameter value.

Table 2 Simulation parameters

SIMULATOR	Network Simulator 2.35
Number of Nodes	25,35,45,55,65,75,85, and 95
Area	1000m x 1000m
Communication range	250m
Packet Size	1001 bytes
Interface Type	Phy /WirelessPhy
Mac Type	IEEE 802.11
Queue Type	Drop Trail/Priority Queue
Queue Length	50 Packets
Antenna Type	Omni Antenna
Propagation Type	TwoRayGround
Routing Protocol	AODV
Transport Agent	UDP
Application Agent	CBR
Simulation Time	100sec
Mobility Model	Random Waypoint

4.1 Simulation results

1) Packet Delivery Ratio (PDR), based on evaluating currently data packets recorded in the trace file generated by CBR source and received by CBR sink at receiver. PDR is defined by the following equation.

$$PDR = \frac{P_{recv}}{P_{sent}} \quad (1)$$

where P_{recv} is the total data packets receiver received and P_{sent} is the total data packet source sent.
Here in Figure 3, details PDR performance for the original AODV, AODV as a function of blackhole nodes and proposed algorithm. Each network has a fixed 10% of the total node as a malicious node. Data presented in Figure 3 show that the data transmission process is severely affected when more blackhole nodes engaging in interrupting the process of the routing discovery, about 91.5% of data were dropped in AODV. However, deployment of our proposed blackhole attack mitigation algorithm based on standard deviation outlier detection outperforms AODV where it achieved dropping all fake RREPs and increases the packet delivery ratio in networks with an average of 92%. Furthermore, the algorithm shows its stability where PDR successfully improved on each network as the number of nodes increases.

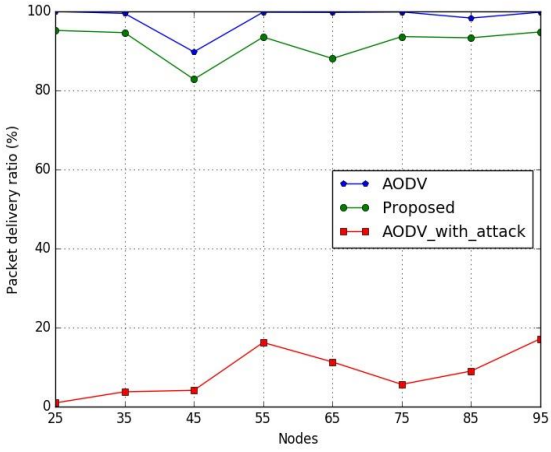

Fig 3 Comparison of packet delivery ratio

2) Throughput (TH), is the average of successfully data packets delivery over the radio channel. Throughput can be calculated using the below equation

$$TH = \frac{Psize*8*P_{recv}}{T} \quad (2)$$

where *Psize* is the data packet size, and *T* is the time elapsed from the time the source node receives the first RREP to the end of the simulation.

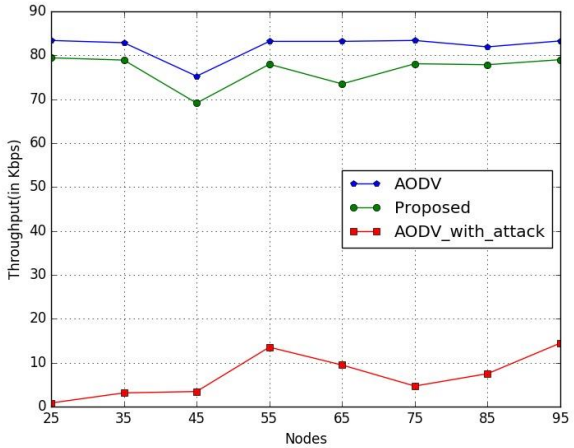

Fig 4 Comparison of throughput

Here in Figure 4 details the throughput performance for the proposed algorithm and AODV under the malicious node environment. In this figure, we use origin AODV without the presence of malicious node as our target performance to compare with remained two modified AODV protocols (means AODV with mitigating algorithm and AODV with blackhole nodes). The throughput performance in AODV_with_attack decreases since there is the engagement of dropping data packets, additionally

mobility of node leading to breakage of links hence this also affects the throughput on the network. Our work has contributed a better throughput performance compare to AODV as a function of blackhole attacks, regardless of the additional task of rejecting all blackhole nodes to secure the data route. Concludingly, the throughput performance of the proposed algorithm is less than that of origin AODV because the proposed method wrongfully discards some valid RREPs

3) Normalized Routing Overhead (NRO) is defined as the number of control packets used in routing discovery (RREQ and RREP) and maintenance (RRER) to a successful data received by the destination

$$NRO = \frac{R_p}{P_{recv}} \quad (3)$$

where *Rp* is the total number of routing packets sent over the network.

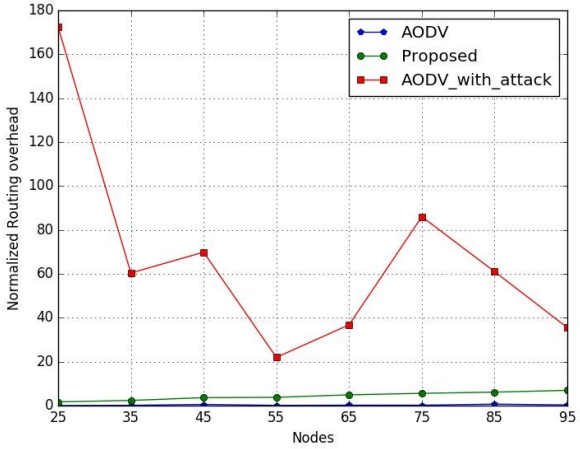

Fig 5 Comparison of normalized routing overhead

Figure 5 details that the proposed algorithm has a higher routing overhead than the original AODV but less than the attacked AODV. In this work, the source performs a routing discovery process more than once if a new blackhole node detected in the network. Therefore, this action contributes an additional RREQ packet on the network layer as the source eager to search for a valid route through re-broadcasted of the RREQ. Regardless, the output is agreeable since it has achieved a better performance than AODV with the attack.

4) Delay of network, defines how long it takes for a bit of data to travel in the network from one source to the destination through the following equation.

$$Delay = \frac{\sum (T_{recv} - T_{sent})}{P_{recv}} \quad (4)$$

where T_{recv} is the time when data packet arrives at the receiver, and Tsent is the time when data packet generated by a sender.

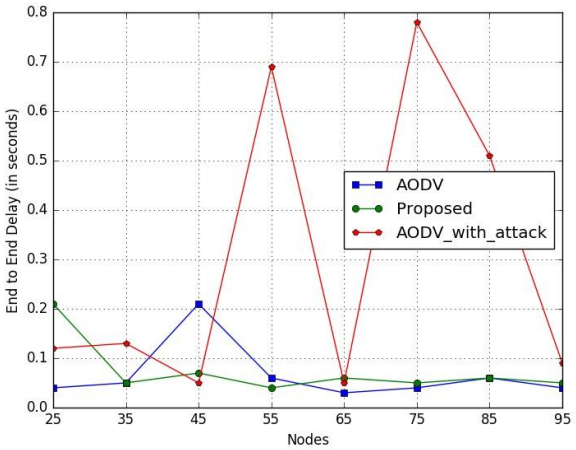

Fig 6 Comparison of average end to end delay

Figure 6, an end to end delay increases when AODV attacked with blackhole attackers. The result of the delay metric in our proposed algorithm varies where in some networks is slightly higher than the AODV, slight minimal than AODV and nearly similar to AODV. The effect of delay in our proposed work is because of RREP validation and advertisement of malicious node id until it reaches originator before rebroadcasting RREQ for the new data route. Therefore, despite additional computation on each node receiving the RREP, the algorithm can perform better in the delay context with an increase in the number of nodes than AODV with the attack, hence the output is reasonably acceptable

5 Conclusion and Future work

In a MANET, each node in the network is a master, which means that individually a node has full control over the network and it has caused AODV prone to multiple attacks. We propose an algorithm to eliminated multiple blackhole nodes to ensure the safety of the communication route from the source to the destination. The experimental simulation results show that the proposed algorithm effectively detects and mitigates blackhole nodes and above all, improves both performance metrics vs nodes. Further research is underway to test the performance of the algorithm with parameter mobility and pause time, and to farther improve the reduction in normalized routing overhead and end-to-end delay to implement this work for MANET's application.

References:

[1] T. Noguchi and M. Hayakawa, "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, 2018, pp. 539–544, doi: 10.1109/TrustCom/BigDataSE.2018.00082.

[2] A. Sharma and S. Jain, "A Behavioral Study of AODV with and without a Blackhole attack in MANET", International Journal of Modern Engineering Research, vol. 1, issue. 4, pp. 391-395.

[3] A. Sardana, T. Bedwal, A. Saini, and R. Tayal, "Black hole attack's effect mobile ad-hoc networks (MANET)," in *2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, India, 2015, pp. 966–970, doi: 10.1109/ICACEA.2015.7164846.

[4] Shaveta, P. Luthra, and Er. Gagandeep, "Implementation of blackhole attack under aodv routing protocol," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, 2017, pp. 575–579, doi: 10.1109/ICECDS.2017.8389502.

[5] S. Sharma and R. Gupta, "Simulation Study of Blackhole Attack In The Mobile Ad Hoc Networks," vol. 4, p. 8, 2009.

[6] S. Jain and A. Khuteta, "Detecting and overcoming blackhole attack in mobile Adhoc Network," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Greater Noida, Delhi, India, 2015, pp. 225–229, doi: 10.1109/ICGCIoT.2015.7380462.

[7] T. Noguchi and T. Yamamoto, "Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks," presented at the 2017 Federated Conference on Computer Science and Information Systems, 2017, pp. 797–802, doi: 10.15439/2017F101.

[8] L. Baghel, P. Mishra, M. Samvatsar, and U. Singh, "Detection of black hole attack in mobile ad hoc network using adaptive approach," in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, 2017, pp. 626–630, doi: 10.1109/ICECA.2017.8212741.

[9] S. Renuka Devi, S. Saraswathi, P. Yogesh, "A Cooperative Multilayer End-Point Approach to Mitigate DDoS Attack", WSEAS Transactions on Information Science and Applications, vol 11, 2014, pp.1-11

[10] T. Delkesh and M. Jabraeil Jamali, "EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs," *J. Ambient Intell. Humaniz. Comput.*, pp. 1–18, Mar. 2018, doi: 10.1007/s12652-018-0782-7.

[11] Y. F. Alem and Z. C. Xuan, "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," in *2010 2nd International Conference on Future Computer and Communication*, Wuhan, China, 2010, pp. V3-672-V3-676, doi: 10.1109/ICFCC.2010.5497455.

[12] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," 2013. [Online]. Available: https://tools.ietf.org/html/rfc3561.

[13] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," *IEEE Access*, vol. 7, pp. 95197–95211, 2019, doi: 10.1109/ACCESS.2019.2928804.

[14] A. Koujalagi, "Considerable Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocol in MANET (Mobile Ad Hoc Network)," *Am. J. Comput. Sci. Inf. Technol.*, vol. 06, no. 02, 2018, doi: 10.21767/2349-3917.100025.

[15] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed. Elsevier Inc, 2011.

[16] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*, 2nd ed. Springer US, 2012.