Multiple Black Hole Attack in Mobile Ad Hoc Network -Analysis and Detection

Harshini T[1], Somnath Sinha[2]
thirumurthyharshini@gmail.com[1],ssin.mca@gmail.com[2]

[1,2] Department of Computer Science
Amrita School of Arts and Sciences, Mysore
Amrita Vishwa Vidyapeetham, India.

Abstract. Mobile ad-hoc network is a short-lived and self-prepared wireless community including mobile nodes. Therefore, safety in MANET, the fundamental functionality of the network is of most critical concern. MANETs should be able to communicate easily and this is a very challenging and critical problem, because the threats to mobile networks are increasing. Protection in the Mobile ad-hoc Network is one of most complicated issues, given the lack of centralized authority and limited resources. In this document we have explored some available detection and prevention schemes A new approach to stopping MANET from black-hole attacks is suggested in this paper.

Keyword: Blackhole attack, Blackhole, routing protocols, detection, MANETs, centralized authority.

1 Introduction

Mobile ad hoc networks (MANETs), due to the challenges that the related standards pose, have become one of the most important fields of research in recent years. MANET is the new and emerging technology that allows users to communicate, irrespective of their geographical location, without the need for a physical infrastructure, which makes it sometimes known as the network for "less infrastructure." A self-organizing and adaptive ad-hoc network. Security is one of the most challenging issues in Mobile ad-hoc Network due to the lack of centralized authority and limited resources [1]. Device in MANET should also be able to detect the presence of many other devices and make the necessary arrangements to facilitate data and service communication and sharing [2]. Ad hoc networking enables devices to maintain network connections and remove gadgets from and to the network without any difficulty. Such factors gave MANETs excellent focus as well as the ability to configure themselves and sustain themselves. The unclear protection line, i.e., is another unique function of MANETs posing protective threats. No security built-in. The MANETs have no dedicated routers and switches, their nodes usually work with transmission without communication protection of packets to each other, providing access to both legitimate users and attackers. Node Source (S), for example, can be communicated with node Destination (D) using the shortest path S-J-I-d, as illustrated in **Figure 1**. If node J moves away from node S, the other route to node D (S-G-H-I-D) has to be identified. Security in MANETs is the main concern therefore for fundamental network functionality. Network services are available, confidentiality and data integrity can be achieved by ensuring security problems are met. Security attacks are often the result of MANETs because of their features, such as open media, a dynamic change in

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2303937

topology, the lack of central monitoring and management, cooperative algorithms and no clear protection mechanism. These factors altered the situation in the field of fighting security threats for the MANET [3].

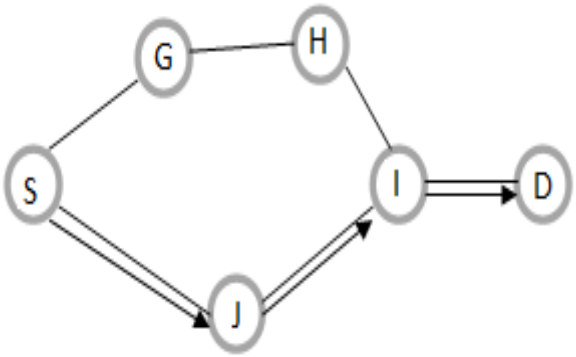


Fig. 1. MANETs communication among Nodes.

MANETs are more sensitive to such attacks, as communication is based on the shared confidence between nodes, network monitoring, authorization, a vigorous shift in topology and lack of resources is not a key point [3].

2 Literature review

In [4] mentioned about the weakness of AODV routing protocol and the possible vulnerabilities of black hole attack. Illustrated some simple and efficient detection and prevention techniques which require low overhead but high true positive value. One important observation to be mentioned here is that all these techniques are well working under single black hole attack [4]. For cooperative black hole attack more robust and complex detection schemes will require which are beyond the scope of the paper. The paper had shown, through simulation the attack scenario and the effect of the attack on throughput and packet delivery fraction and proposed detection techniques for the single black hole attack using trust value of the nodes [4].

In [5] authors focused on simulation study of RREQ flooding attack and its prevention mechanism in AODV routing protocol. The performance on the WLAN was analyzed by parameters such as throughput and end to end lag [5]. Flooding attack by other packets aside from RREQ packet isn't studied and also proposed a prevention method against this harmful attack [5].

In [6] It is essential to be able to determine the identity of the nodes participating in these networks, that the ad hoc mobile networks can be formed, combined or divided into different networks on a fly. In the operation of a Manet, it is also necessary to check whether a node has also been compromised [6]. The implemented detection mechanism allows local agencies to

collected and analyzed audit data, which enables the main operations of links and network layers. On the basis the data analysis and the transfer to the nearby nodes for further decisions, each agent assigns a compromised status [6].

In [7] mentioned AODV routing protocol is a DSDV protocol model for the dynamic hyperlinks. Each node in a wireless network keeps a routing table that includes information concerning the path to a specific target. Where a packet is sent through the use of a node, it first validates that a route to the target is already applicable with its authentication table. If so, sending the packets to the destination allows use of that direction. If a route is not available or the path entered before is disabled, a node is started for path exploration. A packet of (RREQ) Route Request is broadcast over the node. Each node receiving the RREQ packet first tests if it is the target of the packet and sends a packet RREP packet [7]. If not the way to go, the routing table must check. Otherwise it transmits the RREQ packet to its neighbors by broadcasting it. If a goal entry in the routing table, the next move is to determine the amount of the ' Destination list ' in the RREQ packet number available in the routing table. The broad series of the final packet from goal to source is a series. If the number in the table is higher than that of the packet, this means that the route is a new path and packets can be sent via it. The main node sends a RREP packet to the node that receives the RREQ packet [7]. The RREP packet is sent to the origin through the use of the opposite direction the origin node upgrades your routing table and sends your packet through this route. When a node identifies a hyperlink failure, a packet of RERR (Route Error) is sent during the operation to all other nodes using the link to communicate with various nodes. Because AODV does not have safety mechanisms, malicious nodes often attack by simply failing to comply with AODV rules. A malicious M node may execute a range of AODV assaults. This article guarantees the routing protection of the AODV routing method by minimizing the possibility of a Black Hole attack. [8].

In [9] The D-MBH algorithm proposed uses an incomplete RREQ an unspecified final address, calculates a DSN threshold and produces black Hole node list. In contrast to existing schemes, there is no significant improvement in overhead storage. Algorithm says when malicious RREPs are sent for source node attraction, noxious nodes should be detected when route discovery is done, to protect AODV from single as well as cooperative BH attacks [9]. Two single and collaborative BH attacks algorithms have been proposed to mitigate. Proposed detection of the D-MBH senses black-hole and multiple nodes, measures the threshold of DSN (ADSN), generates a List of BHs and calls for the suggested black-hole attack collaborative (B-CBH) algorithm. The proposed CBH algorithm uses ADSN, BH and hop data derived from the RREP to construct the CBH list. [9].

In [10] Described BH attacks where nodes are malicious violate the safety of the network and often cause loss of a packet to interrupt its normal operation. When these malicious nodes cooperate, the damage becomes more serious. There is a blackhole attack of two kinds, one known as a BH attack, and one known as a BH attack [10]. There are a few blackholes. BH attack is a sort of layer attack in which a route inquiry (RREQ) is waiting for a malicious node and the route answer (RREP) is waiting for the source as the quickest way to the last from other ends. The malicious node is provided to all the data that was destined for the Route if the source was selected to send data and data is sent via the chosen path. This leads to a loss of packet [10].

In [11] Secure knowledge algorithm proposed in the AODV protocol to reduce BH attack. Manets safety of moving nodes is challenging due to their specifications such as peer-to-peer architecture, battery life, computer capacity and heterogeneity, operation without central coordinators, dynamic topology, insecure operating environments and frequent interruption of the link. MANETs routing is viewed as reactive and proactive routing [11]. Whenever routes are required, a reactive protocol initiates and proactive protocols keep Compatible and up to date tables with routing information from each node. It is regarded as routing protocol reactive in this paper, such as AODV. Because of AODV's lack of security, malicious nodes may attack by breaking the protocol's specifications. The main AODV vulnerabilities are disappointing increases in sequence numbers and decreases in hop counts. BH Attack is a denial-of-service attack that redirects every packet to the network a certain node, which claims to have a new route, and absorbs or drops the packet to a certain node or destination. Paper concentrates on black-hole mitigation of AODV attacks by taking account of packet drop reasons [11].

In [12] Analyzed the impact of the AODV protocol blackhole attacks. Three metrics are simulated to show what the AODV is doing and how it is impacted by blackholes. The blackhole effect of AODV increases delay while performance and PDR drop. MANET contains several mobile nodes. For the purpose of communication, several routing protocols are designed [12]. Security is a key concern because of its versatility. Attack Blackhole attracts packets and gets all the packets you need to send to the destination instead that it drops the packets. The report concentrates on analysis of the AODV BH attack routing protocol. First, they have launched A BH attack in AODV, then the effect of BH attack on AODV was investigated in Measures like performance, delay termination, and packets delivery. [12].

In [13],[12] The analysis was carried out, the operation of the BH attack AODV protocol. The analysis showed a timely increase in AODV throughput when the nodes rise, but that the effects of blackhole attacks drastically decrease. When nodes rise, the total number of packets dropped for blackhole AODV is higher while normal AODV is smaller. The end-to-end latency and PDR are much higher for standard AODV relative to blackhole AODV.

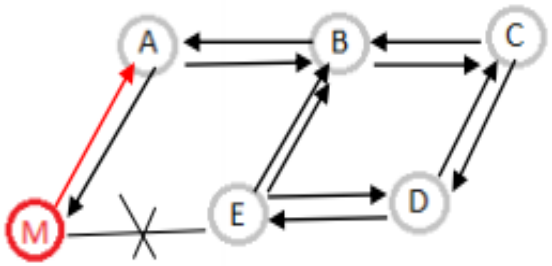
In [14],[12] In different performance parameters, the AODV impact of malicious nodes was analyzed. And according to simulations, With the development of nodes the performance for regular AODV rises, On the contrary for blackhole AODV it decreases. The AODV is less PDR than normal AODV and a blackhole attack is less PDF than normal.

In [15] analyzed that the Black hole Attack on various Parameters for efficiency, including overhead and the PDR of end-to-end delay. Two AODV and Improved AODV protocols were had analyzed in different intervals. The study assessed the performance of these protocols in the BH Attack. The results of the simulation show that IAODV is better than AODV. Twice compared to IAODV, the overhead of the AODV is affected. In addition, the malicious node effect on IAODV is lower than the AODV effect. Based on their simulation results research and analysis, we conclude that IAODV is more sensitive than AODV to Black hole assault. However, it is still a challenge to detect black hole attacks in wireless networks. During the simulation of a mobile node, a mobility system is used to define its location and speed change [15]. The only model commonly used and studied during the routing process. Protocol simulations is a random mobility model because of its simplicity and availability. Each mobile node is waiting at the beginning of the simulation Called for a while break time, tp and selects

one location by randomness[17]. After staying at their previous position, the MN chooses a new random target for a period from tp to its end. A node is moving through the region on a spontaneous speed uniformly distributed between v0 and vmax where v0, vmax are the lowest and highest node speed. This selection procedure at spontaneous speed is being replicated time and time until the simulation is done again complete[18]. We can say a node can be selected independently from nearby nodes for its destination, speed, and direction [15].

3 Problem statement

A blackhole attack has a two-way impact on the network. The node takes advantage of the ad hoc wireless routing protocol as a relevant path towards its destination, and then Consumes packets intercepted without transmission [1]. A node is using its protocol for routing in a Black Hole attack to advertise for a short the target road node. Instead of the routing table monitor, the aggressive node announces that it has new routes. In the attack, the attacker node is constantly able to respond to the path request so it can adapt and drop the facts packet.
The "A" node here wishes to convey with the "D" node and transmit data packs and the process of route discovery starts. The malicious node approach coupled and its results demonstrate how issues with the Black Hole arise. The M node is a malicious node and affects the pathway to the objective node when RREQ packets from the "A" node are received. The RREP is then sent before the other node to the "A" domain. It assumes that node "A" is often the active path to complete an active road discovery. Node "M" receives all data packets sent by node "A" and node "M" drops off all information packets in order to go node "A".



Reducing the number of hops or increasing the DSN of the Route Reply (RREP) packets.

DPRAODV (Dynamic, Prevention and Reactive AODV): To confront the Black Hole attacks. DPRAODV relates to the RREP sequence number and threshold value and updates their threshold value each time. The RREP sequence number value is suspected of being malicious if it is found to be greater than that of the threshold value and is combined with a list of blacklisted nodes.

Sequence number based scheme: Compares between the RREP of the next neighbor the source and number of sequences discovered by it. If the variation is too high and flaw is detected and the intermediary node is treated as malicious. Here two tables are maintained i.e., Route request and route reply tables and updates the table each time when a new packet is reached the sequence number.

ERDA (Enhancement Route Discovery for AODV) Scheme: Three parameters are combined 1. RREP_table to record the Route Reply "RREP", 2. MALI_LIST to trace any wicked or suspected node access, 3. RT_UPD table updates the routing table. The routing table update control is added.

(IDS) Intrusion detection system: This can be a network or a host-oriented technique. In this technique, a few nodes are treated as IDS nodes that are chosen for observing the RREQ and RREP packets in their communication range. This node will be blocked and this information is transmitted to all other neighbors in the network.

(**ABM) Anti-Blackhole Mechanism scheme**: In this technique, malicious nodes which selectively reach black hole attacks are detected and separated, by installing the IDS on the MANET. An ABM (Anti-Blackhole Mechanism) is achieved by all IDS nodes, evaluating the doubtful value of a node in the degree of unusual variations between RREQ and node-borne RREP.

Honeypot based detection scheme: Honeypot is a technology with higher potential for the range of network security. It can be used to diverts attackers and hackers distant from critical resources and It also use to study an attacker's techniques and instruments. It plays a role as a defend observation and recent warning instruments.

Watchdog solution: This detects malfunctions by holding a buffer that comprises packets recently sent.

(TOGBAD) Topology graph based anomaly detection: It's a hierarchical form for the detection of routing intrusion in multihop Networks Tactical. It is used topology graph Detection of anomalies for attackers attempting Routing attacks to launch [16].

BDSR Scheme: The BDSR recognize and prevents a BH attack depends on the merger of pro-active and re-active MANET Architecture of security using virtual and unexisting address to bait the malicious node in view of answer RREP. Baited's Black Hole Node responds to the RREP mechanism of BDSR. Malicious nodes can therefore early in the network be detected and blocked.

(S-ZRP) Detection by broadcasting the bluff probe packet: In the S-ZRP method numerous nodes in the black hole are identified and stopped, how the approach prevents the receipt and retransmission of the packets by the black hole nodes.

4 Ns2 implementation

NS2 is an ideal choice for checking out the effects of blackhole attack in MANET. Malicious nodes try and attract the information packets to bypass via it by using claiming fresh route through it and finally drop all the records packets, therefore decrease the network performance.

Table 1. Simulation Parameters

Parameters	Values
NS2	Versions 2.35
Simulation area	1000x500 (sq. m)
Simulation time	150s
Mac Layer	802.11
Routing protocol	AODV
Malicious Nodes Number	1-10
Radio Propagation channel	Two Ray Ground
Model of antenna	Antenna / Omni Antenna

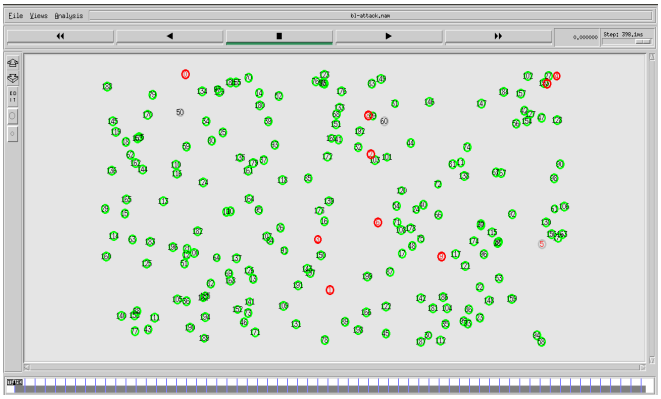


Fig 2. Simulation overview in NS2.

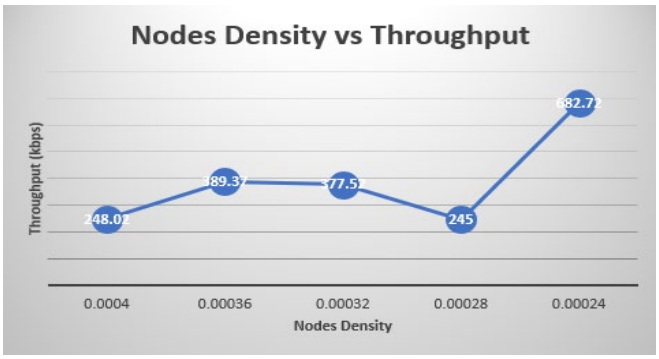


Fig 3. Throughput before BlackHole attack.

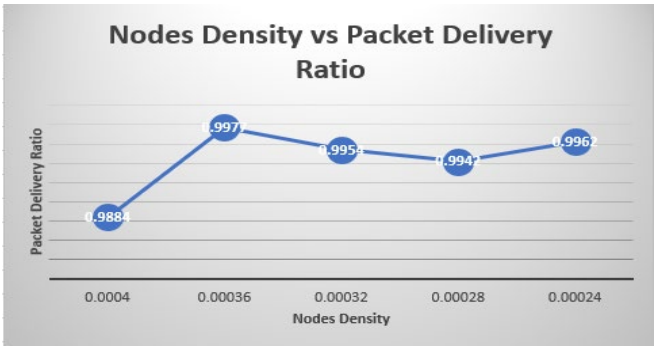


Fig 4. Packet-Delivery ratio (PDR) before implementing Blackhole attack.

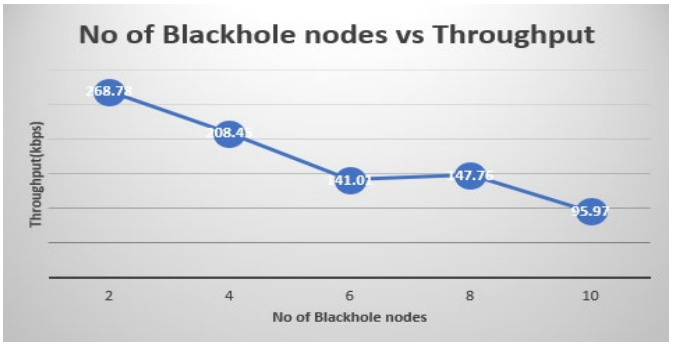


Fig 5. Variation of Throughput after implementing Blackhole attack.

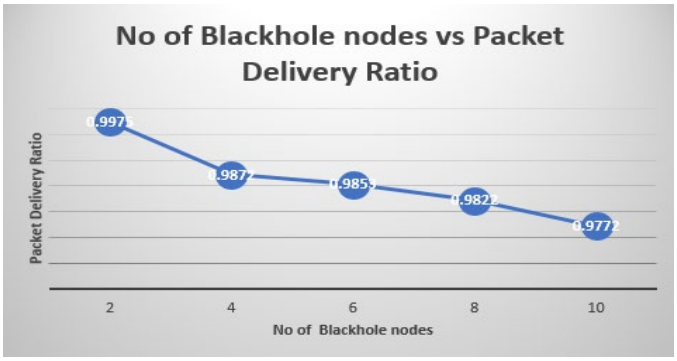


Fig 6. Variation of Packet-Delivery ratio after implementing BlackHole attack.

5 Prevention of attack.

A black-hole attack is created mainly using two different aspects, one by announcing the valid route from source to go to destination and by consuming the data packets passing through the nodes. Much work has been done so far on prevention of this attack but the accuracy level is not satisfactory. In our propose method to maintain the safest route through the neighbors every nodes maintain a reputation table based on the trust value given to the neighboring nodes. Before forwarding the data packets by any node the trust value has to be checked. The trust value is assigned to the nodes on the basis of individual nodes parameters collected by the centralized authority (CA). In MANET centralized authority is not preferable but to increase the security level CA is considered and every node can get the idea of trust value about their neighbors from CA.

6 Conclusion.

We have explored MANET's vulnerability and the possible vulnerabilities to a black hole attack in the current study. We demonstrate simple and efficient techniques for detection and prevention. Blackhole is recognized and prevention based on the proposed technologies is calculated in this implementation work. Before and after the attack behavior, the graphical representation is simulated. Prevention is also carried out by using the AODV routing protocol and the NS2 simulator. In future the author will attempt to investigate and compare the other current prevention mechanism.

References

[1] Sinha, Somnath, Aditi Paul, and Sarit Pal.: The sybil attack in Mobile Adhoc Network: Analysis and detection. pp 458-466 (2013).

[2] Sharma, S., Singh, U. K., Phuleriya, K. C., & Goswami, D. N.: SCAODV: A Protocol to Prevent Black Hole Attacks in Mobile Ad Hoc Networks. International Journal of Computer Science & Communication, 6(2), 36-41 (2015)

[3] Singh, U. K., Goswami, D. N., Phuleria, K. C., & Sharma, S.: An analysis of security attacks found in mobile ad-hoc network. International Journal of Advanced Research in Computer Science, 5(5) (2014)

[4] Sreelakshmi, K., Anand, S., & Sinha, S.: Black Hole Attack in Mobile Ad Hoc Network–Analysis and Detection. IJRTE Access, vol. 7 (2019)

[5] Lakshmi, H. N., Anand, S., & Sinha, S.: Flooding Attack in Wireless Sensor Network-Analysis and Prevention. IJEAT Access, vol 8 (2019)

[6] Komninos, N., Vergados, D., & Douligeris, C.: Detecting unauthorized and compromised nodes in mobile ad hoc networks. Ad Hoc Networks, 5(3), 289-298, (2007)

[7] Sharma, S., & Gupta, R.: Simulation study of blackhole attack in the mobile ad hoc networks. Journal of Engineering Science and Technology, 4(2), 243-250 (2009)

[8] www.ipcsit.com

[9] Arathy, K. S., & Sminesh, C. N.: A novel approach for detection of single and collaborative black hole attacks in MANET. In: Procedia Technology, 25, 264-271 (2016)

[10] Ranjan, R., Singh, N. K., & Singh, A.: Security issues of black hole attacks in MANET. In: International Conference on Computing, Communication & Automation, pp. 452-457. IEEE press (2015)

[11] Siddiqua, A., Sridevi, K., & Mohammed, A. A. K.: Preventing black hole attacks in MANETs using secure knowledge algorithm. In: International Conference on Signal Processing and Communication Engineering Systems, pp. 421-425. IEEE press (2015)
[12] Chaudhary, R., & Ragiri, P. R.: Implementation and Analysis of Blackhole Attack in AODV Routing Protocol. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, pp. 1-5. (2016)
[13] Kumar, S., Rana, D. S., & Dimri, S. C.: Analysis and Implementation of AODV Routing Protocol against Black Hole Attack in MANET. In: International Journal of Computer Applications, 124(1) (2015)
[14] Parmar, M. K., & Jethva, H. B.: Analyse impact of malicious behaviour of AODV under performance parameters. In: IEEE International Conference on Advanced Communications, Control and Computing Technologies, pp. 719-724. IEEE press (2014)
[15] Kumar, J., Kulkarni, M., & Gupta, D.: Effect of Black hole Attack on MANET routing protocols. In: International Journal of Computer Network and Information Security, 5(5) (2013)
[16] Gerhards-Padilla, E., Aschenbruck, N., & Martini, P.: TOGBAD—an approach to detect routing attacks in tactical environments. In: *Security and Communication Networks*, *4*(8), pp 793-806 (2011)
[17] K. Vijayakumar, Chokkalingam Arun, "Integrated cloud-based risk assessment model for continuous integration",Int. J. Reasoning-based Intelligent Systems", Vol. 10, Nos. 3/4, 2018.
[18] K. Vijayakumar, S. Suchitra and P. Swathi Shri, "A secured cloud storage auditing with empirical outsourcing of key updates", Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.