ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

# Study Of Blackhole Attack In MANET

Ashish T. Bhole, Prachee N. Patil

***Abstract:-In the mobile ad hoc networks, the major role is played by the routing protocols in order to route the data from one mobile node to another mobile node. But in such mobile networks, routing protocols are vulnerable to various kinds of security attacks such as black hole node attacks. The routing protocols of MANET are unprotected and hence resulted into the network with the malicious mobile nodes in the network. These malicious nodes in the network are basically acts as attacks in the network. In this research, we are considering the one such attack on mobile ad hoc network called black hole attack. According to the aim of project, we will modify the existing DSR protocol with the functionality of black hole attack detection as well as prevention without the affecting overall performance of the network. Mobile nodes in the mobile ad hoc networks are act as host node and router node. It means nodes in the MANET are responsible for both data forwarding and routing mechanisms. But few malicious nodes which acts as misbehaving & selfish nodes. Such nodes do not deliver packets to the destination and packets are dropped by such nodes. We will investigate the performance of existing DSR protocol with this new modified security enabled DSR protocol using the performance metrics like throughput, delay and jitter. These nodes are called as black hole attacker nodes.***

*Index Terms*— **Black Hole Attack, Selfish Node, DSR, Dos Attacks.**

## I. INTRODUCTION

The mobile ad hoc network means MANET is nothing but the temporary network in which the mobile nodes collected independently on other mobile nodes in the same wireless network. These mobile nodes in such networks are moving arbitrarily all over the complete network. MANET networks are basically building temporary wireless networks and they are not requiring any kind of infrastructure for deploying as well as centralized administration [1]. The communication among these mobile nodes depends on the kind of routing mechanism used called multihop routing protocols. These routing protocols are having the functionality of forwarding the data packets from sender mobile number to the intended recipient [1]. Every mobile node in the mobile network is operating as the both forwarding node means routing operations and host node. Thus in other words we can say that, routing protocols for the mobile ad hoc network are introduced for building the communication routes as well as wireless communication network [2][3] . Building of dynamic communication a route in the entire network is done among the source node to destination node for communication purpose on demand way and hence this is the core functionality of MANET routing protocols. The mobile ad hoc networks are not having the fixed network topology due to the reason that mobile nodes are frequently changing their positions and movement. Network topology for the MANET networks is not fixed because of the frequent nodes movement in the network. Mobile ad hoc networks having different types of routing protocols like reactive, hybrid, and proactive protocols type of routing protocols. We can use these protocols with different network scenarios and mobility patterns. The reactive protocols such as DSR (Dynamic Source Routing) protocol and AODV (Ad hoc on demand Distance Vector Routing) protocol are frequently used MANET protocols. Apart from this, DSDV (Destination Sequenced Destination Vectoring) as well as OLSR (Optimized Link State Routing) are examples of reactive protocols. Zone Routing Protocol (ZRP) is one kind of hybrid protocol for the mobile ad hoc networks [1].

## II. PREVIOUS WORKS

Although, so many routing protocols are introduced for the wireless communication network by conducting various researches over those routing protocols, however such routing protocols having the problems of dependency over the mobile nodes majorly for the operation of routing and hosting for data sending. Every routing protocol is trusting over all the mobile nodes in networks for proper working. Mobile networks are open in nature and hence this is resulted into different kinds of network attacks which is happening due to such mobile nodes in the network. Mobile ad hoc network is threaten to various kinds of network attacks such as Denial of Service Attacks, Gray hole attacks, black hole attacks, worm hole attacks etc. This all attacks are possible only because of the mobile nodes in the MANET those are acting as misbehaving nodes in the network [4]. In other words, due to the malfunctioning, malicious and selfish nature of mobile nodes are resulted into misbehaving nodes. Any kinds of software or hardware failures are responsible for the malfunctioning nodes. The selfish nodes are only accepting the inputs from other mobile nodes in the network but not forwarding it to other forwarding nodes and just dropping those packets. Malicious nodes in the network taking other mobile node into the wrong direction rather than the intended direction by advertising information that he has shortest path for the intended recipient of information. This attack is called of DoS attack. All the received packets are dropped by the malicious nodes. In case of black hole node attack, misbehaving behavior of the nodes resulted into the selectively droppings of packets [6]. Thus due to this kinds

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

of attacks, MANET network becomes the vulnerable for the poor performance treats of used routing protocols. There are many solutions are introduced for addressing this wireless networks attacks and still the researches are going on. But if we add the routing mechanism for this network, it resulted into the performance degradations and lower throughput for those networks [5]. The In black hole attack, all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into black hole in universe. So the specific node is named as a black hole. A black hole has two properties in order to detect. First, the node exploits the ad hoc routing

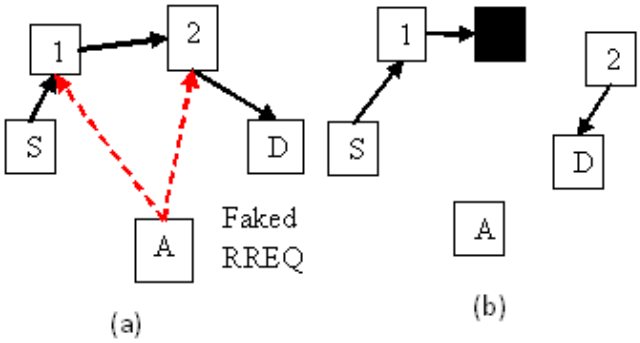


**Fig.1: Black Hole Is Formed By Faked RREQ.**

Protocol, such as DSR, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. Black hole attacks in AODV protocol routing level can be classified into two categories: RREQ black hole attack and RREP black hole attack. The attacker forms a black hole attack between the source node and the destination node by faked RREQ message as it is shown in Fig. 1

In the figure given below, the attacker unicasts the faked RREP message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node. Then RREP black hole is formed as it is shown in Fig. 2

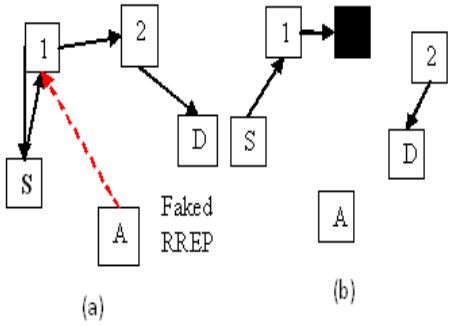


**Fig. 2 Black Hole Is Formed By Faked RREP**

## III. PROPOSED APPROACH

In Thus for the proposed approach, we are basically carrying our investigation over the mechanism of black hole node detections and their avoidance while keeping the performance of routing protocol. For maintaining the performance of routing protocols under the existence of black hole attack, we need to redesign and develop the routing protocol which will handle such attacks in the network and also maintaining the performance of such networks. For the investigation purpose in this study, we are using the DSR (Dynamic Source Routing Protocol). We did the changes in the DSR path building mechanism to detect the black hole node in the network and according removing that node from the given path. DSR designing is with the objective of fault tolerance. We propose an additional route to the intermediate node that replies the RREQ message to check whether the route from the intermediate node to the destination node exists or not. When the source node receives the Further Reply (FRp) from the next hop, it extracts the check result from the reply packets. If the result is yes, we establish a route to the destination and begin to send out data packets. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to whole network to isolate the malicious node [6]. If the next hop has no route to the requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node But here we assume the black hole nodes do not work as a group and propose a solution to identify a single black hole. However, the proposed method cannot be applied to identifying a cooperative black hole attack involving multiple nodes. We may also develop a methodology to identify multiple black hole nodes cooperating as a group. We are implementing this approach over the DSR protocol

## IV. WORK DONE

For the simulation of black hole attack we modified the existing routing protocol called DSR with the functionality of detection of black hole nodes and prevention of the black hole node attack. We used the network simulator version 2, for the simulation purpose with ns2 version ns-2.29 was used with different network scenario. In the following section we will first see the details regarding to the NS2 simulator and their usage.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

### *A. Network Simulator (NS2)*

As the name indicates the NS2 is the simulator which was developed for the simulation of the various kinds of the networks, their routing mechanisms, routing protocols, wireless, wired networks, wi-fi networks etc. NS2 is nothing but the discrete event simulator along with the functionality of objects oriented concepts. NS2 was developed in the UC Berkely. The languages such as C++ and OTcl were used for the development of NS2 simulator In order to shows the simulation of the black hole attacks, we have to use the modified DSR protocol which is simulating different types of misbehaving nodes such as malicious, selfish (type 1 and type 2). From the simulation results, we have aim to find out the detection of the black hole attack or misbehaving nodes from the network and on the detection of it prevention mechanism for it. For the simulation we have to consider the following network scenario: *Network Model: Random waypoint Model (which is default with NS2)*
*Number nodes: 10/20/30*
*Routing protocol: DSR/DSR (Modified)*
*Traffic type: CBR*
*Data payload: 512 bytes*
*Rate: 2 packets/sec*
*Simulation time: 200s*
Before running the simulation script, the modified DSR replaced with the existing DSR protocol which is by default with the NS2.

### *B. Result:*

**Table I: Simulation Results For 5 Nodes**

| | No. of nodes | Through put (packets/ TTL) | Delay (sec) | Jitter (sec) |
|---|---|---|---|---|
| **Modified DSR** | **5** | **375** | **0.0012** | **0.00015** |
| **Existing DSR** | **5** | **380** | **0.0011** | **0.00026** |

Thus, on the basis of our conducted results for both existing and proposed DSR algorithm, we claim that our modified DSR provide the security while maintaining the performance level and overall system lifetime. As shown in the above table, throughput, delay and jitter performances for the existing DSR and modified DSR which are showing slightly difference. As the number of nodes and network sizes grows this performance crosses the same equal performance for both existing DSR and modified DSR systems. Thus our approach is showing security enhancement while maintaining network performance.

## V. CONCLUSION

Existence of the misbehaving nodes or attacks in the mobile ad hoc network always degrades the overall performance of the present network system in terms of packet deliver ratio, end to end delay and throughput. This is indirectly influencing over the mobile ad hoc networks existing routing protocols. During this study, we conducted out research over the investigation of the one of well know MANET attack called black hole attack and proposed new DSR protocol with mechanism of black hole detection and avoidance while preserving the performance of this modified DSR. In addition to this, this approach providing the security mechanism with the DSR protocol in order to secure the wireless communication systems from black hole attacks or the misbehavior nodes. According to the design approach used for the DSR, simulation network first detecting those black hole nodes which are assumed to be the black hole attackers and then just preventing them just by avoiding those nodes from the routing path which are building dynamically during the entire simulation time. This technique is also looking for the performance of DSR, because most of time it happened that adding the security mechanism in MANET routing protocols is resulted into the performance degradation of that protocol. For future work on the basis of this existing study, we recommend to go for the real time approach design and deployment of this approach on small mobile ad hoc network in order to check the performance evaluation of it.

## REFERENCES

[1] Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF," A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks". IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005.

[2] Zhou L, Chao H-C. "Multimedia Traffic Security Architecture for the Internet of Things". IEEE Network 2011, 25(3):29-34. doi: 10.1109/MNET.2011.5772059

[3] Yang H, Lou H, Ye F, Lu S, Zhang. "Security in Mobile Ad Hoc Networks: Challenges and Solutions". IEEE Wireless Communications 2004, 11(1):38-47. doi: 10.1109/MWC.2004.1269716

[4] Umang S, Reddy BVR, Hoda MN. "Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption". IET Communications 2010, 4(17):2084-2094. doi: 10.1049/iet-com.2009.0616

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 4, October 2012

[5] Wu B, Chen J, Wu J, Cardei M. "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In Wireless Network Security. on Signals and Communication Technology". Edited by Xiao Y, Shen X, Du D-Z. Springer, New York; 2007.

[6] Marti S, Giuli TJ, Lai K, Baker M. " Mitigating Routing Misbehavior in Mobile Ad Hoc Networks". 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, 6-11 August 2000.

[7] Tseng Y-C, Jiang J-R, Lee J-H. "Secure Bootstrapping and Routing in an IPv6-based Ad Hoc Network". Journal of Internet Technology 2004, 5(2):123-130.

[8] Hu Y-C, Perrig A, "Survey of Secure Wireless Ad Hoc Routing". IEEE Security & Privacy 2004, 2(3):28-39. doi: 10.1109/MSP.2004.1.

[9] Raja Mahmood RA, Khan AI. "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks". International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18-20 November 2007.

[10] Saini A, Kumar H, "Comparison between Various Black Hole Detection Techniques in MANET".National Conference on Computational Instrumentation, Chandigarh, India, 19-20 March 2010.

## AUTHORS PROFILE

Ashish T. Bhole received B.E. Degree in Computer Engineering in 1999 from SSBT's COE & T, Bambhori; Jalgaon affiliated to North Maharashtra University, India, M. Tech. in Computer Science & Engineering in 2008 from S. A. T. I., Vidisha affiliated to Rajiv Gandhi Technological University, India and currently pursuing Ph.D. in Computer Science & Engg. His research area includes Computer and Wireless Networks, Network Security, Routing Protocols and Traffic Engineering. He has 12 years of teaching & research experience. He has published 20 papers in various International & National Journals, Conference Proceedings. Presently he is working as Associate Professor with the Department of Computer Engineering, SSBT's College of Engineering & Technology, and Jalgaon, India. Prof. Bhole is a Member of IEEE, ACM, Institution of Engineers (India), Internet Society, USA & Life Member of Indian Society for Technical Education.

**Prachee N. Patil** is a Research Scholar in the Department of Computer Engineering, SSBT's COE & T, Bambhori, and Jalgaon, India. She has received B.Tech Degree in Information in 2003 from College of Engg, Dhankwadi, Pune affiliated to Bharati Vidyapeeth University, Pune, and Maharashtra, India. She has 6 years of teaching experience. Her research area includes Network Security, Database Security and web applications. She is a Life Member of Indian Society for Technical Education.