ISSN:0975-9646

A Technique to remove Black Hole Attacks in MANETs

Vikash Kumar

Department of Computer Science Engineering
Lovely Professional University, GT-Road (NH-1)
Phagwara, Punjab, India-144411

Abstract- **A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. The popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet. Black hole attack is very serious issue in MANET. In black hole attack, a node which is malicious sends the route reply message to the source node to publicize itself for having the shortest path to the destination node. A malicious node utilized the routing protocol to advertise itself. This attack is having shortest path to the node whose packets it want to intercept. While transferring the data from the source node to destination node, it must be delivered privately to the recipient side. There are many methods present to avoid black hole attack. In this method, black hole attack is prevented through SRD-AODV. By using this method, we are able to prevent black hole attack by using AODV protocol in an effective way.**

Keywords— **Ad-Hoc on Demand Distance Vector Routing Protocol (AODV), Black hole attack, RREP, RREQ, SRD-AODV**

I. INTRODUCTION

Mobile Ad hoc Network (MANET) consists of a set nodes of equipped with wireless interfaces. In MANET have some special characteristics such as no fixed infrastructure, self organizing, adaptive and dynamic topology. It is an autonomous system in which nodes are connected by wireless links and nodes also behave like a router as shown in Figure 1. MANET are more vulnerable to attacks due to wireless transmission media [1]. In MANET, nodes are limited size and battery imposes limitation on the power capacity as well as transmission range. So, design of network protocols in ad hoc networks becomes challenging due to limited processing power and storage. The main goal of any protocol is to maximize performance with minimum resource utilization. The performance depends upon hop count, delay loss rate, throughput and the dynamic topology needs two fundamental requirements are protocol should be distributed and be able to multiple loop-free [5]. In this work, we have addressed routing issues of MANET in presence of malicious nodes. Routing is a core problem in wireless adhoc networks for sending and receiving data from one node to another node.

.

A. MANETS:

A Mobile Adhoc Network (MANET) is "an independent system of mobile nodes connected by wireless links" [1].

Every node not only operates as an end-system but also as an intermediate node to route the packets. The nodes can freely move about and organize themselves to form a network. The nodes are limited by their battery power for performing various operations. Routing a packet from source to destination involves an adequate number of intermediate nodes to be traversed. Therefore, battery power of a node should be used efficiently in order to keep the node alive for sufficient time to avoid early exhaustion of a node/ network. Energy management is therefore an important concern as it is a "fuel" that keeps the network alive. Preserving power helps lengthen network lifetime and leads to the development of lightweight devices [2].Efficient battery/energy management [3-5] and system power management [6-7] are the most important means of increasing the lifetime of a node. They basically deal with the supervision of energy resources by controlling the battery usage of the nodes to increase its lifetime hence increasing the lifetime of the system; moreover it maintains the power level for future transmissions. The need for energy management in MANETs is due to the limited energy of the nodes because of which any node may exhaust and become unavailable rendering the entire network inefficient and inaccessible.

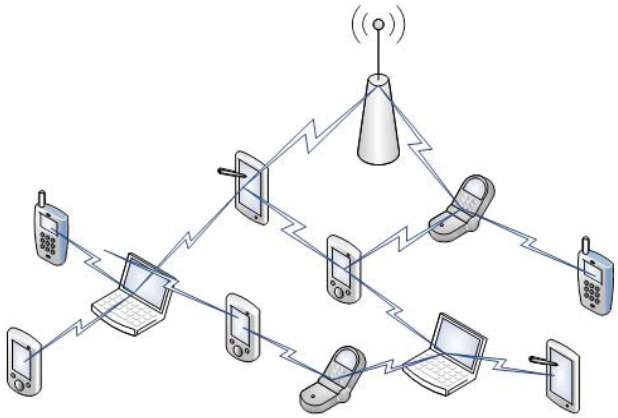

Fig.1 Mobile ad hoc networks [1]

The standard of AODV protocol, the source node contrasts the sequence number of destination which is enclosed in RREP packets when a source node got multiple RREP; it examines the best one as the route enclosed in that packet of RREP. In the event that sequence numbers are equal, it chooses the route which has smallest count of hop. As the outcome, the transmission of data will stream toward the node which is malicious by source node and it will be dropped. [3]

B. AODV Routing Protocol

AODV is an ad hoc on demand distance vector routing protocol that makes route to the destination when it is needed by the source node. It keeps up these routes as and when required by the source node. It provides fast adjustment to low processing, low network utilization, memory overhead, dynamic link conditions, and decides unicast routes to destinations inside the ad hoc network. One of the recognizing characteristic of AODV protocol is its utilization of sequence number of destination with each route. Sequence number of destination is made by the destination to incorporate information about route which is send to the requesting node. For communicating between portable nodes, Route Requests (RREQs), Route Replies (RREPs), Route Errors (RERRs) are the types of messages characterized by AODV. At the point when a source node needs to associate with a destination node, firstly it examines in the already present route table, in the

matter of whether a crisp route to that destination is accessible or not.

Fresh route implies an entry of valid route whose sequence number is larger than it in the RREQ. Bigger the sequence number, fresher is the route. On the off chance that sufficiently new route is accessible, it utilizes the same. Else the node launches a Route Discovery by transmitting a control message of RREQ to its every neighbour. This RREQ message will further be sent by the nodes which are intermediate to their neighbours having a crisp route to the destination.

The RREQ message will in the end achieve the destination node, which will respond with a route reply message (RREP). The RREP is transmitted as a unicast to the source node with the reverse route settled amid the Broadcast of RREQ. Also, the RREP message permits intermediate nodes to take in a forward route to the destination node. Hence, toward the end of the process of route discovery, packets can be conveyed from the source node to the destination node and the other way around. A route error message (RERR) permits nodes to tell errors because of breakage of link, for example, when a past neighbour moves to another position and is no more reachable. Every portable node would intermittently send Hello messages (HELLO), consequently, every node knows which nodes are its neighbouring nodes. [4]

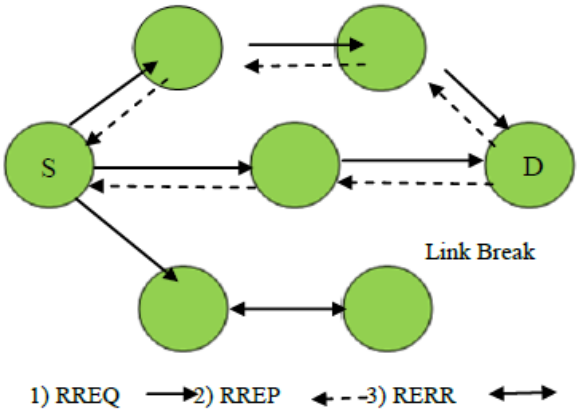

Fig.2 Working of AODV Protocol [4]

II. BLACK HOLE ATTACK

MANETs are powerless against different attacks. Most common types of attack are the dangers against MAC, network and physical layer which are the most essential layers that work for the mechanism of routing of the ad hoc network. Attacks in the network layer mostly have two reasons: not sending the packets or including and changing a few parameters of routing messages, for example, hop count and sequence number. A fundamental attack that an opponent can execute is to quit sending the data packets. Subsequently when the opponent is chosen as route, it denies the communication to happen. In black hole attack, the node which is malicious stays for the neighbours to launch a RREQ packet. As soon as the node gets the RREQ packet, it will quickly forward a false RREP packet with an altered Upper sequence number. Thus that source node expects that node comprises of fresh route in the direction of destination. The source node disregards the RREP packet got from different nodes and starts to forward the data packets over the node which is malicious. A malicious node acquires all the routes near itself. It doesn't permit sending any packet at any place. This attack is known as black hole as it consumes all data packets and objects. [5]

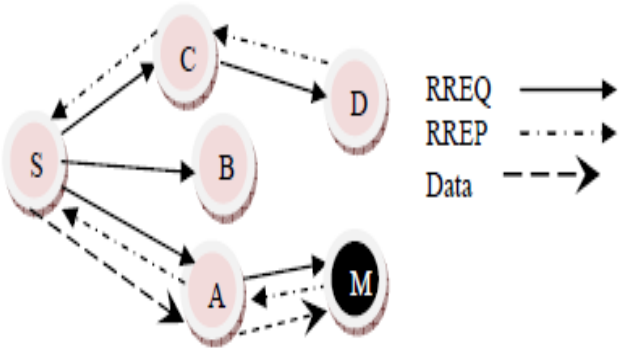

Fig.3 Black Hole attack in MANETs [5]

In the Fig.3, node S wishes to forward data packets to destination node D in the network. Node M is a malicious node which goes about as a black hole. The attacker answers with false answer RREP containing higher altered sequence number. Hence, data communication starts from S towards M rather than D. [5]

III. RELATED WORK

Hansraj Bhakte in [6] discusses about secure route discovery for preventing Black hole attacks on AODV based MANETs. A mobile ad hoc network comprises of remote portable nodes that has capability of communication with each other without requirement of any centralized administration and infrastructure. MANET is a rising exploration area with viable applications. Routing assumes a vital role in the network's security. Generally, security in routing in wireless MANETs seems to be an issue which is not an easy task to solve. Issues of routing security of MANETs are studied and examine one attack called "black hole" issue in this paper which can undoubtedly be utilized against MANETs. A solution for this problem is proposed for ad hoc on-demand distance vector routing protocol.

Dr. S. Tamilarasan in [7] throws a light on the AODV protocol and also about black hole attack. Ad hoc networks are raising technology, because of their unconstrained nature, are often created environments which are not secure and make them helpless against attacks. These attacks are occurred because of the taking part of the nodes that are malicious against numerous services of network. Protocols of routing are typical focus of these nodes. Ad hoc on demand Distance vector routing (AODV) is a broadly accepted network protocol for routing for MANETs. Black hole attack is one of the extreme threats of security in ad hoc networks. A solution for recognizing the malicious node in AODV protocol which is experiencing black hole attack is proposed in it.

Yash Pal Singh et.al [8] portrays a survey of already present techniques for identifying black hole attack against AODV routing protocol in MANETs. In mobile ad hoc networks, nodes generally coordinate and send one another's packet with a specific end goal of communication. Also few nodes may deny doing all this, either for sparing their resources or for deliberately disturbing general communications. This kind of bad conduct is normally considered as black hole attack, which is regarded as a standout amongst the most dangerous attack that prompts to collapse in the network. In a black hole attack, a malicious node replies for every route request with a forge reply guaranteeing to have the freshest and briefest route to the destination. Notwithstanding, when the packets of data reaches the malicious node rejected them. A few detection methods are portrayed in this paper and also their qualities and shortcomings are also discussed.

Rashmi in [9] discusses about clustering approach for locating and anticipating black hole attack in Ad hoc on demand distance vector protocol for routing in MANETs. A black hole attack in MANET happens because of the malicious nodes which pull in the packets of data by erroneously publicizing a new route to the destination. In the explained approach, each individual from the cluster will ring once to the head of cluster, to recognize the unusual difference between the quantities of data packets got and sent by the node. In the event that anomalousness is seen, all the nodes will darken the malicious nodes from the network.

Twincle G. Vyas et.al [10] talked about distinctive types of techniques of recognizing and anticipating black hole attack. Mobile ad hoc network (MANET) is a self actualized network of portable nodes created anywhere and anytime without requirement of any centralized administration. Because of the dynamic network topology, lack of centralized observing, absence of administration point, autonomous terminal. Mobile Ad-hoc networks are profoundly helpless against security attacks contrasted with wireless network which is based on infrastructure or wired network. In black hole attack, a malicious node provides forge information of having briefest route to the destination node to get all the packets of data and decline it.

IV. MOTIVATION

Mobile ad hoc network which is also sometimes called mobile mesh network is a self organizing network of mobile devices which are connected to each other by wireless connections. There is no centralized administration and also no pre defined infrastructure. There are many routing protocols in ad hoc wireless networks. But routing protocols are susceptible to many routing attacks. A black hole attack is one of the conceivable attacks in MANETs. This type of attack is a big issue in security. While exchanging the information from source node to the destination node it ought to be conveyed safely to the destination node. In this research, we are preventing black hole attack through SRD-AODV. By using this method, we are able to prevent black hole attack using AODV protocol in an effective way.

The research is based on the following objectives:

1. Division of network into grids.
2. To prevent co-operative black hole attack using multiple sinks.
3. To implement SRD-AODV to prevent co-operative black hole attack.
4. To prevent the co-operative black hole attack using grid deployment and multiple sinks.

V. PROPOSED SCHEME

The main aim of this research work is to prevent black hole attack in mobile ad hoc networks. In this work, we are focusing on the Cooperative Black Hole attack which means there is more than one black hole nodes attack on the network. Firstly, the network is divided into various grids and then deploys the sink in each grid where information is collected (one sink per grid). This one hope communication between nodes and sink eliminates the requirement for multi-hop communication between source and destination. The main assumption is that sink nodes cannot be compromised by the attackers. After that all the nodes in a particular grid will send the data to the respective sink and then sink will forward the data to the destination. So if we avoid the formation of multi-hop communication between source and destination then we can prevent the black hole attack. The flowchart for proposed methodology is as follows:

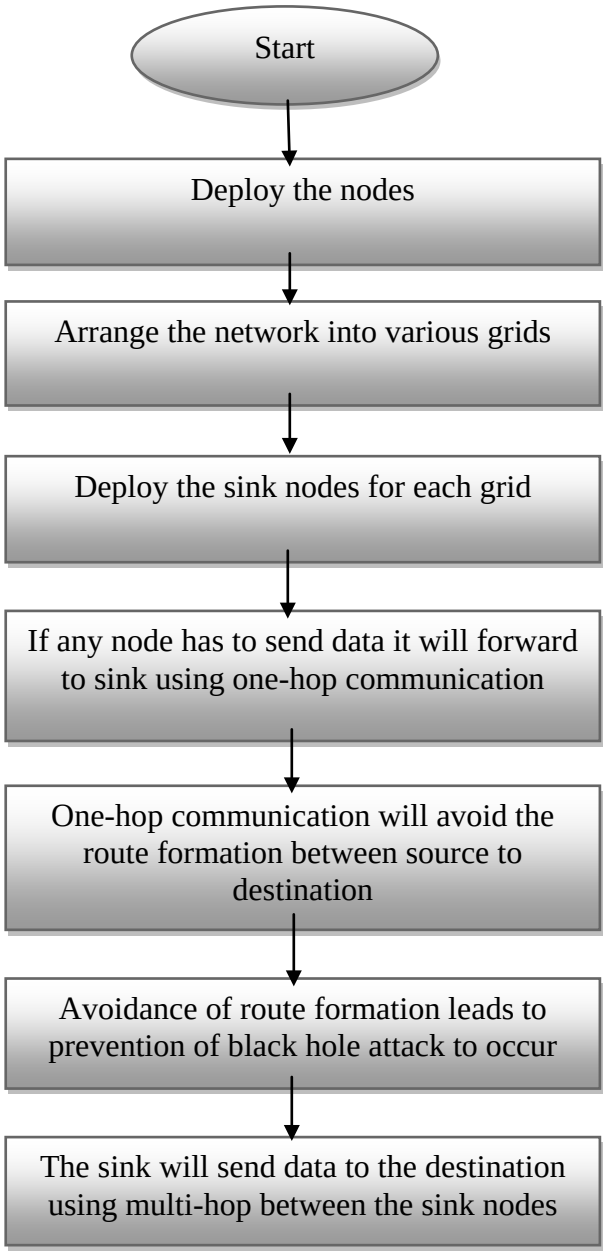

Fig.4 Flowchart of the proposed algorithm

VI. RESULTS

Black hole attack is primary security problem in ad-hoc network. Many approaches that have used to detect black hole attack. The black hole which can easily deploy against the MANET is described [18]. Black hole attack is mainly occurred in MANET and very hard to detect which is performed in network layer. Black hole attack is mainly two types. Black hole attack is attack on the one node and change the route of source to the destination and they follow the wrong path of that malicious node will be follow. We are concentrated on way to reduce the delay in the network. In future we will prevent the co-operative black hole attack using grid deployment and multiple sinks. In our future work we will compromise the proposed work with SRD-AODV.

.

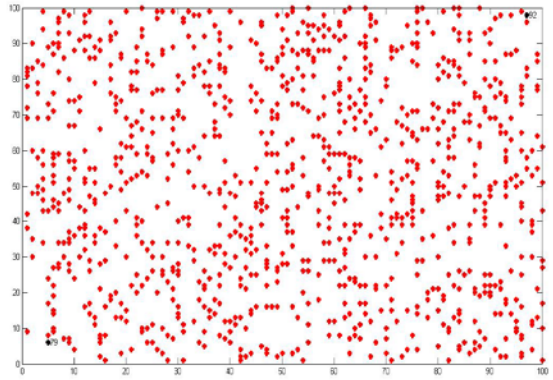

Fig.5 Node Deployment Scenario

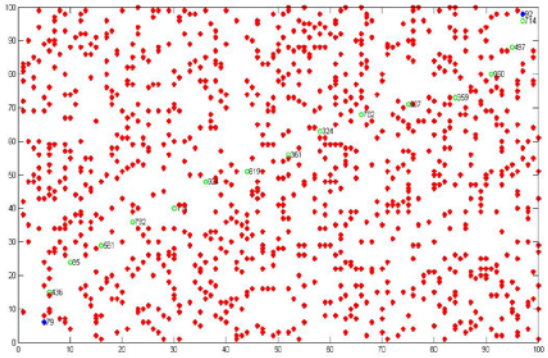

Fig.6 A path is formed from source to destination node

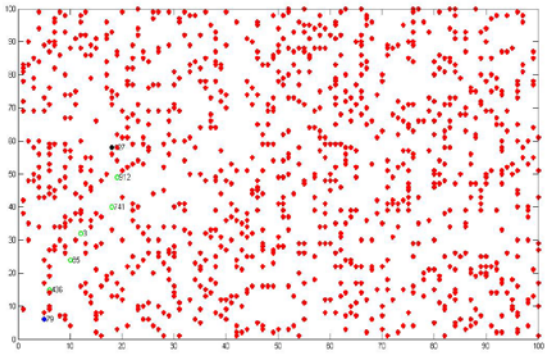

Fig.7 It shows the reply from the attacker node

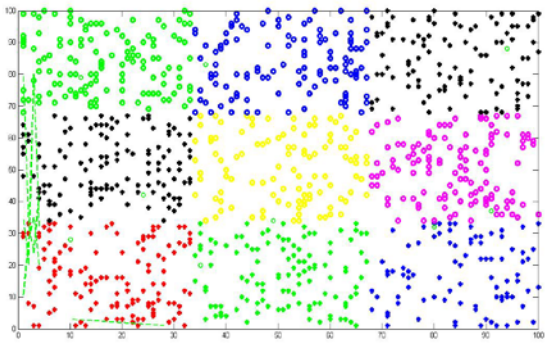

Fig.8 Multiple sink nodes being placed after the formation of the grids

Fig.9 This figure represents the amount of energy that is remaining in the network. (existing scheme)

Fig.10 This figure represents the routing overhead in the network. (Proposed scheme)

VII. CONCLUSION

Security of the network is most important and very biggest challenge in mobile ad-hoc network. There are various kind of security attacks are possible in mobile ad-hoc network. MANET there is no fixed infrastructure is available, the reliability is also a one issue in MANET. There are some specific functions should be available in the MANET like the establishment of the network should be fast, must provide good security to the communication and self reconfiguration. The infrastructure less architecture this is like no particular architecture is going to present this architecture changes by the region, the very high forms of network topology which may sense that the network topology must be in dynamic nature, and the resources of mobile device must be limited and also many new goals are presented in the MANET. Black hole attack is primary security problem in ad-hoc network. The black hole attack refers to place in the network where incoming traffic is show that discarded to drop the source to the data not reached the distension. MANET has no need for wireless router to communicate with the internet. We will find the black hole attack in MANET to prevent through AODV-based. All the nodes in a particular grid will send data to the respective sink and then sink will forward the data to the destination So if we avoid the formation of multi-hop communication between source and destination then we can prevent the black hole attack.

REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, Piet Demeester, “An Overview of Mobile Ad Hoc Networks:Applications and Challenges”, Department of Information Technology (INTEC), Ghent University, ghent, Belgium.

[2] Mohit Kumar, Rashmi Mishra, “An Overview of MANET: History, Challenges and Applications”, Indian Journal of Computer Science and Engineering (IJCSE), Vol.3, No.1, Feb-Mar 2012..

[3] Seryuth Tan, Phearin Sok, Keecheon Kim, “Using Cryptographic Technique for Securing Route Discovery and Data Trasnmissin from

Black Hole Attack on AODV-based MANET", International Journal of Networked and Distributed Computing, Vol.2,No. 2 , April 2012.

[4] Nitesh A. Funde, P.R. Pardhi, "Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, Issue 10, October 2013.

[5] Payal N. Raj, Prashant B. Swadas, "DPRAODV: A Dynamic Learning System Against Black Hole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[6] Hansraj Bhakte, rahul Kulkarni, "A Review- Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs", International Journal of Science and Research (IJSR), Vol 3, Issue 12, December 2014.

[7] Dr.S. Tamilarasan, "Securing AODV Routing Protocol from Black Hole Attack", International Journal of Computer Science and Telecommunications, Vol. 3, Issue 7, July 2012.

[8] Yash Pal Singh, Dr. P.K Singh, Jay Prakash, "A Survey on Detection and Prevention of Black Hole Attack in AODV-based MANETs", Journal of Information, Knowledge and Research in Computer Engineering, Vol. 2, Issue 2, October 2013.

[9] Rashmi, Ameeta Seehra, "A Novel Approach for Preventing Black-Hole Attack in MANETs", International Journal of Ambient Systems and Applications (IJASA), Vol.2, No. 3, September 2014.

[10] Ms. Twincle G.Vyas, Mr. Dhaval J.Rana, "Survey on Black Hole Detection and Prevention in MANET", International Journal of Advanced Resaerch in Computer Science and Software Engineering, Vol.4, Issue 9,September 2014.

[11] Sarita Badiwal, Vandna Verma, "Survey of IDS in MANET against Black Hole Attack", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol.2, Issue 5, May 2013.

[12] Bhoomika Patel, KhushbooTrivedi, "A Review–Prevention and Detection of Black Hole Attack in AODV based on MANET", International Journal of Computer Science and Information Technologies, Vol.5 (3), 2014.