| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 8, August 2020||

Security Issues of Black Hole Attack in Wireless Ad Hoc Network: An Overview

Nagendra Singh Tomar[1], Seema Shukla[2], Santosh Kumar[3]

Research Scholar, Dept. of Electronics &Communication Engineering, MITM, Bhopal, India[1]

Professors, Dept. of Electronics &Communication Engineering, MITM, Bhopal, India[2&3]

ABSTRACT: MANET is a type of wireless network that can be easily deployed anywhere in critical situations such as natural disasters, military operations, etc. Therefore, it is very useful and important in today's scenario. It has many practical applications. However, it is vulnerable to security attacks despite unique features. The security of the entire network depends on routing. It is not possible to find general solutions that can be used to detect black hole attack in MANETs.In this paper, we have included the main problem of MANET, black hole attack, the techniques developed in literature for its solution and the work that has been done earlier, we have included in this paper. And we have found a solution to this attack related problem.

KEYWORDS: MANET, AODV,security Attack, multipath AODV Performance Metrics, NS-2.

I.INTRODUCTION

In the early 1970s the Mobile Ad Hoc Network was known as the Packet Radio Network sponsored by the DefenceAdvanced Research Projects Agency (DARPA). They had a project called Packet Radio that had several wireless terminals built for communication with each other on the battlefield and this is where it started. These early packet radio systems preceded the Internet, and were part of the inspiration of the original Internet Protocol suite. In this age of today, infrastructure-less networks and mobility have become an area of new research and development due to their ad hoc nature. Due to the dynamics of wireless communication, security is the main issue in this network, due to which its performance is found to be decreased. There are many features of this mobile ad hoc network that make it different from other networks such as each node has autonomous behavior. Centralized firewall is absent. Network topology is dynamic in nature and does not require infrastructure to deploy it anywhere. Because of all these features of MANET, it attracts the attention of network researchers, but due to the lack of infrastructure and dynamic topology, some major problems and challenges of this network are also available which limit the performance and security of MANET.

Security attacks are an important issue in this network that has emerged as an important research area. Being a dynamic topology and wireless medium, it faces various types of attacks, understanding and resolving security attacks responsible for MANET is a concern. MANETs suffer from many types of security attacks and threats such as: denial of service, flood attack, impersonation attack, selfish node abuse, routing table overflow attack, wormhole attack, black hole attack, etc.

In this work, we have worked on one of the various security attacks on black hole attack and tried to solve it. This is the internal attack of the network by malicious nodes. This causes the link break within the network, in which case the data is not successfully delivered to the destination. These networks are vulnerable to attacks by malicious nodes. We need to ensure the integrity of the messages transferred from the source to the destination. There are possibilities that a malicious node may alter the message and pass it to the network resulting in either loss of data. And in some cases very little data is transferred. Therefore security parameters need to be implemented to protect MANETs from malicious users. The author presents a simulation-based study of the effects of attacks in MANET.

To overcome this security issue and eliminate the limitations of the single path routing strategy, multi-path routing strategy or alternative path routing is done. As the name itself suggests, it will have multiple paths between the source and the destination, through which data can reach the destination easily and easily. Routing algorithms are required to transfer data. Ad hoc on-demand distance vector routing is a very popular routing algorithm. Therefore, we have included it for data transfer in this work. However, it is vulnerable to a well-known black hole attack, where a malicious node incorrectly advertises good routes to a destination node during the route discovery process. This attack becomes more serious when a group of malicious nodes cooperate. In this work, a defense mechanism against coordinated attack by black hole nodes in a MANET is presented. In which the multipath based AODV algorithm is designed whose main goal is to receive maximum packets without loss.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 8, August 2020||

The rest of the paper begins with performance analysis of AODV & Multipath AODV routing protocol in MANET in Section II, III andsection IV, MANET Attacks, Literature Review and Problem Statement, Section-V, VII AODV, Multi-Path AODV and last section discussed about conclusion and References.

II.MANET ATTACKS

Attack is a very challenging task to secure a wireless network because of its features such as unreliable wireless communication, resource constraints, unknown topology before self-organizing and deployment, physical tampering, and unsafe environments. This section focuses on the attacks of MANET, its classification, and the methods initiated by them. MANETS are vulnerable to various types of attacks. A large number of possible attacks against MANET routing exist. These attacks include link spoofing, identity spoofing, man-in-the-middle attack, replay attack, wormhole attack, black-hole attack, routing table overflow attack, sibyl attack, and more. [1.] The purpose of these attacks is to interrupt routing decisions, and compromise communication to obtain sensitive information. In fact, MANET attacks can be divided into two major categories, passive attack and active attack.

1. Passive Attack: Passive attack is an e-bastion of data exchanged by an attacker without modification. Therefore, this attack does not disturb the functions of the network. So, this attack violates confidentiality and analyzes data that was gathered by eavesdropping. In addition, passive attack detection is difficult because it does not affect network operation. Such attacks can be controlled by the use of an encryption algorithm.

2. Active attack: Active attacks allow intruders to initiate intrusive activities such as modifying, injecting, forging, fabricating or dropping data, or shutting down packets, resulting in various disruptions in the network [5]. Some of these attacks are caused by an intruder's activity and others may be caused by a sequence of activities involving the intruder. Active attacks (compared to passive attacks) disturb network operations and can be so severe that they can bring down the entire network or significantly reduce network performance, as in cases of denial of service attacks. Is in The following is a description of the different types of attacks:

Wormhole Attack: In this type of attack, the two attacking nodes are connected to each other through a link known as a tunnel. The malicious nodes present on either side capture the packet from a valid node and, by escaping the packet, transmits it to another malicious node in the network. In a typical wormhole attack, the attacker receives packets over a point in the network, forwards them via wireless or wired links with much less than the default link used by the network, and then places them in the network. it depends on. In this paper, we assume that a wormhole with two endpoints is by-directional, although multi-end wormholes are possible in theory.

Black Hole Attack:A black hole attack is a type of service attack, in which a malicious node falsely absorbs all packets by falsely claiming a fresh route to the destination and dropping them without forwarding them to the destination. In such an attack the defective node advertises itself to be a new route to the destination and the shortest route without checking its routing table information. There are two types of black hole attacks in the network:

- **Internal black hole attack:** Here a defective node exists inside the network. It actively participates in communication of source and destination. This is called an internal attack because the malicious node is internally related to the network. This attack is more serious because the malicious node actively participates in the network.
- **External black hole attack:**Here the faulty node remains outside the network and denies access to network traffic. This attack can become an internal attack when it takes control of an internal malicious node and controls it to attack other nodes in the network.

Gray hole attack: This attack is also known as a routing misbehavior attack that leads to packet drop. This is a two stage. The node advertises itself as having a valid route to the destination during the first phase, while in the second phase, the nodes release intercepted packets with a certain probability. The attacker behaves maliciously for a period of time until the packet is dropped and then changes to its normal behavior. Both the common node and the attacker are the same. Due to this behavior it is very difficult to detect in the network to detect such an attack. The second name of the gray hole attack is the node misbehaving attack [12].

Flooding attack: In flood attack [9], the attacker exhausts network resources, such as to consume bandwidth and node's resources, such as interrupting routing operations due to computational and battery power or severe degradation of network performance. For example, in the AODV protocol, a malicious node may transmit a large number of RREQs

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 8, August 2020||

in a short period of time to a destination node that does not exist in the network. Because no one in RREQ will respond, it will fill the entire network.

Denial of Service: Denial of service can send so many unnecessary repeated requests to a server so that the server crashes due to heavy load. The attacker can interrupt or delete a server's response or client's request and assume the server is not responding. This slows down the network or disrupts the service of a system.
Man in Middle Attack: In this attack, the malicious node places itself between the source and the destination. Then, catches all the packets and drops or modifies them. Hop by hop communications has been made sensitive to MANET against this attack.

III. LITERATURE REVIEW

Literature review is the major task of all research. By this, the basic problem in the field of research work was found here. This chapter reviews research by MANET Black Hole Security Attack and its various authors working in the field of solutions. We have read some research papers and conceptualized the mind and focused on the work of such an attack prevention plan.

Vinay Singh et. al. [1] presented a "Survey: Black Hole Attack Detection in MANET, describes the issues of black hole attacks", describes major issue in MANETs. In this paper discus some important technique used to detect the black hole attacks in MANETs using AODV routing protocol and their merits and demerits which play major role for future research.

Zulfiqar Ali Zardariet. al. [2] presented a "A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs", Describes a major technique, called dual attack detection for black and gray hole attacks for MANETs. The proposed DDBG technique selects the intrusion detection system node using the associated doming set technique with two additional features; the energy and its existence in the blacklist are also tested before inserting nodes into the IDS set.

AbdulsalamAlsmadyet. al. [3] presented a "Black Hole Attack Prevention in MANET using Enhanced AODV Protocol", Describes that one of the major attacks in the MANET is a black hole attack, this attack is classified as one of the Denial of Service attacks. This paper proposes an enhanced approach using the AODV protocol to prevent the effect of black hole attack in MANET. The results suggest that the proposed approach has a better result than the current one in terms of overhead, packet delivery ratio and end-to-end delay.

HoudaMoudniaet. al. [4]presented a "Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET", Describes the traditional way of protecting wired or wireless networks with infrastructure, it is not directly applicable to MANETs. Since prevention techniques are never sufficient, the use of an intrusion detection system is a major importance in MANET protection. In this paper, a new scheme is proposed for mobile ad hoc networks using an adaptive neuro fuzzy interference system and particle swarm optimization for black hole attack detection.

SandeepLalasahebDhendeet. al. [5]Presented a "A Survey on Black Hole Attack in Mobile Ad Hoc Networks", Describes the routing security problems of MANET and investigates "black hole attacks" that can be easily employed in detail against MANET.

Danista Khan et. al. [6]Presented a "Study of detecting and overcoming black hole attacks in MANET: A Review", Describes various network layer attacks. Worm holes, black holes, gray holes, Byzantines, and Sibyl attacks are some examples of network layer attacks that destroy network topology resulting in data loss and network degradation. In this paper, we have discussed various techniques that can be used to detect and prevent MANET from black hole attacks. In a black hole attack, a node declares itself to be the closest route to all destinations. This node absorbs all the data packets of the network using routing protocols and thus reduces network performance.

SandeepDhende*et. al. [7]*Presented a "SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs",Describes security attacks; Some of them are black hole and gray hole attack. One of its major challenges is the attack of the black ND black hole. In this paper, researchers proposed a secure AODV protocol (SAODV) to detect and remove black holes and gray hole attacks in MANTE. The proposed method is simulated using NS-2 and it seems that the proposed method is more secure than the existing one.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 8, August 2020||

Taku Noguchi *et. al. [8]*Presented "Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks", Describes a new threshold-based black hole attack prevention method. To examine the performance of the proposed methodology, we compared it to existing methods. Our simulation results show that the proposed method outperforms existing methods from the point of view of black hole node detection rate, throughput, and PAX delivery delivery rate.

LokeshBaghel*et. al. [9]*Presented "Detection of Black hole Attack in Mobile Ad hoc Network using Adaptive Approach", Describes the black hole attack and its effects. This attack of a black hole in the network can be easily deployed by an adversary. It can be felt that the proposed work is more secure than the already existing solutions. We also assimilated its performance with some standard AODV routing protocols. The experimental results suggest that the proposed approach is far better and acceptable than the standard AODV.

Mohamed A. Abdelshafy*et. al. [10]*Presented "Resisting Black hole Attacks on MANETs", describes a new concept of SPT in which the detection of a malicious intruder is accomplished by following normal protocol behavior and exposes the malicious node to its malicious behavior. We present a black hole resistance mechanism (BRM) to resist such attacks that can be incorporated into any reactive routing protocol.

Mohamed A. Abdelshafy*et. al. [11]*Presented"A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET", Describes a novel strategy to detect single and collaborative black hole attacks with reduced routing and computational overhead. The proposed D-MBH algorithm detects a single and multiple black hole nodes that use an additional routing request with non-existent target addresses, computes a threshold ADSN, constructs a black hole list, and proposes D -CBH invoices the algorithm. The D-CBH algorithm creates a list of associative black hole nodes, using ADSN, black hole list and next hop information extracted from RREP.

Shruti Singh et. al. [12]Presented "A Survey on Black Hole Attack in MANET", Describes the security characteristics, security is a very important feature during the implementation of MANET or other networks. MANET is widely used in our daily life such as meeting, conference, medical emergency ood, large emergency situations like earthquake and military operations. In this chapter we discuss security services in MANET. We also discuss security attacks at various levels and our major concern about the network layer attack is on the black hole attack and its current solutions.

Muhammad Imran et. al. [13] presented a "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks", Describes a detection and prevention system for black hole attack detection in MANETs. For this purpose, we deploy some specialized nodes in the network called DPS nodes, which continuously monitor RREQs transmitted by other nodes. DPS nodes detect malicious nodes by observing the behavior of their neighbors. When a node with suspicious behavior is found, the DPS node declares that suspicious node a black hole node by transmitting a threat message. Therefore, the black hole node is separated from the network by rejecting all types of data. Simulations in NS-2 show that our proposed DPS mechanism has reduced the packet drop ratio with a significantly lower positive rate.

HetaChangela*et. al. [14]*Presented a "Algorithm to Detect and Overcome the Black Hole Attack in MANETs", describes the effect of black hole attack in AODV-based networks has been studied. Throughput, packet distribution fraction (PDF) and network parameters from average end to delay are calculated with a normal network (without a black hole) and a network with a black hole.

Nilima H Masulkar*et. al. [15]*Presented"An Improved Multipath AODV Protocol Based On Minimum Interference", describes the minimal interference multi-way routing protocol for MANETs based on the AODV protocol. The main goal of the propose method is to determine all node-disjoint routes from source to destination with minimal routing overhead. When the route is broken, the data is continuously transmitted through another route. Also in selecting the node-dystrophic path; The protocol also takes into account the energy and distance of the intermediate node to extend the lifetime of the network.

Outcome of Literature Survey: From a review of the literature, it is revealed that MANET is one of the most important technologies of the future in the field of computer networks. This technique is very useful and can be easily applied in the whole environment etc. Using mobile ad hoc network is quite many cial, but it has many challenges like mobility, security. Security is a very essential feature of any network during deployment. Main issues of security threats or attacks in ad hoc networks. In this article, we discuss about MANET and it specifically deals with the challenges and security attacks aboutblack hole attack with its existing solutions. Through literature we have found a multipath strategy, and this concept has used our work.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 8, August 2020||

IV.PROBLEM STATEMENT

Through some papers in the previous chapter, the author comes to know about several security challenges in MANET, one of them is black hole attack. The literature found that this attack is caused by malicious nodes. Malicious nodes have a detrimental effect on the network. Density plays an important role to mitigate the effects of a security attack. The reliable source-based AODV routing protocol given for the MANETs approach is efficient and adaptable.
In addition this work focuses on addressing the performance issue in MANET. This is not very effective due to improper selection of malicious nodes. A black-hole attack in a mobile ad-hoc network is caused by malicious nodes, which attract data packets by incorrectly advertising a fresh route to the destination. Therefore some improvement on this proposed methodology is needed to provide security in MANET.

V. AODV ROUTING

AODV routing algorithm is designed for MANETs. It is used on demand strategy, means when builds path between desired by every source nodes. It maintains these paths or routes when they are needed by the sources [3, 5]. AODV make routes using a route request or route reply query cycle. If destination node initiates for packets to source node, it does not have a route then broadcasts RREQ packets across the network. Nodes receiving data packet and update information regarding network nodes for the source node and set up backwards paths in the route tables.As long as the route remains active means data packets periodically travelling from the source to destination. Once the primary nodes stop sending data packets, if the links will time out and eventually to be deleted from the mediate node routing tables. If a link break occurs while acknowledge RERR message to the primary node to inform it of the now unreachable destination [1, 3, 6]. AODV routing protocol offers a quick adaptation to dynamic link conditions, low processing and memory overhead and low network utilization. It avoids problems associated with classical distance vector.

VI. PROPOSED MULTIPATH AODV

Inthis work, single path on demand routing algorithm extended to multipath routing algorithm in given below. In multipath aodv provide an alternative path for data transmission. In multipath each source node and destination node have a set of paths which consist of a multiple path if primary path fails reinitiate the protocol and search one or more alternate paths. Multipath routing protocols generally are considered more reliable and robust than single-path routing protocols [18]. Furthermore, whenever a link failure is detected on a primary route, the source node can select the optimal route among the other available routes. This mechanism enhances route availability and consequently reduces control overhead. It also enhances data transmission rate, and increases the network throughput. In multipath AODV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. Multipath AODV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. On demand multipath protocols discover multiple paths between the source and the destination in a single route discovery process. A new route discovery is needed only when all these paths fail. In contrast, a single path protocol has to invoke a new route discovery whenever the only pathfrom the source to the destination fails. Thus, on demand multipath protocols have fewer interruptions to the application when routes fail.

VII. CONCLUSION

We studied the problem of black hole attacks in this paper. Many researchers have developed various techniques to suggest different types of prevention mechanisms under the black hole problem. And studies have shown that AODV has done well in diagnosing this problem. According to this work, we look at how the AODV routing protocol works and then implement a black hole attack on a trust-based MULTI PATH AODV mechanism to prevent it at the same time.Our full implementation shows that the proposed method of trustThe mechanism applied to the AODV protocol gives better results in all cases of MANETCompared to normal AODV in case of black hole attack.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

||Volume 9, Issue 8, August 2020||

REFERENCES

[1] Vinay Singh, Dr. Ajit Singh and Malik Mubasher Hassan "Survey: Black Hole Attack Detection in MANET" 2nd International Conference on Advanced computing and software engineering (ICACSE-2019) Page-522-525.
[2] Zulfiqar Ali Zardari, Jingsha He, NafeiZhu "A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs" Future Internet 2019 Page-2-17.
[3] AbdulsalamAlsmady, HadeelAlazzam and Areej Al-Shorman "Black Hole Attack Prevention in MANET using Enhanced AODV Protocol" Conference DATA'19, December 2–5, 2019, Dubai, United Arab Emirate Page-2-7.
[4] HoudaMoudnia,∗, Mohamed Er-rouidib, HichamMouncifc, Benachir El Hadadia "Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET" International Workshop on Web Search and Data Mining (WSDM) April 29 - May 2, 2019, Leuven, Belgium Page-1176-1181.
[5] SandeepLalasahebDhende, Dr. S. D. Shirbahadurkar, Dr. S. S. Musale and Shridhar K Galande "A Survey on Black Hole Attack in Mobile Ad Hoc Networks" 4th Int'l Conf. on Recent Advances in Information Technology | IEEE RAIT-2018 | Page-978-984.
[6] Danista Khan and MahzaibJamil "Study of detecting and overcoming black hole attacks in MANET: A Review" IEEE-2017 Page-978-981.
[7] SandeepDhende, SandeepMusale, Suresh Shirbahadurkar and AnandNajan "SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs" IEEE WiSPNET Conference 2017 Page-2391-2394.
[8] Taku Noguchi and Takaya Yamanmoto "Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks" Conference on Computer Science and Information Systems 2017 Page- 797-802.
[9] LokeshBaghel, Prakash Mishra, MakrandSamvatsar and Upendra Singh "Detection of Black hole Attack in Mobile Ad hoc Network using Adaptive Approach" International Conference on Electronics, Communication and Aerospace Technology ICECA 2017 Page-978-990.
[10] Mohamed A. Abdelshafy and Peter J. B. King "Resisting Black hole Attacks on MANETs" 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) 2016 Page-1-7.
[11] Arathy K Sa and Sminesh C Na "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET" Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016) Page-264-271.
[12] Shruti Singh, AbhishekBajpai and Suryambika "A Survey on Black Hole Attack in MANET" International Conference on Recent Cognizance in Wireless Communication & Image Processing, Proceeding Springer India 2016 Page-933-941.
[13] Muhammad Imran1, FarrukhAslam Khan1, Haider Abbas and MohsinIftikhar "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks" ADHOC-NOW Workshops 2014, LNCS 8629, 2015 Page-111-122.
[14] HetaChangela and AmitLathigara "Algorithm to Detect and Overcome the Black Hole Attack in MANETs" International Journal of Computer Applications (0975 – 8887) Volume 124 – No.8, August 2015 Page-22-26.
[15] Nilima H Masulkar, Archana A Nikose "An Improved Multipath AODV Protocol Based On Minimum Interference" International Conference on Advances in Engineering & Technology – 2014 (ICAET-2014) Page-1-8.