A Prefatory and Comparative Analysis of Black-Hole Attacks in MANET

Rajasekhar c
Computer Science and Engineering
Mount Zion College of Engineering
Kadammanitta Pathanamthitta, Kerala, India

Nisha Mohan P M
Computer Science and Engineering
Mount Zion College of Engineering
Kadammanitta Pathanamthitta, Kerala, India

Abstract:- The protection of the transfer of data packets between two wireless sensor nodes is being an integral element by security in WANET (Wireless Ad Hoc Network). Nodes have particular characteristics & add to major security architecture problems. WSN is being more security problems compared to other wireless networks; Messages, resources and its climate could be attributed to the existence of broadcasting. Black Hole Attack is being the traditional and main attack of WSNs. A form of a wireless network is being the Mobile Ad hoc Network (MANET) that offers different applications in various fields. The hottest issues have been MANET security in the world of networks. to different kinds of attacks is being vulnerable MANET that impair its connectivity and functionality. The most common active attacks that compromise efficiency is known to be the black-hole attack. AODV was strengthened by us in this analysis by implementing and unveiling A new lightweight technique for isolating and detecting black-hole attacks using timers and baiting that are single and cooperative. The MANET nodes are helped by the suggested approach to define and isolate the network's black-hole nodes during the complex topology transition. We compare several techniques in AODV for mitigating Blackhole attack. In this circumstance, in between source to destination may be presented by many malicious nodes. Consumed or lost are being simply all the packets through the malicious nodes.

Keywords:- *MANET, AODV, Black Hole Attack.*

I. INTRODUCTION

A core infrastructure that interacts is managed Between the network's nodes might manage the wireless communication network, or less infrastructure could be an infrastructure named Ad hoc networks. Cellular ad hoc network technology is a MANET. WANET which links mobile nodes with each other. In MANET, a central node does not rely on being a node but instead works together to transport data from nodes that do not directly access each other, to coordinate communications, or to carry data between them. In other words, a bridge may be worked by nodes among sender & receiver nodes when in the same coverage are not being sender and receiver. To a dynamic changing is being led by the mobility of nodes in a network topology. Routing protocols (RPs) of MANET are intended to respond to any complex changes in topology. Energy from MANET is one of the most significant communication considerations since there is a finite amount of energy in each node in the network; thus, we can deal with effective mechanisms and protocols to prevent any excessive use of energy [1]. Using a wireless link, MANET links nodes to each other, where an essential network resource is considered by bandwidth. The bandwidth of the wireless connection is bigger than that of wired smaller than that of communications. A vibration, interference from another signal, or the wireless link signal may be affected by fading [2]. To different kinds of attacks and risks is being prone by MANET. Since bind nodes are used wireless links by MANET together, an unauthorized person can access or change data and it is considered an eavesdropping danger. There is no central infrastructure in MANET that communication between nodes is managed, so to supply the destination node with data is dependent by nodes on themselves. A malicious attacker node, however, connection link or drop forwarded information can be changed. To be one of the most extreme attacks to MANET are being considered the attack against DoS (Denial of Service), in which battery of other nodes is depleted by a malicious attacker node, by telling them a large amount of data is to forward.

A. Manet Attacks

Due to the unavailability of centralized management security, lack of security mechanism in routing protocol, and open media, MANETs are vulnerable to many attacks. Attacks are grouped into two forms of MANET [3].

a. Internal Attack: To the domain of the network is belonged by the malicious node.

b. External Attack: In this type of network attack, doesn't belong to the attacking node.

Figure 1 below displays the various layers of MANET and their subsequent attacks.

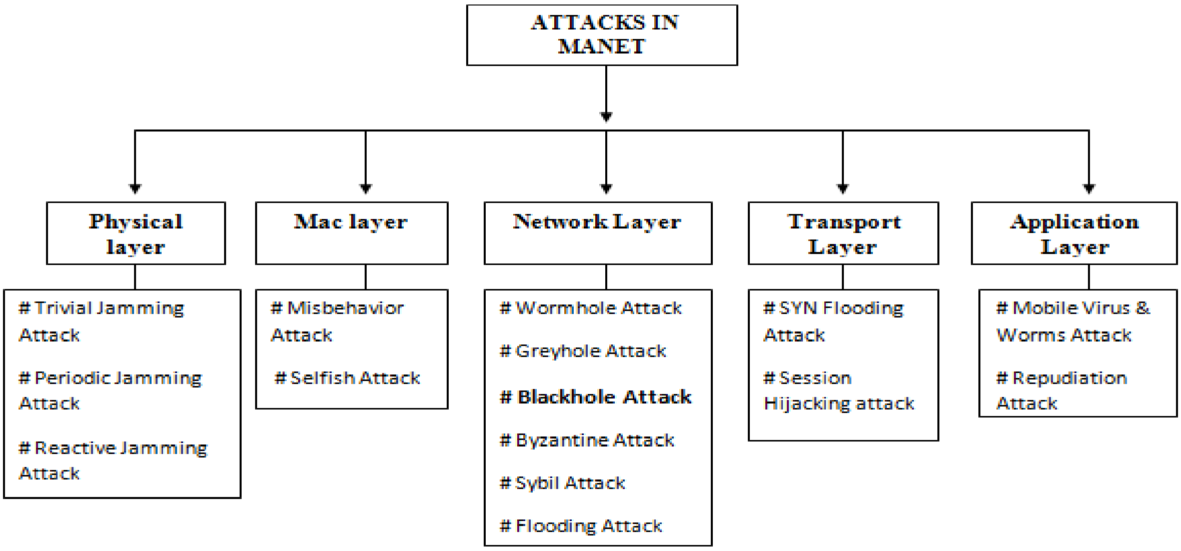

Fig. 1. Attacks in Manet

B. AODV (Ad hoc On-Demand Distance Vector)

AODV is MANET in on-demand or Reactive routing protocol. Bidirectional connections are commonly used by AODV. Unicast communication and Multicast communication are supported by AODV. To stop looping and as a criterion for route freshness, AODV uses the sequence number. The AODV protocol defines routes and, where possible, preserves the routes and does not preserve routes from one node to other nodes. In AODV, each node retains the sequence number and the nodes monotonically raise their sequence number any time there is a shift in the neighborhood network. In AODV, routing tables are used to store routing information. The routing table has parameters such as destination sequence number, a destination address, next-hop address, or lifetime. When a sender's computer needs to connect with the receiver device, the path discovery process in AODV begins. When the nodes find an established path, the sender first scans its routing table to find every available route to the destination, sends data to the next hop, and so on. And if the node does not find any path, the process for route exploration continues. In the route discovery process, RREQ (Route Request) packet is first broadcasted sender/source node to all its intermediate nodes. The intermediate nodes retain a reverse route table containing the sender's information after receiving the RREQ packet [4].

C. Blackhole Attack

A node is said to be a blackhole node in a blackhole attack as it attracts packets from source by defining itself to destination from shortest path as providing and a new route to the destination. By transmitting the packet to the source node is answered that initiates route discovery by spoofed path, Blackhole node may also be destination node [5]. It is an aggressive form of attack where the attacker node argues that even though it does not have any path to it, to any chosen node has been the shortest route in the network; therefore, through it is traveled by all packets and a black-hole node is helped to forward or discarding packets during the transfer of data. They broadcast is requested, any answer is trusted regular nodes and advantage of this is taken by black-hole node and proceeds to respond to any request believing that to the requested node has been the shortest route from it. In order destination node to find the route from it, nodes typically initiate the exploration process. A request is transmitted from source node to destination node, and every node this request is accepted to checks if to destination node has a new path from it. Once this request is answered by the black-hole node, automatically a reply is sent to the broadcaster saying that the destination node has been the newest and shortest path.

D. Main Challenge

To stop the harm that may be caused by various forms of threats, MANET protection is important. Most of the Common attacks are also known to be black-hole attacks that disrupt the network as well as attempt to prevent network connections. AODV routing protocol functions to search the shortest route in any 2 nodes who, when the path is necessary, want to communicate on the network. In the AODV protocol, no algorithm helps to detect & avoiding a black-hole attack.

II. LITERATURE SURVEY

In this section different state of the art method of blackhole attack has been described by us on AODV protocol in MANET. Various video watermarking methods have been presented in the literature. In this section, we will define techniques developed in the reactive routing protocol, particularly techniques of baiting against black-hole attacks, and the limitations of each technique, and how the developed technique can be overcome by smart black-hole attacks. We say that the attacker node understands the strategy utilized in terms of smart black-hole attacks and can use all its features against the attacker node.

S. Shrestha et al. (2020) To classify blackhole nodes also thus reduce the loss of data by discarding path with such Blackhole nodes, an algorithm centered on the approach of exchanging sequence number present in control packets, in particular, Route Reply (RREP) is generally utilized AODV routing protocol is proposed. The findings of the simulation demonstrate that proposed algorithm outperforms legacy IDS for AODV. For sharing of information is being a dynamic network by MANET b/w mobile nodes and its infrastructure-less design is being popular. In MANETs, however, due to the absence of national regulatory bodies, different security threats exist in comparison to their infrastructure-based counterparts. In MANETs, one of the most difficult problems of security is blackhole attack. By disrupting data flow between source & destination, a Blackhole attack dramatically reduces network performance. [6]

S. Pandey and V. Singh (2020) MANET, which deals with the complex nature of its development and is also a self-configurable form of network, consists of different configurations. In this type of networks, a mechanism for routing is to be developed by the primary task that owing to nature of ad-hoc network a high QoS parameter is given. Here, for the computation of the trust, uses of AODV is an on-demand routing mechanism. This suggested technique is used to detect blackhole attacks in-network by Support Vector Machine (SVM) & Artificial Neural Network (ANN). Findings supplied by us as Stable AODV are among black hole AODV and SAODV (security mechanism). Finally, on the various number of nodes checked the results, it has experimented with an increase in energy consumption of 54.72 percent for 100 nodes, the performance is 88.68kbps, the transmission ratio of packets is 92.91 percent and end-to-end (E2E) delay is around 37.27ms. [7]

V. Sharma et al. (2020) proposes, highly common attack i.e., blackhole attack is against to TCP analysis. Under the different circumstance, For the results of the Adhoc network attack analyzes to dependable transport layer protocol TCP. Using average throughput metrics has measured performance, Standardized load and E2E delay of routing & assumptions have been drawn based on this. Society and researchers have realized the need for information security in recent years, particularly in multi-path, unstructured networks like MANET. The connected devices in such a network are self-configured & small and can communicate in a lower infra-environment. Architecture gives the network challenges by making it more vulnerable to multiple risks and attacks to take benefit of the position of the network. [8]

H. Diab & A. M. El-Semary (2019) A protected routing protocol of MANET known as BP-AODV is proposed to resolve security breaches of SAODV Protocol along with initial AODV Protocol. Also, during the routing process, BP-AODV can protect against cooperative attack by black hole and defend against black hole attack during the forwarding process. BP-AODV is generated by expanding AODV protocol functionality along with the use of chaotic map features. That is assured by the experimental results the SAODV protocol is the most secure of BP-AODV protocol and During routing method, cooperative malicious nodes or malicious node may effectively combat blackhole attack. Findings also show that BP-AODV may strongly defend against blackhole attack that takes place throughout forwarding method. Even though routing protocol for MANETs broadly utilizes AODV, blackhole attack is being vulnerable. Lu et al. protected MANET routing protocol, called SAODV, has been developed to fix security flaws related to the initial AODV protocol & remedy the Blackhole attack. SAODV Protocol protects malicious nodes in its routing method from blackhole attacks. [9]

S. Sivanesh and V. R. Sarma Dhulipala (2019) black hole attack and simulating rushing were Proposed A benchmark review of the network layer attack Utilizing Network Simulator (NS-2). For a most susceptible attack to be calculated PDR (Packet Delivery Ratio) have been considered by them, E2E delay & performance as metric of evaluation. Here, for data forwarding operations has configured AODV routing protocol. Our Simulation Result Outcome, which is evident in comparison with the rushing attack, is more vulnerable to the black hole attack. For the past few decades, wireless networking technology has a global trend by MANETs. Such types of ad-hoc networks are less infrastructure, topology complex & often have no centralized network management, making it simpler for intruders to launch multiple attacks on MANETs. [10]

E. Elmahdy, et al. (2018) A new solution is proposed in MANETs to offer reliable & safe data transmission under probable blackhole attacks depends upon protocol and homomorphic security encryption scheme of ad hoc on-demand multipath distance vector (AOMDV). Performance of the proposed system is stable, but with the intervention of malicious network nodes, that of AOMDVV is found to be degrading. In our proposed method, the improvement of the PDR & network efficiency in presence of blackhole nodes is shown by simulation results that are susceptible to all forms of MANET attacks. Thus, a significant factor in promoting safe communication in a wireless environment between mobile nodes has been turned out by security. [11]

A. Kumari and S. Krishnan (2018) Where the nodes serve as both the node and the router fully autonomous Mobile ad-hoc network. In MANETs, It lacks centralization. Nodes are constantly traveling in MANETs and have open access at the cost of a large number of attacks are put. Therefore, a critical matter is a security in such networks. To be studied is needed Different attacks have been studied to search for a solution to this problem. In a Blackhole attack, packets are taken away from the unauthorized node in the source and the destination node path transmitted by the source drops them by not leading them to the target node. Blackhole attack deteriorates network performance launches the malicious behavior. [12]

M. B. M. Kamel et al. (2017) Improving the security of the routing protocol for AODV was proposed. The method isolates malicious nodes attempting to attack the network depends upon their prior data is isolated by the approach. To detect the degree of confidence of that node with every participating node attaches trust level. Examined to avoid a black hole attack will examine each incoming packet. This is a kind of network consisting of autonomous nodes that interact directly without a central controller or top-down architecture of the network. The lack of MANET base stations requires nodes to depends upon their neighboring nodes to transmit messages. The relationship between nodes is untrusted because node mobility is made by the dynamic nature of MANET. At the network layer, a denial of service attack can begin may be started by a malicious node instead of forwarding packets to the destination called black hole attack, discard packets [13].

S. R. Deshmukh et al. (2016) In the early stage of route exploration, an AODV-based secure routing mechanism is proposed to detect & avoid black hole attacks also affected routes. With RREP, a validity attribute is added to ensure that no attack occurs along the path. In NS2, the proposed approach is simulated & performance analysis is performed. MANETs are increasingly burgeoning with the use of mobile devices. MANETs' self-configuring and less proprietary infrastructure make them easy to deploy anywhere & highly dynamic. Lack of structured administration & teamwork is a reason why MANET is susceptible to active attacks, like a black hole. Blackhole attack is prevalent in both MANET and WSNs. Black Hole affected node spuriously reacts to the shortest route to destination without a significant actual path to the destination, also invites traffic to drop it. According to the protocol, it will not work if the network containing those nodes is used for routing. In MANET, widely used protocols such as DSR, AODV, & so on are not intended to tackle black hole attack or black hole affected paths [14].

M. A. Abdelshafy and P. J. B. King (2016) A Blackhole Resisting (BRM) Mechanism may be introduced for resistance to such attacks in any reactive RP. It doesn’t need costly authentication or encryption, however relies on timers and thresholds applied locally to recognize malicious nodes. There is no need to make any improvements to packet formats, so overhead is a limited number of nodes & no further communication. With NS-2 simulation, Network performance with and without our frameworks under AODV attack with blackhole attacks was comparable to SAODV, suggesting that the effect of black hole attack is reduced significantly. MANET routing protocols are built such that all nodes work together without interfering with the performance of RP. AODV is a reactive MANET routing protocol vulnerable to dramatic network collapse in presence of a black hole attack. An article suggests the concept of self-protocol trustworthiness (SPT) to make implicit malicious statements of malicious conduct in malicious intrusion by dealing with normal protocol conduct and the identification of malicious nodes [15].

III. COMPARATIVE ANALYSIS

We have analyzed a comparative approach in MANET with the black hole attack in this section. Various approaches were proposed in recent years to overcome single black hole attacks. But several detection methods neglect to discuss the problems of the cooperative black hole. Besides, some malicious nodes, hiding from the current detection scheme, work together to deceive the usual into their fabricated routing data. As a result, several cooperative detection systems are suggested to avoid coordination with black hole attack.

A. Black Hole attack under AODV Protocol

By connecting the attacker to the same node, the AODV protocol's throughput and PDR can be calculated with a Blackhole attack. There is a possibility that parameters, such as throughput, PDR, etc., will differ accordingly if an attacker needs a certain node. The efficiency enhancements can be shown below in Fig 2.

The average throughput is very high in the absence of the attacker, as we can see in the above graph so that most Packets that were transmitted from the source can reaching the intended destination without any loss of packets. Throughput is also high because there is no intruder during the transfer of data in a networking area. The average throughput in absence of an attacker is very high, as we can see from the graph above so that most packets sent from the source can get to the destination without loss packets. The throughput is also high because there is no intruder during the transfer of data in a networking area. Likewise, a green line showing throughput in presence of an attacker indicates that throughput steadily decreases when a node is targeted.

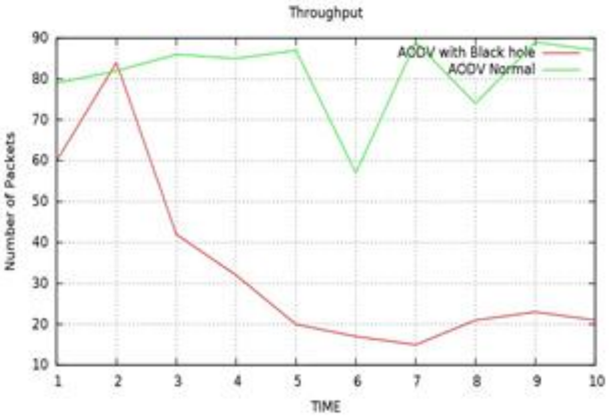

Fig. 2. Analysis of Throughput under AODV

The difference in output due to the intruder. In the sense that the packet transmitted by the sender fails to reach the destination. There is thus a drop in throughput.

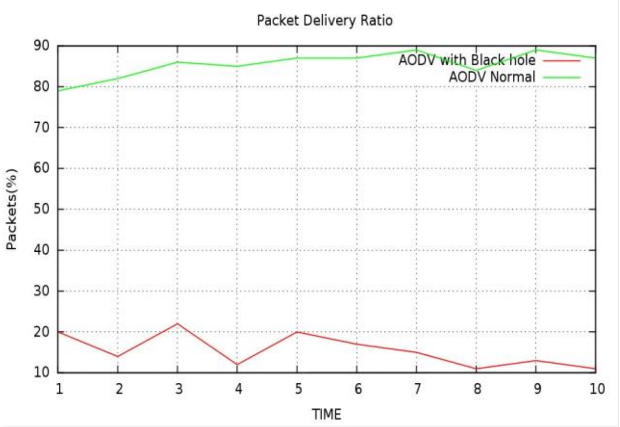

Fig. 3. Analysis of PDR under AODV protocol

In figure 3, You may also evaluate PDR by adding an attacker to each of the nodes using a similar approach. In this case, in the case of regular in absence of attacker, packet transmission, the distribution of the packet the ratio is very high in the transmission and stays stable. This indicates that the ratio of no. of transmitted packets to no. of received packets is very high. It is assumed that at the destination, all packets will be received. Although we can easily see that in presence of an attacker, the attacker receives packets from source & transmission of packets to destination has dropped to PDR to very low values.

TABLE I. COMPARISON OF SINGLE BLACK HOLE ATTACK DETECTION SCHEMES

Schemes	Simulator	Routing protocol	Results	Defects
Redundant Route & Unique Sequence Number Scheme [16]	AODV	NS-2	Verify 75 percent to 98 percent of routes	Attackers will listen to the channel & refresh final sequence tables. The Number
Neighborhood-based and Routing Recovery [17]	AODV	NS-2	The probability of one attacker may be identified 93 percent	Failed to forge false reply packets while attackers cooperate to
Random 2 hop ACK & Bayesian Detection Method [18]	DSR	GloMoSimbased	True positive rate may accomplish 100 percent when existing two witness	Proposed method is not effective when k equals to 3, minimizing true positives
IDS based on ABM	MAODV	NS-2	Packet loss rate may be reduced to 11.28 percent & 14.76 percent	Cooperative isolation malicious node, however, failed at collaborative black hole attacks
Improve QoS by proposed Trust based algorithm.	AODV	NS-2	Compare the performance of blackhole AODV with original AODV and Trust-based algorithm.	High end-to-end delay

Different detection schemes are described in sequential order for single black hole attacks. Table 1 indicates the comparisons between various systems. No matter what kind of routing detection is utilized, the attackers will bypass the detection mechanism. Consequently, to solve this problem, multiple key encryption or hash-based methods are used. The black hole subject remains an active research area.

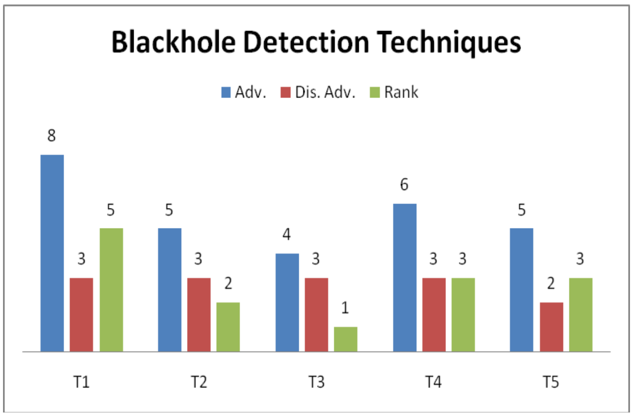

Fig. 4. Various techniques used to detect black hole attack

In the above graph, we define the Various techniques used to identify the black hole attack. Four scenarios of given parameters were taken with or without the black hole node for our simulation. For each case, we have adopted various positions and node movements. Then, to evaluate the results, we varied the blackhole nodes and simple nodes.

TABLE II. RANK OF BLACK HOLE MITIGATION TECHNIQUES

Techniques	Advantages	Disadvantages	Rank
T1 T2 T3 T4 T5	8 5 4 6 5	3 3 3 3 2	5 2 1 3 3

It calculates the ranks by counting the advantages and disadvantages of various techniques. In the AODV protocol, when there is no attack, almost all of the packets enter the destination. Almost all packets cannot reach the destination as we consider the attack. If a connection fails, a routing error is sent to sending node & the procedure repeats.

IV. CONCLUSION

We reviewed AODV in detail & the blackhole strike of AODV in this report. We calculate the effect of blackhole nodes on AODV on ad hoc networks. One of the most extreme attacks impacting the service of MANET is known to be a black-hole attack. Separation & detection of every black-hole node in the network is included as an important feature to avoid network failure. This work is helpful for researchers to know the various techniques used to avoid the black hole attacks and the positive and negative sides of those techniques. Also, it proves that if two or more effective techniques are combined to prevent black hole attacks, definitely it will reduce the black hole attack at an optimum level. We also analyze the impact of a black hole attack in MANET based on different performance matrices. In our future works, we will try to come up with a method for preventing & detecting collaborative black hole attacks in MANET. In contrast to the blackhole attack effect, we discovered that E2E delay with no black hole attack is marginally increased. In ad hoc networks, the identification of blackhole remains a difficult challenge.

REFERENCES

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

[2]. S. Barleen, S. Manwinder, “Detection and Isolation of Multiple Black Hole Attack Using Modified DSR,” International journal of Emerging Trends in Science and Technology IJETST, vol. 01, no. 04, pp. 540-545, 2014.

[3]. S. Aman, Y. Rakesh, K. Harjeet, “Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET,” International Journal of Innovative Research in Science, Engineering and Technology vol. 4, no. 5, 2015.

[4]. https://www.cs.jhu.edu/~cs647/aodv.pdf

[5]. K. Satoshi, N. Hidehisa, K. Nei, J. Abbas, and N. Yoshiaki, “Detecting Blackhole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method,” International Journal of Network Security, vol. 5, no. 3, pp. 338–346, 2007.

[6]. S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," 2020 8th International Electrical Engineering Congress (iEECON), Chiang Mai, Thailand, pp. 1-4, 2020.

[7]. S. Pandey and V. Singh, "Blackhole Attack Detection Using Machine Learning Approach on MANET," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp. 797-802, 2020.

[8]. V. Sharma, Renu, and T. Shree, "An adaptive approach for Detecting Blackhole using TCP Analysis in MANETs," 2nd International Conference on Data, Engineering, and Applications (IDEA), Bhopal, India, pp. 1-5, 2020.

[9]. A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019.

[10]. S. Sivanesh and V. R. Sarma Dhulipala, "Comparative Analysis of Blackhole and Rushing Attack in MANET," 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), Tiruchirappalli, India, pp. 495-499, 2019.

[11]. E. Elmahdi, S. Yoo and K. Sharshembiev, "Securing data forwarding against blackhole attacks in mobile ad hoc networks," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, pp. 463-467, 2018.

[12]. A. Kumari and S. Krishnan, "Simulation-Based Study of Blackhole Attack Under AODV Protocol," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, pp. 1-6, 2018.

[13]. M. B. M. Kamel, I. Alameri and A. N. Onaizah, "STAODV: A secure and trust-based approach to mitigate blackhole attack on AODV based MANET," 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, pp. 1278-1282, 2017.

[14]. S. R. Deshmukh, P. N. Chatur and N. B. Bhople, "AODV-based secure routing against blackhole attack in MANET," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, pp. 1960-1964, 2016.

[15]. M. A. Abdelshafy and P. J. B. King, "Resisting blackhole attacks on MANETs," 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, pp. 1048-1053, 2016.

[16]. M. Al-Shurman, S. Yoo S-M, Park, “Black Hole Attack in Mobile Ad Hoc Networks,” 42nd Annual ACM Southeast Regional Conference (ACM-SE’42), Huntsville, Alabama, pp. 2-3, 2004.

[17]. B. Sun, Y. Guan, J. Chen, UW. Pooch, “Detecting Black-hole Attack in Mobile Ad Hoc Networks,” 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, pp. 22-25, 2003.

[18]. D. Djenouri, N. Badache, “Struggling Against Selfishness and Black Hole Attacks in MANETs,” Wireless Communications & Mobile Computing, vol. 8, no. 6, pp. 689–704.