Prevention of Black Hole Attack in MANET: A Review

Arpit Bakshi[1], Rakesh Kumar[2]

[1]M.Tech (Scholar, CSE)

[1]NITTTR, Chandigarh, India, [2] NITTTR, Chandigarh, India,

[2]P.hd. (Assistant Professor, CSE)

Abstract: ***This paper has dealt with the studying MANET (Mobile ad hoc network) with its issues, characteristics and routing with the examination of black hole attack that result in dropping of messages. The black hole attack might take place because of the malicious nodes that are consciously misbehaving and has smashed node interface. In this paper, an overview of MANET has been presented with its issues, routing protocols with its characteristics. The concept of security attacks has been shown following black hole attack. A glance of existing techniques is being given of various approaches of Black hole attack proposed by researchers in their research with the techniques used for the mitigation of black hole attack.***

Keywords: MANET, Black hole attack, malicious nodes, routing protocols

1. INTRODUCTION

MANET (Mobile Ad hoc network) is known as the structure of wireless networks having movable nodes with the dynamically change topology [1]. It depicts the complex distributed system consisted of the collection of nodes of wireless that are linked by wireless links. It is an integration of decentralized mobile nodes which are not dependent on any static infrastructure [2]. Therefore, MANET is known as infrastructure-less ad hoc network. It has nodes that work as a router for the purpose of communication in the network. Because of the low cost and mobility, MANET is appropriate for the applications, like vehicle networks, emergency operations etc. Because of the dynamic topology and mobile nodes, routing in MANET is error prone as compare to the existing routing protocols [3]. The main aim of routing protocols in MANET is to set up an effective and favourable route among the communication entities. If any of the attacks messes with the communication than the full infrastructure will be damaged. The nodes in MANET are more vulnerable by means of security attacks than the traditional infrastructure. Numbers of attack are there by which the malicious nodes may harm a network with static infrastructure and later make it uncertain for communication. Black hole attack is one of those attacks. It is the one by which a malicious nodes exhibits itself with the shortest path towards destination in the network. It may cause DoS (Denial of Service) by reducing he received packets [4].

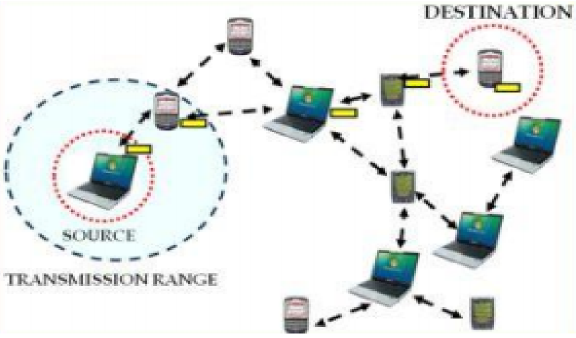

Figure 1 MANET (Mobile Ad hoc Network)

1.1 Issues in MANET

The various issues in MANET have been discussed below in tabular form [5].

Table 1: Issues in MANET

Issues	**Description**
Randomly Changing Topology	• MANET topology keeps on altering over the time. Therefore, one protocol which is suitable for one topology could not work the next time when topology gets dynamic. • The nodes executes in a nomadic environment in which the nodes are allowed to leave and join in the wireless network. • After the node came in the node's radio range, than it can communication with that node.
Limited Energy	• Nodes in the MANET have less battery power for the execution. • It is assumed that the nodes can transfer more traffic to the target node so that it can be busy in treating the packets. • Because of this, the

	nodes take more power and in the end, get exhausted so that the target node can provide the services.
No centralized control	• Because MANET has no centralized control over the network that can result to different security problems. • Every node behaves as client as server. • The environment of traffic monitoring has resulted in randomly and distributed changing environment.
Scalability	• The node that joins the network radio range may come and leave the network at any time. So, it is tough for someone to assume the nodes in the system. • The protocols being applied to the network has to be compatible for the static change of the network.
Threat from Compromised node inside network	• Due to mobility nature of MANET a malicious node can frequently change its target thus it is very difficult to identify malicious node in large network. Therefore, Threats from malicious node inside the network is much more severe than the threats from outside the network.

1.2 Routing in MANET

Routing Protocol is second hand to find suitable routes between communicate nodes [6]. It is a self-directed collection of mobile users that speak moderately over bandwidth constraint wireless link. Since the nodes are mobile, the network topology may change unpredictably over time [7]. The network is de-centralized and all the network activities like discover the topology and delivering messages must be execute by the nodes [8]. They do not use any access point to bond to other nodes .It must be able to switch high mobility of the nodes. MANET routing protocols could be broadly secret into three major categories as shown in table below [9]:

Table 2: Routing protocols in MANET

Routing Protocols	**Description**
Proactive Routing Protocols	• It possesses in order of the purpose route before it is needed for the routing of data to the purpose. • The benefit of these protocols is that a source node does not need route discovery actions to find a route to a purpose node. • Disadvantage of this protocol is, it is slow as it has vast amount of traffic as these have to maintain a reliable and up-to-date routing table which requires substantial messaging overhead and thus uses large piece of the bandwidth to keep information up to date. • The benefit of these protocols is that a source node does not need route discovery actions to find a route to a purpose node.
Reactive Routing Protocols	• A different proactive, reactive routing protocol does not make the nodes to start a route discovery process until a route to purpose is required. • The benefit of these protocols is that overhead messaging is reduced which results in less usage of bandwidth.
Hybrid Routing Protocols	• The hybrid routing protocols occupy both reactive and proactive property by maintaining intra zone information pro-actively and inter-zone information reactively • Often re-active or pro-active feature of a particular routing protocol might not be enough; instead a mixture might yield better solution.

1.3 Characteristics of routing protocols

There are number of routing protocols in MANET. Few of them are defined in the table below [10]. The comparison has been made on the basis of route acquisition, delay, flood and multipath capability for DSDV, DSR, ZRP and AODV [11].

Table 3: Routing protocols characteristics

Routing Protocols	**Route Acquisition**	**Flood**	**Delay**	**Multipath capability**
DSDV	Priority computation	NO	NO	NO
DSR	On demand when required	Yes (More usage of caching lessens flood scope)	YES	Not Explicitly (Can quickly restores a route)
AODV	On demand when required	Yes, Conservative for reducing scope of flood	YES	Not exactly, the recent research shows viability
ZRP	Hybrid	Outside a source zone	Only if the destination is out sourced	NO

2. Security Attacks In Manet

Similar to other networks, MANET also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself [12]. In MANET, security is a challenging issue due to the vulnerabilities that are associated with it. Intrusion detection is therefore incorporated as a second line of defence in addition to key based authentication schemes. The ranges of attacks that can be mounted on MANETs are also wider than in case of conventional static networks [13]. In mobile wireless networks there is no infrastructure as such and so it becomes even more difficult to efficiently detect malicious activities by the nodes inside and outside the network. The attacks could be broadly classified in two categories namely passive attack and active attack [14].

i. In passive attack, the attacker does not obstruct with the usual operation of the routing protocol, however, only get the information via listening to the network traffic.

ii. In active attack, the attacker changes the exchanged data that has deletion of the information too. Less attacks that are mostly encounter which disrupt the normal network behavior are worm hole, grey hole and black hole attack. In this review, we have focused on Black hole attack.

The focus of this review paper is on how the black hole attack can be analyzed and detected.

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [15]. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [16]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. After the establishment of route, the node will decide whether to drop all the packets or forward it to the unknown address. The method how malicious node fits in the data routes varies [17].

Below figure 4 shows the problem of black hole attack. In the figure, the node S is trying to send the data packet to node M and starts the route discovery process [18]. M node will proclaim it as an active route for the particular destination when it has RREQ packets received from the source node. Then it will send the response to the S node before some another node [19]. Node S believes that it is the adjacent active route to the destination and completion of active route discovery takes place. Node S ignores another replies and starts transferring the data packets to node M. The node M drops the data packets [20].

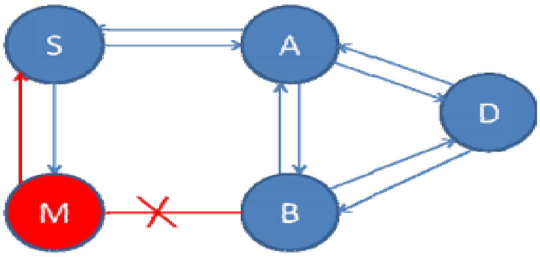

Figure 2 Black hole attack

Black hole is generally divided into two types [21]:

i. Single Black Hole Attack

In this type of attack, only single malicious node attacks on the route. The DSR protocol is susceptible to the well identified black hole attack.

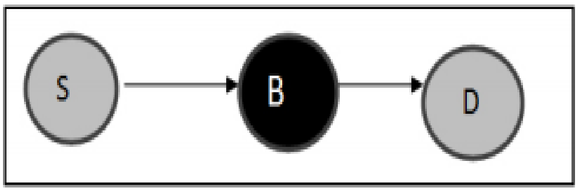

Figure 3 Single black hole atta

ii. Co-operative Black Hole Attack

This type of attack means that the malicious nodes operate in a group. In this, the more composite form of the attack is Co-operative Black Hole Attack in which the multiple malicious nodes conspire jointly resultant in complete disturbance of the routing with packet forwarding functionality of the network.

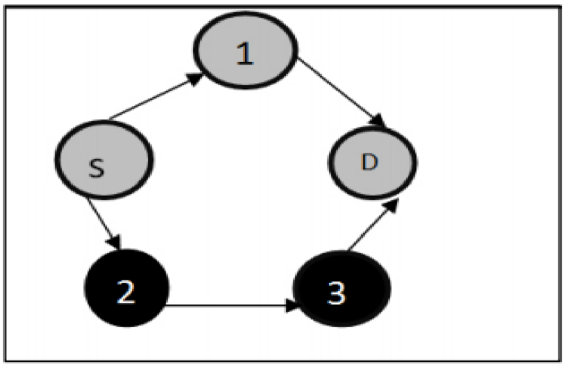

Figure 4 Co-operative black hole attack

The review of the techniques utilization of black-hole attack detection is shown in below table by considering three aspects, namely, Speed, Power utilized and performance [22]. The techniques discussed are, Cross layer cooperation, Trustiness and Neighbors, Route redundancy and Message Parameters, Fuzzy Logic, Mobile Agents and Clustering Algorithms [23].

Table 4: Summary of techniques used in Black hole attack

Techniques	**Speed**	**Power utilized**	**Performance**
Cross layer cooperation	Good	Low power utilized as computation level is less	Acceptable but cannot withstand in the co-operative attack
Trustiness and Neighbors	Good for black hole but slow in co-operative black hole attack	Moderate power utilized but more will be used in the centralized as compare to hybrid and distributed	Good with single black hole attack but cannot withstand in the co-operative attack
Genetic Algorithm	Moderate as soon as necessary data is presented	More power is utilized as the extensive output in these algorithms mainly in centralized node case	Good and could be utilized by means of co-operative black hole attack
Route redundancy and Message Parameters	Low with the use of multiple RREP with the sequence number in the process of detection	More power can be utilized for the processing of the control packets mainly in centralized strategies case	Good and secure
Fuzzy Logic	Moderate	More power utilized because of the heavy computation done on data for producing the attack degree in each node	Excellent and could be utilized with the cooperative black hole attack
Mobile Agents	Moderate	Moderate power utilized	Good and could be utilized by means of co-operative black hole attack
Clustering Algorithms	Moderate	More utilization of power	Excellent and could be used with cooperative black hole attack

3. RELATED WORK

Wei Li, (2010), has proposed a Genetic Algorithm based intrusion detection system which was tested with TCP/I networks. This made use of spatial and temporal29 ICRTIT-2012implementations of network based connections in encoding the network based rules. **Yuteng Guo, (2010),** discussed a method to improve detection accuracy and efficiency, a new Feature Selection method based on Rough Sets and improved Genetic Algorithms is proposed for Network Intrusion Detection. The effectiveness of the algorithm is tested on the classical KDD CUP 99 data sets, using the SVM classifier for performance evaluation. **Sheenu et. al, (2009),**investigated the effects of Black hole attacks on the network performance. The authors has simulated Black hole attacks in Quaint Simulator and measured the packet loss in the network with and without a black hole. The simulation is done on AODV (Ad hoc On Demand Distance Vector) Routing Protocol. The network performance in the presence of a black hole is reduced up to 26%.**Sanjay et.al, (2003),** has addressed the problem of coordinated attack by multiple black holes acting in group. The authors have presented a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. **Dokurer et. al, (2007),** has investigated the effects of Black Hole attacks on the network performance. The authors has simulated black hole attacks in Network Simulator 2 (ns-2) and measured the packet loss in the network. **Wahane, G., (2013)** has discussed mobile ad Hoc Network (MANET) as a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined organization of available links. This research work suggests the modification of Ad Hoc on Demand Distance Vector Routing Protocol. The proposed system has also decreased the end to end delay and Routing overhead. **Lu, Songbai, et al., (2009)** has discussed ad hoc on-demand distance vector routing as a widely adopt network routing protocol for Mobile Ad hoc Network. On the basis of AODV, this paper has proposed AODV suffering black hole attack, which can simulate black hole attack to MANET by one of nodes as a mean one in network. BAODV can be regarded as AODV, which is used in MANET exited black hole attack.

4. CONCLUSION

MANET has become a novel standard in infrastructure less network. In this network, the nodes get interlinked with each other with no access point. The messages are transferred and relayed among the nodes. Different routing algorithms are used for transferring the packets among indirect nodes means there is no straight range for intermediate nodes. These are impulsive in nature and centralized system absence formulates them susceptible for different attacks. The black hole attack is known as one of the attack having malicious nodes that plays itself as a better route towards the destination.

References

[1]. Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of the 6th annual international conference on Mobile computing and networking, ACM, pp. 255-265, 2000.

[2]. Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Computing and Information Sciences, I(1), 2011.

[3]. Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile ad hoc networks," Proceedings of the 42nd annual Southeast regional conference, ACM, pp. 96-97, 2004.

[4]. Kaur, Harjeet, Manju Bala, and Varsha Sahni, "Study of Blackhole Attack Using Different Routing Protocols in MANET," International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, II (7), 2013.

[5]. Yunwu, Wang, "Using fuzzy expert system based on genetic algorithms for intrusion detection system," Information Technology and Applications, International Forum, II, pp. 221-224, IEEE, 2009.

[6]. Yunwu, Wang, "Using fuzzy expert system based on genetic algorithms for intrusion detection syste," Information Technology and Applications, International Forum, IEEE, II, pp. 221-224, 2009.

[7]. Crosbie, Mark, and Gene Spafford, "Applying genetic programming to intrusion detection", Working Notes for the AAAI Symposium on Genetic Programming, pp. 1-8. Cambridge, MA: MIT Press, 1995.

[8]. Goyal, Anup, and Chetan Kumar, "GA-NIDS: a genetic algorithm based network intrusion detection system," Northwestern university, 2008.

[9]. Guo, Yuteng, Beizhan Wang, Xinxing Zhao, Xiaobiao Xie, Lida Lin, and Qingda Zhou, "Feature selection based on rough set and modified genetic algorithm for intrusion detection," In Computer Science and Education, 5th International Conference, pp. 1441-1446, IEEE, 2010.

[10]. Kozushko, Harley, "Intrusion detection: Host-based and network-based intrusion detection systems," Independent study, 2003.

[11]. Sharma, Sheenu, and Roopam Gupta, "Simulation study of blackhole attack in the mobile ad hoc networks," Journal of Engineering Science and Technology, IV (2), pp. 243-250,2009.

[12]. Sherif, Ahmed, Maha Elsabrouty, and Amin Shoukry, "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)," In Computational Science and Engineering (CSE), IEEE, 16th International Conference, pp. 346-352, 2013.

[13]. Sujatha, K. S., Vydeki Dharmar, and R. S. Bhuvaneswaran, "Design of Genetic Algorithm based IDS for MANET," Recent Trends In Information Technology (ICRTIT), International Conference, pp. 28-33, IEEE, 2012.

[14]. Michiardi, Pietro, and Refik Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks," European Wireless Conference, pp. 15-17, 2002.

[15]. Ramaswamy, Sanjay, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall E. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks," International conference on wireless networks, pp. 570-575. 2003.

[16]. Dokurer, Semih, Y. M. Erten, and Can Erkin Acar, "Performance analysis of ad-hoc networks under black hole attacks," SoutheastCon, Proceedings, IEEE, pp. 148-153, 2007.

[17]. Wahane, Gayatri, and Savita Lonare, "Technique for detection of cooperative black hole attack in MANET," Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference pp. 1-8. IEEE, 2013.

[18]. Medadian, Mehdi, Mohammad Hossein Yektaie, and Amir Masoud Rahmani, “Combat with Black Hole Attack in AODV routing protocol in MANET,” Internet, First Asian Himalayas International Conferencie, IEEE, pp. 1-5,2009.

[19]. Yang, Bo, Ryo Yamamoto, and Yoshiaki Tanaka, “Historical evidence based trust management strategy against black hole attacks in MANET,” Advanced Communication Technology (ICACT), 14th International Conference, IEEE, pp. 394-399. 2012.

[20]. Lu, Songbai, Longxuan Li, Kwok-Yan Lam, and Lingyan Jia, “SAODV: A MANET routing protocol that can withstand black hole attack,” Computational Intelligence and Security, International Conference, IEEE, II, pp. 421-425, 2009.

[21]. Tan, Seryvuth, and Keecheon Kim, “Secure Route Discovery for preventing black hole attacks on AODV-based MANETs,” ICT Convergence (ICTC), pp. 1027-1032, IEEE, 2013.

[22]. Dave, Dhaval, and Pranav Dave, “An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET,” Advances in Computing, Communications and Informatics, International Conference on, pp. 1690-1696, IEEE, 2014.

[23]. Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” Human-centric Computing and Information Sciences, I (1), 2011.

[24]. Dhote, Vimal, Anand Motwani, and Jyoti Sondhi, “A Review on Black Hole Attack in Mobile Adhoc Network,” International Journal of Computer Applications, 11, 2015.

AUTHOR

Arpit Bakshi, a research scholar in the field of computer science and engineering. He is pursuing M.E from NITTTR, Chandigarh. Presently, he is working as a Lecturer in Polytechnic College, Bikaner. He has completed his B.Tech from Bikaner Engineering College, Rajasthan Technical University, Kota in 2013. He is an active researcher and his areas of research are Adhoc Network, Wireless Sensor Network, Computer Network