A Survey on Black Hole Attacks and Comparative Analysis of Various IDS Schemes in MANET

Rashmi Ahlawat
Mtech. Research Scholar Technocrats Institute of Technology Bhopal, India

Setu K Chaturvedi, Ph.D
Professor & HOD (Dept. of CSE) Technocrats Institute of Technology Bhopal, India

ABSTRACT

A wireless communication system which do not require any fixed infrastructure for the establishment of its configuration is called Mobile Adhoc Network(MANET).This infrastructure leads to the misbehavior of some nodes which attack and degrade the performance of the network. In this paper we perform an analysis of various schemes that can be applied to improve the performance of MANET when a black hole attack occurs and provide a solution using anomaly based IDS scheme.

Keywords

DSR , AODV , MANET , IDS , malicious nodes

1. INTRODUCTION

A mobile ad hoc network is a collection of wireless nodes that can be rapidly deployed without the support of any existing network infrastructure or centralized administration. Nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. In this system the mobile hosts are free to move arbitrarily and at the same time they often acts as routers. MANET has some challenges such as [1,2] routing ,security and reliability ,quality of service ,inter-networking ,power consumption ,multicast ,location aided routing etc. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use a path and routing protocols such as AODV,DSR and DSDV.

The rest of the paper is organized as follows section 2 describes the security issues and various attacks performed , section 3 deals with classification of Intrusion Detection and Prevention systems, section 4 tells about the routing protocols, section 5 deals with several solutions that are provided for black hole attack on DSR and AODV protocols, section 6 presents the proposed scheme and finally in section 7 the results are discussed with the conclusion in Section 8.

2. SECURITY ISSUES AND DIFFERENT TYPES OF ATTACK IN MANET

Attacks in MANET usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses. Using cryptography or authentication can prevent the network against attacks that come from outside, malicious '*insiders*' also threaten the security.
Different types of attacks are explained as follows:

2.1 Passive Eavesdropping

An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to deduce the network topology to understand how nodes are located or are communicating with another. Therefore, it can gather information about the network before attacking. It may also listen to the information that is transmitted using encryption although it should be confidential belonging to upper layer applications. Eavesdropping is also a threat to location privacy [3].

2.2 Selective Existence (Selfish Nodes)

This malicious node which is also known as selfish node use the network for its advantage to enhance performance and save its own resources such as power .These nodes do not participate in the network operations and they do not change the content of packets to save its battery life. To achieve that, selfish node puts forth its existence whenever personal cost is involved. Therefore these selfish node behaviors are known as selective existence attacks. [4].

2.3 Gray Hole Attack (Routing Misbehavior)

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack .This attack is known as routing misbehavior [5] .

2.4 Black Hole Attack

The difference of Black Hole Attacks [6] compared to Gray Hole Attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

There are other attacks also such as impersonation modification attack, attack against the routing tables and sleep deprivation torture attack

3. DETECTION AND PREVENTION

Intrusion detection is the process of monitoring the events occurring in the network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices [8]. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. An IDS can be classified as network based or host-based according to the audit data that is used [9,10].

Network Based (NIDS):
Network-based IDS runs on a gateway of a network and captures and examines the network traffic that flows through it.

Host Based (HIDS):
A host-based IDS relies on capturing local network traffic to the specific host.

The primary classes of detection methodologies are [7]:

Signature-based (Misuse detection model)

It compares known threat signatures to observed events for identifying intrusion. This is very effective at detecting known threats and exhibits low false positive rates but largely ineffective at detecting unknown threats and many variants on known threats.

Anomaly-based detection

It compares definitions of what activity is considered normal against observed events to identify significant deviations (anomalous behavior). This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time. The IDPS then compares the characteristics of current activity to thresholds related to the profile.

Specification-based detection

It defines a set of constraints that describe the correct operation of a program or protocol. It checks the execution of the program with respect to defined constraints. This technique provides a capability of detecting previously unknown attacks with low false positive rate.

4. ROUTING PROTOCOLS IN MANET

Routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs. Two most popular routing protocols in MANET are AODV and DSR.

4.1 Overview of AODV

Ad-Hoc On-Demand Distance Vector Routing is abbreviated as AODV .It is a reactive protocol in which the route from source to destination is established as and when it is required .AODV completes its routing in two important phases as explained below.

Route Discovery Process: When the source nodes want to send data packets to the destination it initiates the route discovery process .The source nodes first checks whether a valid route is available in its routing table .If it does not finds any route to the destination in its routing table then it broadcasts a route request (RREQ) to all the neighbors. Upon receiving RREQ by a node which is either destination node or an intermediate node with a fresh route to destination, it replies by unicasting a route reply (RREP) message to the source node[16].

Route Maintenance: After the route discovery phase the source node gets the route to the destination and at the same time it is the responsibility of the source node to keep the maintenance. If there is any link break or failure a route error (RERR) message is passed to all the nodes in the network.

4.2 DSR

The Dynamic Source Routing (DSR) protocol is reactive routing protocol. All the data packets that the source wants to send to destination contains the complete list of nodes that the packet has to traverse[6] .In other words the send packets contains the route that it will use to reach the destination .The routes are stored in the memory and the packet header of the data packet contains the source route. The new routes are cached and no routing loops are formed in DSR.If the source nodes want to send data packets to the destination node and it has no route available then it will initiate the route discovery process which is similar to AODV.RERQ packets ie ROUTE REQUEST packets are send and every node except the destination node will broadcast it. The destination node or the node that has route to the destination will create a RREP packet ie ROUTE REPLY packet which contains the complete list of nodes that the RREQ packet has traversed . The selection of RREP can be based on hop count or latency .All nodes add all useful information in their respective route cache.

5. COMPARITIVE ANALYSIS OF VARIOUS SCHEMES PROPOSED TO DETECT BLACK HOLE

5.1 Resource-Efficient ACcounTability (REAct) Scheme based on Random Audits [11]

William Kozma Jr. et al. proposed a reactive misbehavior detection scheme called REAct scheme . REAct identifies misbehaving nodes based on a series of random audits which are triggered when the performance drop. Source-destination pair using REAct can identify any number of independently misbehaving nodes based on behavioral proofs provided by nodes. REAct constitutes of three phases :audit phase which combines information from honest nodes to identify the malicious nodes ,search phase which shows how the source selects nodes for audit in order to identify misbehaving ones and identification phase where the target node sends a feedback to the sender when a biggish packet drop ratio is recognized. Then the source node chooses an audit node, and utilizes the bloom filter to produce a behavioral proof. Finally, the segment location of malicious node can be distinguished from comparing the source node’s behavioral proof.

The simulation shows that REAct scheme not only reduces the communication overhead ,but enlarges the identification delay. REAct is designed for non-cooperative black hole attack only. It’s unsuccessful in the collaborative black hole scenario because other malicious node is able to manipulate a fake proof and send to the audit node. The behavioral proof only records the information of transmission packets rather than the nodes. It fails to verify who the producer of the behavioral proof is. Finally, using the binary search method to find the attacker is easily expose audit node’s information. The attacker is able to cheat source node by changing its behavior dynamically.

5.2 Next Hop Information Scheme [12]

N. Jaisankar et al. proposed a security approach based on next hop information scheme and is composed of two parts, detection and reaction. In the first part, the field_next_hop is added to the RREP packet. Before source node sends the data packets, the leading RREP packet is examined between intermediate node and destination node. Each node maintains a black identification table (BIT), and the fields in this table are as follows -source, target, current_node_ID,Packet_received_count (PRC), Packet_forwarded_count (PFC), Packet modified count (PMC). Then the PMC is updated by tracing the BIT from their neighborhoods. If the node acts correctly, the corresponding count value multiplies. After that, a malicious node can be found out if the number of receiving packets differentiates from sending packets. The second part is isolating the black hole, thus each node maintains an isolation table (IT) and stores the black node ID. The ID is broadcasted to all nodes in order to eliminate the malicious node by checking the isolation table.

In the simulation result, the packet delivery ratio is improved by 40-50% than AODV when facing attacks, and the number of packets dropped is decreased by 75-80%.This solution modifies the original RREP packets to collect the information of malicious nodes rather than sending further packets

5.3 Feedback Solution

Herminder Singh et.al. [13] have discussed the AODV protocol suffering from black hole attack and proposed a feedback solution which comparatively decreases the amount of packet loss in the network. It examines the no. of sent packets at each node which will always be equal to zero in the case of malicious node. After the malicious black nodes have been detected we can adopt a feedback method to avoid the receptance of incoming packets at these black holes. The packets coming at the immediate previous nodes to black nodes are propagated back to the sender and the sender follows an alternative safer route to the destination.

The performance analysis shows that the amount of packet loss in case of presence of black hole is much more than that in the absence of such a node. However, it cannot detect black hole nodes when they worked as a group .The solution is based on certain assumptions which are not always valid in the nature of mobile adhoc networks.

5.4 Behavioural Analysis by Introducing Trust Tables

In [14] Yaser khamayseh et.al. Proposed a protocol and modifies the behavior of the original AODV to check the reliability of the received routes before sending the data packets .It introduced a data structure referred as trust table at every node. This table is responsible for holding the addresses of the reliable nodes. Each node has a table prepared to hold the addresses of the reliable nodes. During the process of route discovery, for each node receives a RREQ, it checks the behavior of the broadcasting node. The RREP is extended with an extra field called trust field, this field is use to indicate there liability of the replying node. Once the behavior of the broadcasting node is normal, it is added to the trust table of the receiving node. The value of the trust field is initialized to zero by the replying node and might be modified by its previous hop during the trip of the RREP.

The value of the trust field could be modified either to 2 if the replying node is the destination itself or to 1 if the replying node is not the destination but still exist in the trust table. In case the trust field value equals to 1 or 2, the source node sends, otherwise the source node waits for further route. The protocol outperforms the original AODV in terms of packet delivery ratio, number of dropped packets, end-to-end delay, and overhead. The results show that, when the node is attacked by two black hole nodes and the pause time is set to zero, the protocol outperforms the original AODV. The protocol does not eliminate the black hole node from the network. The conditions of passing the behavioral analysis filter are not satisfied enough to judge the reliability of the node. Moreover, the protocol does not consider the behavior of two black hole nodes working together as a team. Although the proposed method gives reliable routes but it consumes high network delay.

5.5 Bait DSR (BDSR) based on Hybrid Routing Scheme [15]

The BDSR scheme works in two stages .It merges the proactive and reactive defense architecture. In the initial stage it uses a proactive architecture, i.e. uses a Bait id concept for the detection of malicious nodes present in the network. Upon the completion of initial stage it switches to reactive defense strategy. It uses DSR based secure routing protocol which detects and avoids the black hole attack. BDSR (Baited Black hole DSR) uses the concept of sending bait id and attracts black hole to reply the fake routing information. Proactive detection is used initially to send a virtual and random address as its destination address. If there is any malicious node it is detected and included in the black hole list. Proactive detection is used only in the initial stage. There by reducing the routing extra overhead. it becomes reactive detection. Upon the completion of the process it checks the packet delivery ratio. If there is a drop in packet delivery ratio destination node sends alarm to the source which triggers the black hole detection. BDSR mechanism merges the advantage of proactive detection in the initial stage followed by the reactive detection.

In this scheme the packet format of the RREP and RREQ is modified. Compared with the primitive DSR scheme and watch dog method, the simulation results show that BDSR provides an excellent packet delivery rate. The packet delivery ratio of BDSR is 90% which is more superior to DSR and WD approach. Moreover, the communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

5.6 Improved AODV Based on Hop Count

In [16] Jaspal Kumar et.al. proposed a protocol and modifies the behavior of the original AODV by introducing Improved AODV. IAODV mainly integrates two features: Multipath and Path accumulation Multipath-Single path AODV initiates a new route discovery when it detects one path failure to the destination, whereas in multipath it creates a fresh route in case all the existing routes fail or expire .In the proposed algorithm the source node selects shortest and next shortest path based on a single hop from the RREQ. If the neighbor node is in its routing table then route the data packet else the node is malicious and sends false packets to that node. The source node will invoke RREQ and inform all the neighboring nodes about the misbehaving nodes and add the status of stranger to the routing table of source node

The overhead of AODV is effected by twice as compare of IAODV. IAODV has a more packet delivery ratio, less average end to end delay and fewer overhead In AODV there is no path accumulation, it is single path reactive routing protocol with less security whereas IAODV is multipath hybrid routing protocol with path accumulation and more security. The values for average end-to-end delay are nearly similar in all the cases i.e. for both AODV and IAODV and there is a slight increase in the routing overhead.

6. PROPOSED SCHEME

We evaluate multiple black hole impact on the performance of MANET using AODV protocol and also provide solution that minimized the effect of black hole attack to some extent , thus improve the performance of MANET. The Black hole attack or any other attack on MANET can be found using intrusion detection systems and therefore the proper measures or solution can be used in order to avoid data losses in the MANET. This work focuses on development of the following two points as given below:

a) Creation of single or multiple black hole nodes in the network by modifying AODV Routing protocol that already exist in the NS2 simulator and creating MAODV protocol.

b) Afterward develop the solution in the form of IAODV protocol that can minimize the effect of blackhole attack and improves the network performance to some extent.

We made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. When a packet is received by the "recv" function of the "aodv/aodv.cc", it processes the packets based on its type. If packet type is any of the many AODV route management packets, it sends the packet to the "recvAODV" function. If the received packet is a data packet, normally AODV protocol sends it to the destination address, but behaving as a Black Hole it drops all data packets as long as the packet does not come to itself. In the code below, the first "if" condition provides the node to receive data packets if it is the destination. The "else" condition drops all remaining packets.

Code:

```
if ( (u_int32_t)ih->saddr() == index)
forward((blackholeaodv_rt_entry*) 0, p, NO_DELAY);
else
```

//for blackhole attack in the wireless ad-hoc network, after taking the path over itself, misbehaving node drops all packets.

```
Drop (p, DROP_RTR_ROUTE_LOOP);
```

6.1 Simulation Environment

The simulation is done on NS-2.34, linux platform (ubuntu10.04).Table 2 shows the parameter of the NS2 simulation.

Table 2: Simulation Parameters

S.No.	Simulation Environment	Values
1.	Simulation Time	500 s
2.	Grid Area	750m*750m
3.	Mobile Nodes	20
4.	Speed	20m/s
5.	Traffic	CBR
6.	Routing Protocols	MAODV, IAODV
7.	Packet Size	512
8.	Transport Layer	UDP
9.	Mac Layer	802.11

6.2 Parameters Used

The parameters that are used to analyze the network performance are :

Normalized Routing Load

The normalized routing load is known as the ratio between control packets sent to that of receiving data packets

Packet Delivery Fraction

It is the ratio of CBR data packets received by all destinations (sinks) over the total number of packets sent by all the sources within the simulation time.

7. RESULTS AND DISCUSSIONS

Using outputs from awk script following graph and results are generated for packet delivery fraction.

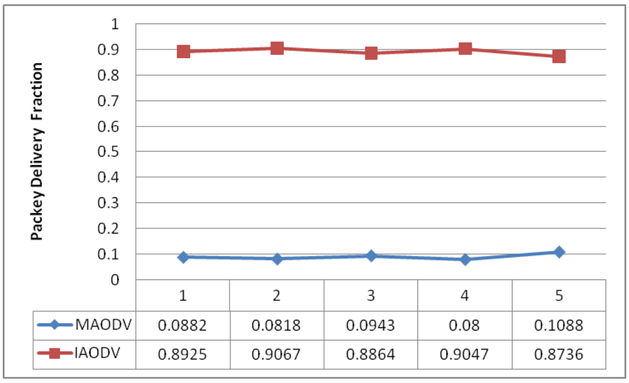

Figure 1: Comparative study of IAODV and MAODV protocol on the basis of Packet Delivery Fraction.

Due to the malicious node attack, its being observed that in case of MAODV the packet delivery fraction which is the ratio of CBR data packets received by all destinations (sinks) over the total number of packets sent by all the sources within the simulation time of the network is very less and it increases under the same situation when ids protocol is activated .Due to the malicious node attack, its being observed that in case of MAODV the packet delivery fraction which is the ratio of CBR data packets received by all destinations (sinks) over the total number of packets sent by all the sources within the simulation time of the network is very less and it increases under the same situation when ids protocol ie IAODV protocol is activated.

Normalized Routing load is evaluated based on messages like RREQ and RREP with the statistics of number of routed packets to that of received packets.

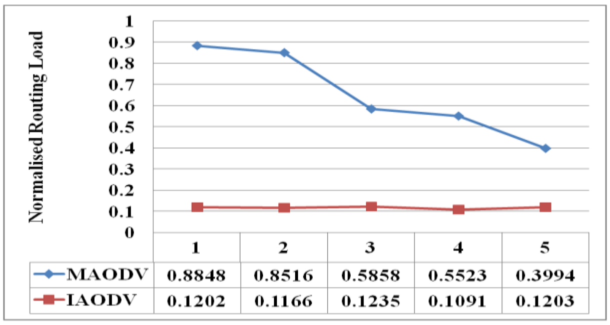

Figure 2: Comparative study of IAODV and MAODV protocol on the basis of Normalized Routing Load.

When the network is under attack the no. of routing packets and the no. of received packets both are reduced with the increase in the number of malicious nodes . This misbehaving activity of the malicious nodes is seen to impact the performance of network . Normalized routing load which is the ratio between routing packets sent to that of receiving data packets is reduced considerably by the proposed IAODV protocol as seen in figure 2.

8. CONCLUSION

This paper has reviewed various works that are related to black hole attack detection mechanism in particularly two main routing protocols in MANET ie DSR and AODV. The various authors have given several proposals for detection and prevention of black hole attacks in MANET but every proposal has its own advantages and disadvantages in their respected solutions .The various schemes are presented in chronological order .In this paper we made a comparison among the existed solutions on various parameters and developed an improved IDS scheme which reduces the normalized routing load considerably and increases the packet delivery fraction. The black hole problem is still an active research area for researchers and this paper will help the researchers to understand the various attacks and develop more improved IDS schemes thereby removing the shortcomings of the present IDS.

9. REFERENCES

[1] HaoYang, Haiyun & Fan Ye – “Security in mobile adhoc networks: Challenges and solutions,” Pg. 38-47, Vol 11, issue 1, Feb 2004.

[2] Chlamtac, I., Conti, M., and Liu, J. J.-N. “Mobile adhoc networking: imperatives and challenges”, Ad Hoc Networks, 1(1), 2003, pp. 13–6

[3] G. Vigna, S. Gwalani and K. Srinivasan, “An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks”, Proc. of the 20th Annual Computer Security Applications Conference (ACSAC’04).

[4] P. Ning and K. Sun, “How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols”, Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003

[5] D. Johnson, D. Maltz and J. Broch, “DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks”. Ad Hoc networking, Chapter 5, page 139-172. Addison Wesley, 2001.

[6] Sabina Barakovic ,Suad Kasapovic,and Jasmina Barakovic “Comparision of MANET Routing Protocols in Different Traffic and Mobility Models”, Telfor Journal,Vol. 2,No. 1,2010.

[7] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks”, Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999. University of Cambridge Computer Laboratory.

[8] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET”, IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008 .

[9] Ioanna Stamouli, “Real-time Intrusion Detection for Ad hoc Networks”, in 2003.

[10] Tiranuch Anantvalee, Jie Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” c 2006 Springer.

[11] Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009

[12] Fan-Hsun Tseng,Li-Der Chou,Han-Chieh Chao, ”A survey of black hole attacks in wireless mobile ad hoc networks”, Tseng ct.al.Human-Centric Computing and Information Sciences, 2011.

[13] Herminder Singh, Shweta “An approach for detection and removal of Black hole In MANETS” International Journal of Researh in IT& Management (IJRIM) Volume 1, Issue 2 (June, 2011).

[14] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein, “A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks”, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[15] Raja Karpaga Brinda .R, Chandrasekar.P “ Detection and Removal of Co-Operative Black Hole\Black Hole Attack in Manet ”, International Journal of Computer Applications (0975 – 8887) Volume 43– No.11, April 2012.

[16] Jaspal Kumar, M. Kulkarni, Daya Gupta “ Effect of Black Hole Attack on MANET Routing Protocols”, I. J. Computer Network and Information Security, 5,pp. 64-72 Published Online April 2013 in MECS.