# Secure Scheme for The Isolation of Black Hole Attack in Mobile Ad Hoc Networks

**[1]Patience E. Idoga And [2]Usman Abdul Gimba**

[1 & 2] Department of Cyber Security
Federal University Dutse, Nigeria

Corresponding Author: dr.pat@fud.edu.ng

**Abstract**
*Black hole attack in MANETS is perpetrated by malicious nodes, using force to gain access to the route right from the source to the terminus via false publicity of shortest hop count in order to get to the last node. To avoid this, a secure scheme is crucial for unicast communication amid approved hosts in mobile ad hoc networks. When the safety of a specific network design is not appropriately planned from the onset, preserving privacy and other forms of safety becomes difficult. Hence, this study examined the black hole attack of mobile ad hoc networks and identifies secure mechanism in which black hole attack can be isolated in mobile ad hoc networks. This study reviewed recent articles retrieved from the Science Direct and IEEE data bases. The review was carried out from 3rd March, 2022 to 22th March, 2022. It was recognized from the review that various frameworks have been designed to detect and secure black hole attack in mobile ad hoc networks.*

**Keywords:** Mobile ad-hoc network, Black hole attack, Detection, MANETS, SEC-DSR, Secure

## INTRODUCTION

Wireless network provides flexible connection for users without the need for wired connections. Systems of wireless connections include; laptops, MP3 player, mobile phone and personal digital assistance (PDAs) etc [1]. Classification of wireless network is infrastructure network and Ad hoc Network [2]. Mobile ad hoc networks (MANETs) are a self-configuring network, requiring at least two mobile devices equipped with wireless communications. MANET is a non-infrastructure network with a centralized administration that can be deployed anywhere. However, this can only be possible where there is no fixed network infrastructure. There are no fixed number of nodes that can communicate on the network, the nodes can increase or decrease, making the network topology dynamic in nature [3]. Each node in a MANET is required to send packets; however, there is an exception when it is in use by itself. A crucial challenge in developing a MANET is furnishing each device to uninterruptedly preserve the data necessary to appropriately regulate congestion [4]. The MANET is equipped with mobile wireless communication technology. Other nodes within the radio range or outside the radio range can communicate with the nodes in MANET [5]. Dues to mobility and low cost, a MANET is suitable for

applications such as campus network, military services, vehicle networks, casual meeting, disaster relief, robot networks, emergency operations, maritime communications and so on [6].

The nodes in MANET perform two functions, the first is each node can act as a host and secondly as a router in other to find the quickest path to forward the packet to the right destination node. That is, each node is independent in nature. Nodes here can move quickly from any location to another. Consequently, it is possible not to find a path designed by a cause after a short period: that is, if an intermediary node changes course. MANET routing has been a thought-provoking job owing to the nodes fast changing topology [7, 8]. The nodes use some routing protocol to support its connectivity like Dynamic Source Routing (DSR), Destination-Sequenced Distance-Vector Routing (DSDV), and Destination Sequence Source Routing (DSSR) and Ad hoc on Demand Vector Routing (AODV) [5, 6]. According to [11, 12], ad hoc network routing protocol are of three types: Table-driven type (proactive), On Demand (Reactive) and Hybrid protocols.

For optimal performance of MANET's networks, its security has been observed to be a crucial concern. MANETs most often are prone to security bouts as a result of its specific characteristics such as exposed medium, topology dynamics, inadequate dominant observation and management, supportive procedures and unclear defense approach [13, 14, 15]. The Lack of MANET infrastructure makes it more prone to attack and opens opportunities for black hole hackers to launch different types of attacks on the network [16]. In view of this, this study aims to identify mechanism in which black hole attack can be isolated in mobile ad hoc networks.

## LITERATURE REVIEW

### Black Hole Attack

The black hole attack is an insider attack and one of the most treacherous attack in mobile ad hoc networks [10, 17]. The main issue associated with MANET when a black hole attack occurs is that, the confidentiality of data is exposed along with excessive network bandwidth consumption and exploitation of the routing protocol.

In a black hole attack, the attacker node advertises itself in MANET as a valid node. After it registers itself with MANET, it can listen to all broadcast route requests from all the nodes in the network. Once it gets the router request packet, the black hole node that wants to intercept a packet, replies to every route request by claiming that it has the shortest route to the destination node. The routing table of the sender node is updated and follows the path of the malicious node to send the packet. By doing that, the network traffic is redirected to the attacker node which in turn drops all. Once the black hole node gets the packet data, the confidentiality of data is disclosed [18, 19].

The most common network security threat for MANET or any non-infrastructure and infrastructure

network is Daniel of Service (DOS) attack, which is also considered as a black hole attack. One of the vulnerable security threat that could disrupt routing protocol is Black hole Attack [2]. Based on AODV, any intermediate node can respond to Route Request (R Request) message, has a fresh route, that can be checked by the destination sequence number contained in the R Request packet. The figure 1 represents the concept of the black hole attack.

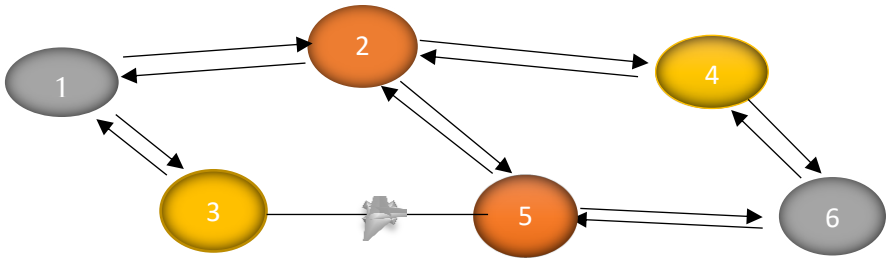


**Figure 1: Representation of a Black Hole Attack**

From the figure 1, the node 1 is the source node and the node 6 is the destination node of the MANET. Node 1, broadcast the route request packet into the network to get a route to node 6. The node 3 which is the black hole node, introduces itself into the MANET. Node 3 listens to the broadcast packet by 1 and reply immediately to node 1 before any other node. In this case, node 1 updates its routing table and use the node 3 route to send the data packet to node 6. Consequently, the node 3 intercepts all the data packets sent by node 1 to node 6 and dropped them. Hence, the confidentiality of the data packet is bridged and network bandwidth is consumed without achieving its objective due to interception of malicious node 3. This is called a black hole attack [20].

## METHODOLOGY

This research reviewed various related articles on mobile ad hoc networks and black hole attack. All reviewed articles (inclusion standards) in this study are those which studied Secure schemes, Black hole attack, MANETs, Mobile ad hoc security, Detection and elimination of black hole attack and written in English language only. On the other hand, the exclusion criteria are those papers without the use of the above-named search words. The articles were retrieved from the Science Direct database and the Institute of Electrical and Electronics Engineering (IEEE) database.

For the Science Direct database, the filter was set from 2008 to 2021, considering both full text articles and abstracts. Keywords such as "MANETs" and "Black hole attack" were used. The search realized a total of 2,080 articles. Another search was conducted for “Black hole attack in MANETs” without changing the parameters of the filter; mining also both abstracts and full text articles. Consequently, a total of 28 papers were realized. Adding the two searches, a total of 2,108 were obtained. However, it was established

that only 18 articles satisfied the inclusion standard.

The search from the IEEE realized 422 articles with the keyword MANETs, 11 articles with the search key "Secure schemes", yielding a total of 433 articles. For both searches, the filter was set from 2015 to 2021. After careful evaluation, only 10 articles satisfied the inclusion measures.
The review consisted of 28 articles and was conducted from 3rd March, 2022 to 22th March, 2022. The study provides few ways in which the black hole attack can be identified and mechanism to secure mobile ad hoc networks against black-hole attack.

**RESULTS AND DISCUSSION**

The number of articles reviewed in total was 28 and all these articles were written in English language. All the articles are of conceptual and experimental analyzes. It could be realized from studies [21, 22 & 23] that various frameworks have been designed to detect and secure black hole attack in mobile ad hoc networks. One of such framework is the SEC-DSR framework. The SEC-DSR framework is a non-cryptographic light weight mechanism. In this framework, when a node is receiving an R Request packet, each node in the MANET keeps record of the node details in the R Request packet route field. Additionally, in the SEC-DSR, when a middle node obtains an R REPLY validation for the active contribution of the rejoining node in the R Request advancing process to ascertain if the rejoining node is a black hole attacker or not. Depending on the outcome, a weight value is assigned to the responding node and forwards the R REPLY. Accordingly, all middle nodes in the R REPLY route, allocates a weight value for the responding node [5].

Another framework for identifying and securing black hole attacks in MANETS is through an accusation-based schema suggested by [24]. In this schema, a trust value is allocated by each node for other related nodes in the MANET network via the unceasing observation of neighbors and convey allegations to other nodes as soon as an unusual activity is detected in its environment. When the amount of charges is greater than the given threshold, the questionable node's credentials are annulled. This technique upsurge control packet overhead on MANAET network and also necessitates continuous supervision, resulting in rapid reduction of energy in the nodes [24].

Similarly, [25] suggested using the method "Timers and Bait Control Packets" for identifying black hole attack. Bait timer for each node is randomly set, such that, whenever the timer elapses, the node published a request packet in the network to an unreal node. The foundation node receiving an R REPLY for the bait request, instantly identify the replying node as a black hole attack.

Furthermore, [26] suggested a "Trust" approach called "ESCT" in order to truncate security bouts. Using this technique, individual nodes make the choice of alleged nodes and inform its shortest neighbors. When this is done, each node executes supportive

recognition and realize supplementary trust data to differentiate between actual and black hole nodes. The ESCT utilizes self-recognition, although, it alerts the trust data to each and every node in the system for supportive recognition of vulnerability that could transform to huge overhead. However, in comparison to the SEC-DSR, each node measure in the trust data along with the origin of the route in order to deplete the control packet broadcast overhead.

A Dynamic Source Routing Protocol (DSRP) is another way of detecting and isolating black hole attack in mobile ad hoc networks. This technique is an on-demand procedure requiring that as packets are sent by the source to the destination, routes are exposed. Route detection and upkeep are two basic functionalities of the DSRP. The DSRP function in such a way that at the time of route exposition, a route is recognized via bombarding the R Request in the network. The response is sent via the R Reply packet to the source as soon as the R Request packet is received at the destination node. This is accomplished by a reversal of the route data saved in the R Request. Is possible for any intermediate node to publish the R Reply to the initializing node if a route address is available [27].

On the other hand, at the point of the route maintenance stage, all link disruptions are resolved. When any middle node which is involved in the packet advancing procedure is not aligned with the broadcast range of its nearest neighbor then, a link disruption has occurred. If a node suspects a link disruption when advancing a packet, an error message is sent back to the initiating node detailing the link disruption. Either the initializing node attempts an alternative pathway or it begins a route detection procedure all over again [27, 28].

## CONCLUSION

Network safety is a crucial concern in MANET than in any other systems because of its exposed configuration and inadequate infrastructure. Recent studies on mobile ad hoc networks portray a hierarchical style, with the most interest on the securing of routing protocols. In this study, the mechanism to detect and isolate a black hole attack in mobile ad hoc networks has been discussed. The discovery technique against actual vulnerabilities in mobile ad hoc systems involves the gathering of safety-related information. Though, threats can also be found in safety-related information gathering. This studied identified a number of schemes designed to secure and isolate vulnerabilities in MANETS by thoroughly reviewing the literature on the prevailing black hole attack detection approach.

This study is constrained by factors such as fewer numbers of retrieved studies on black hole attacks and since the databases used for the review requires time to index, it is possible that very current studies on black hole attacks and mobile ad hoc networks are yet to be published.

**REFERENCES**

[1] C.E.Perkins and E.M.Royer, "Ad-Hoc on Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[2] N. Mittal and L. Chand, "Prevention and Detection Techniques under Black Hole Attack in MANETs: A Survey", *Advances in Wireless and Mobile Communications,* 2017 Available: ISSN 0973-6972 Vol. 10 pp. 551-558 [Accessed 29 March 2022].

[3] Anuj Rana, Vijay Rana, and Sandeep Gupta, "EMAODV: technique to prevent collaborative attacks in MANETs," Procedia Computer Science, vol. 70, pp. 137–145, 2015.

[4] N. Modi, V. Kumar Gupta, I.Rajput, "A Survey Paper On Detection Of Gray-Hole Attack in MANET", International Journal of Computer Science & CommunicationNetworks,vol.4, no. 1, pp.09- 12

[5] Mohanapriya, M., and R. Santhosh. "Detection and elimination of black hole attacks in mobile ad hoc networks." *Materials Today: Proceedings* (2021).

[6] N. Choudhary and L. Tharani, "Preventing Black Hole Attack in AODV using timer-based detection mechanism", *2015 International Conference on Signal Processing and Communication Engineering Systems*, 2015. Available: 10.1109/spaces.2015.7058198 [Accessed 29 March 2022].

[7] Dixit, Sweta, Krishna Kumar Joshi, and Neelam Joshi. "A review: black hole and gray hole attack in MANET." *Int. J. Futur. Gener. Commun. Netw* 8, no. 4 (2015): 287-294.

[8] B. Patel, "A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, no. 3, (2014), pp. 2816-2818.

[9] Roshan, Kumar, and Vimal Bibhu. "Preventive Aspect of Black Hole Attack in Mobile AD HOC Network." *International Journal of Computer Network & Information Security* 4, no. 6 (2012).

[10] Bibhu, Vimal, Greater Noida Campus, Pradeep Kumar Kushwaha, Akhilesh Kumar, Ram Manohar Lohia Avadh, and Bhanu Prakash Lohani. "Black Hole Attack in Mobile Ad Hoc Network and its Avoidance."

[11] K. Praveen, H. Gururaj and B. Ramesh, "Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols", *Procedia Computer Science*, vol. 85, pp. 325-330, 2016. Available: 10.1016/j.procs.2016.05.240 [Accessed 29 March 2022].

[12] Yaseen, Qussai M., and Monther Aldwairi. "An enhanced AODV protocol for avoiding black holes in MANET." *Procedia Computer Science* 134 (2018): 371-376.

[13] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning. " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[14] T. Clausen, C. Dearlove, P. Jacquet, and U. Herberg. "The optimized link state routing protocol version 2." (2014).

[15] Y.F.Alem, Z.C.Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010.

[16] S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs", *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017. Available: 10.1109/wispnet.2017.8300188 [Accessed 29 March 2022].

[17] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," Sixth Annual International Conference on Mobile Computing and Networking (MobiCom"2000), Boston, August 6-11, 2000.

[18] K. Arathy and C. Sminesh, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET", *Procedia Technology*, vol. 25, pp. 264-271, 2016. Available: 10.1016/j.protcy.2016.08.106 [Accessed 29 March 2022].

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

[20] A. Kavita, Kavita and V. Jain, "Impacts of Black Hole Attack on Mobile Ad-hoc Networks", 2020 international Journal of Future Generation Communication and Networking, 2020 Vol. 13, pp. 644–653, [Accessed 29 March 2022].

[21] Elmahdi, Elbasher, Seong-Moo Yoo, and Kumar Sharshembiev. "Secure and reliable data forwarding using homomorphic encryption against black hole attacks in mobile ad hoc networks." *Journal of Information Security and Applications* 51 (2020): 102425.

[22] Wazid M, Kumar A. A secure group-based black hole node detection scheme for hierarchical wireless sensor networks. Wirel Pers Commun 2017; 94:1165– 91. Doi: 10.1007/s11277-016-3676-z.

[23] Anwar RW, Zainal A, Outay F, Yasar A, Iqbal S. BTEM: belief based trust evaluation mechanism for Wireless Sensor Networks. Future Generation Computer Systems 2019; 96:605–16. doi:10.1016/j.future.2019.02.004

[24] Arboit, Genevieve, Claude Crépeau, Carlton R. Davis, and

Muthucumaru Maheswaran. "A localized certificate revocation scheme for mobile ad hoc networks." *Ad hoc networks* 6, no. 1 (2008): 17-31.

[25] Adwan Yasin, Mahmoud Abu Zant, Detecting and isolating black-hole attacks in MANET using timer based baited technique, Wirel. Commun. Mobile Comput. 1 (2018).

[26] Ruo Jun Cai, Xue Jun Li, Peter Han Joo Chong, ''An Evolutionary Self Cooperative Trust Scheme Against Routing Disruptions in MANETs", IEEE Trans. Mobile Comput, Vol. 18, P.42-55, 2019.

[27] Mohanapriya, M., and Ilango Krishnamurthi. "Modified DSR protocol for detection and removal of selective black hole attack in MANET." *Computers & Electrical Engineering* 40, no. 2 (2014): 530-538.

[28] Ming-Yang Su. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comput Commun 2010.