ISSN: 2321-7782 (Online)
Volume 2, Issue 5, May 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Behavior based Anomaly detection technique to identify Multilayer attacks

Suhasini Sodagudi[1]
Associate Professor
Department of Information Technology
VRSiddhartha Engineering College
Vijayawada – India

Prof. Rajasekhara Rao Kurra[2]
Director, Sri Prakash Engg College
Tuni Sri Prakash Engg college, Rajahmundry
A.P. – India

Abstract: ***Nodes in a MANET (Mobile Ad hoc networks) possess self-configuring infrastructure-less network. Securing MANETs is an important part of deploying and utilizing them, since them are often used in critical applications where data and communications integrity in important. . The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks. Hence, there is a need to address the problem of coordinated attack by black hole acting in a group. A technique is proposed to identify black hole cooperating with each other and to provide a solution to discover a safe route avoiding cooperative black hole attack using behavioural anomaly based system, which makes it dynamic, scalable, configurable and robust. Moreover, inside a MANET another major security issue is to protect the Data link layer from malicious attacks by identifying and preventing malicious nodes. To address this issue a technique is proposed in the form of identifying man in the middle attack. One of the popular technique to detect MITM attack is IDS(Intrusion Detection System)which is used to monitor network activities. The detection technique deals at subnet level. Hence an algorithm is needed to source of ARP poisoning in the MITM attack which uses filtering rules to capture the network traffic and pass the IP packets. Extensive visualization of the method is illustrated in ns2 simulations with mobile nodes using Ad-hoc on demand Distance Vector (AODV).***

Keywords: attack, anomaly, behaviour, ARP poison.

I. INTRODUCTION

The operation of a computer network is a challenging task, especially if the network is connected to or part of the Internet. One reason is the increasing complexity of the Internet itself, which is characterized by the interconnection of lots of different devices, domains and controlled by separate network management authorities. Existing internet protocols cope up with such configurations and are weaker with security issues against the network infrastructure that cause serious problems. As a consequence, there must be proper systems that need to monitor and supervise their network permanently to guarantee proper functioning and detect and mitigate network problems and quality-of service degradations rapidly. [1][4]Ad hoc networks have a large number of potential applications. They possess a provision of establishing a network in situations where sufficient infrastructure is unavailable or very expensive. Within such an infrastructure-less skeleton, mobile nodes do communicate via access points in which each node acts as a host when requesting/providing information from/to other nodes in the network, and also acts as router in route discovery and maintenance procedures in the network. Due to limited energy supply for the wireless nodes and their mobile behavior, the radio links between them are not consistent for communication purposes due to security vulnerabilities. An intruder always exploits such a system and targets on data traffic or routed traffic and thus creates an inconsistent environment in the network. The impact of mobility on ad hoc routing protocols is expected to be very significant. A systematic framework is needed to investigate the impact of various mobility models on the performance of different routing protocols for MANETs. There are three models of mobility in Manets. Entity mobility model is to simulate a new protocol for ad hoc networks. Trace model is to extract mobility patterns that are observed in real life systems. Synthetic models represent

the behavior aspect of mobile nodes without the usage of any trace files. Random walk model is chosen within synthetic model where a mobile node moves from current location to a new location by randomly choosing the direction / speed. For several reasons, the Synthetic approach is the only approach which research can currently follow with ad-hoc. In this paper, we focus to detect BGHA (black-grey hole attack) with a synthetic design of mobility models. Nodes move independently from each other in this model. As shown in figure 1 the topology changes vibrantly. In this aspect, sufficient system must be incorporated in the routing issue so as to prevent some kind of potential attacks that to make use of data do not reach its intended recipient.

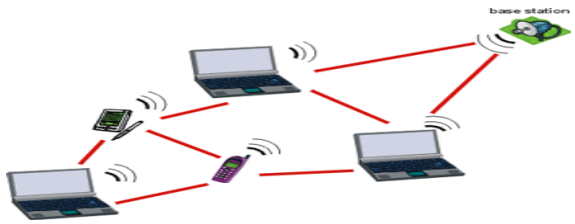

Figure 1. A sample ad hoc network

While dealing the routing issues, black hole attack is more prominent in which the incoming or outgoing traffic is silently discarded ("dropped"), without any information for the source/destination nodes. This can be visualized in the process of auditing the topologies that dynamically change from time to time. The observed black holes themselves are invisible, and can only be detected by monitoring the dropped packet traffic. DSDV is a table driven routing protocol where each mobile node in the network maintains a routing table with entries for every possible destination node. With periodical up gradation the routing table contains entries for all possible paths. This involves frequent route update broadcasts. Unexpectedly, DSDV is sometimes in efficient for larger scale of networks. DSR (Dynamic Source Routing protocol) is another on-demand routing protocol that maintains a route cache, which leads to memory overhead. [4][2]DSR has a higher overhead as each packet carries the complete route, and does not support multicast. AODV (Ad hoc On Demand Distance Vector protocol) is a source initiated on-demand routing protocol where every mobile node maintains a routing table with all entries of routes to the destination node along with the hop information. So whenever a source identifies to send a packet, it uses a specified route as found in its routing table. Else initiates a route discovery process and broadcasts a Route Request (RREQ) message packet to its neighboring nodes, which is further propagated until it reaches any intermediate node with a clear route to the destination specified in the RREQ, or at the destination itself. Thus when each intermediate node receives RREQ, it creates an entry in its routing table for the node that it has forwarded the RREQ, and the source node. Now the destination node or the intermediate node with a fresh enough route to the destination node, unicasts the Route Response (RREP) message to its neighboring node from which it received the RREQ. The intermediate node records this entry for the neighboring node from which it received the RREP, and then forwards RREP in the reverse direction. Upon receiving the RREP, the sender updates its routing table with an entry for the destination node, and the node from which it received the RREP. Entire path is clear for the sender to transmit its packets and thereby routes the data packet through the neighboring node that first responded with an RREP. [9]The AODV protocol is vulnerable to the well-known black hole attack. A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole does not have to check its routing table, it is the first to respond to the RREQ in most cases[2]. When the data packets routed by the source node reach the black hole node, it drops the packets rather than forwarding them to the destination. To defend against this type of black hole attack, we propose a behavior-neighborhood-based method. This technique works with slightly modified DSR protocol and makes use of cached routing data information and current routing tables. All this process includes traffic analysis which enables discovering periodical changes in the network.

Most of the forms in man-in-the-middle attacks include ARP Cache Poisoning, DNS Spoofing, HTTP session hijacking, and more. [3]This attack is one of the most prevalent network attacks against individuals and large organizations due to eavesdropping that happens to take place in victim machines. The end result is that the attacking host not only intercepts

sensitive data, but can also inject and manipulate a data stream to gain further control of its victims. In this paper, we will examine some of the most widely used forms of MITM attacks including ARP cache poisoning. In real world scenario, most victim machines are Windows-based hosts. ARP cache poisoning or ARP Poison routing is one of the oldest forms of modern MITM attack, which allows an attacker on the same subnet as its victims to eavesdrop on all network traffic between the victim machines. This attack is very famous and more prominent since it is the simplest one to execute but difficult to prevent.

The ARP (address resolution protocol) service is to facilitate the translation of addresses between the second and third layers of the OSI communication model. It is well-known fact that data-link layer in OSI deals with direct connection devices and thus uses only MAC addresses and these addresses are mapped to physical at the physical layer of OSI that makes it easy to send via a communication medium to a peer system. The third layer is the network layer that deals with devices that are either directly or indirectly connected and thus uses IP addresses, which are mapped to MAC addresses which are very useful at large. Therefore each layer follows its own addressing mechanism and work together in a communication.

The rest of the paper is organized as follows: Section 2 details the state of art in detection of black hole attack and man-in-the-middle attack. Section 3 details the proposed effective methods to detect two multi-layer attacks in manet as black hole attack and man-in-the-middle attack. Section 4 presents implementation with simulation results. Section 5 describes conclusion and future work.

II. Review of Literature

There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks, routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, forwarding attacks etc. Especially, the problem identified was observed in all these attacks are with the node behavior. Thus misbehavior based attacks became quite common nowadays. It was also cited by some researchers who could propose several techniques to solve these attacks, but failed to investigate the attacks completely. Focusing on these issues, this paper emphasizes to study as much as possible the attacks detection. Looking insight on different types of black hole attacks that exists in MANET, they are partitioned into ordinary black hole attack and collaborative black hole attack. Moreover several detection schemes are discussed clearly and compared.[1] The most common form of black hole is simply an IP address that specifies a host machine not running or an address to which no host has been assigned. That means a dead address will be undetectable only to protocols that are both connectionless and unreliable. Black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. The malicious router can also accomplish this attack dropping of packets or a randomly selected portion of packets for a particular network destination, at a certain time of the day. This is rather called a gray hole attack. In a Manet, such packet drop attack is very hard to detect and prevent. The proactive routing is also called table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbors. Each node needs to maintain their routing table which not only records the adjacent nodes and reachable nodes but also the number of hops. In other words, all of the nodes have to evaluate their neighborhoods as long as the network topology has changed. Therefore, the disadvantage is that the overhead rises as the network size increases, a significant communication overhead within a larger network topology. However, the advantage is that network status can be immediately reflected in the malicious attacker joins. The most familiar types of the proactive type are destination sequenced distance vector (DSDV) routing protocol and optimized link state routing (OLSR) protocol.

The reactive routing is equipped with demand routing protocol. Unlike the proactive routing, the reactive routing is simply started when nodes desire to transmit data packets. The strength is that the wasted bandwidth induced from the cyclically broadcast can be reduced. Nevertheless, this might also be the fatal wound when there are any malicious nodes in the network environment. The weakness is that passive routing method leads to some packet loss. Here we briefly describe two prevalent on-demand routing protocols which are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) protocol.

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets without forwarding to the neighboring nodes. [6]A single black hole attack easily takes place in mobile ad hoc networks. In an instance, if node1 stands as the source and node4 represents the destination, where node3 is taken as a misbehavior node, who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node1 erroneously judges the route discovery process with completion, and starts to send data packets to node3. As stated earlier, a malicious node probably drops or consumes the packet. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

[2]In ARP spoofing attacks like MITM, attackers send a fake ARP response packet pretending that they own the MAC address that is wanted. This causes the requester to cache the fake data. As a result, the victim's machine, which has incorrectly cached information about the owner of the IP address, sends all traffic destined for that IP address to the attacker's node since the victim possess no information about third party in between and just redirects to the attacker. The process of updating a target computer's ARP cache with a forged entry is referred to as "poisoning". This is done by mapping the attacker's MAC address with the IP address of the victim instead. The network is thus made open to vulnerabilities like Man-in-the-Middle attack (MITM), Denial-of-Service (DoS). The machine with IP address B does the MITM attack. So the ARP cache of machine with IP address A and that of IP address C are poisoned. All information transferred between machine A and machine C are now intercepted by machine B. This is extremely potent, when we consider that, not only can computers be poisoned, but routers/gateways and any device with an IP address as well can be poisoned.

III. PROPOSED METHOD

An approach known as MBHARP (Malicious Black hole attack with routing protocol) is proposed to identify black holes in a Manet. To solve this problem in a systematic manner, MANET topology is generated. In packet transmission, from source to destination, the malicious node act in different manner. In this detection process, node behavior is considered. DSR and AODV protocols are used to find safe route. The process is simulated using network simulator.

A. Black Hole Attack

DSR routing protocol is an adaptation of the DSDV & AODV protocols for dynamic link conditions. Every node in an ad hoc network maintains a routing table, which contains information about the route to a particular destination. When a packet is activated, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks its routing table for a route to the destination. If not, relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table present in the RREQ packet. If this is lesser than or equal to the value contained in the RREQ packet, then the node relays the request (RREQ) further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh clear route' and packets can be sent through this route. The intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in Figs. 1a and b. Since DSR has few security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. Malicious node says x can carry out many attacks against DSR.

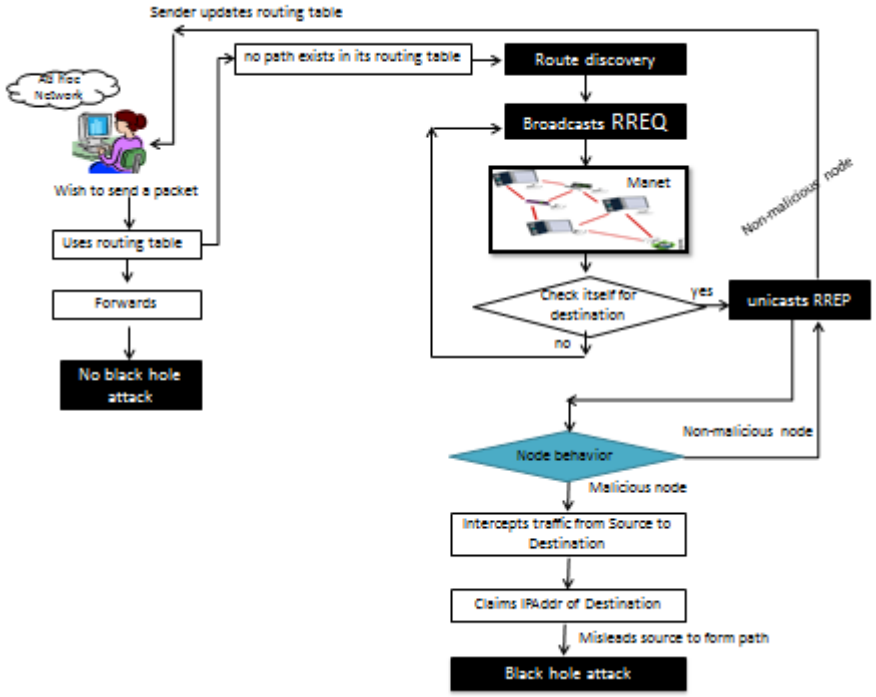

Figure 2. MBHARP approach

In a 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. First, the node exploits the ad hoc routing 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.[4]Black hole attacks in DSR protocol routing level can be classified into two categories: RREQ Black hole attack and RREP Black hole attack. An attacker can send fake RREQ messages to form Black hole attack. In RREQ Black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Black hole attack by faked RREQ message as follows:

Set the type field to RREQ (1);

Set the originator IP address to the originating node's IP address

Set the destination IP address to the destination node's IP address;

Set the source IP address (in the IP header) to a non-existent IP address (Black hole);

Increase the source sequence number by at least one, or decrease the hop count to 1.

Figure 3. Procedure to generate Black hole attack by faked RREQ message

B. MITM Attack

The attacks against layer-2 of ISO-OSI stack, the data link layer, ranges from various ARP attacks like the cache poisoning for wired clients to de-authentication of wireless clients. Fairly simple to implement, these attacks can often go unnoticed by intrusion analysts since intrusion detection systems typically look at the network layer and above to detect attacks. [9]For any method of attack an attacker uses to attack the data link layer, in all cases, an adversary attempts to compromise confidentiality, authentication or availability of information. The attacks succeed for the most part due to the lack of fine controls in the data link layer. Thus layer 2 is considered as a low level platform for attacks, where layer 2 attacks Figure 4. DL2MITM Attack detection continues to trouble more in networks and the implementation of each attack is unique [5]. This being the current

scenario, led to the development of this new algorithm DL2MITM (Data link layer MITM attack) and software, as a proof to examine network traffic for data link layer attacks and proactively responses to attacks.

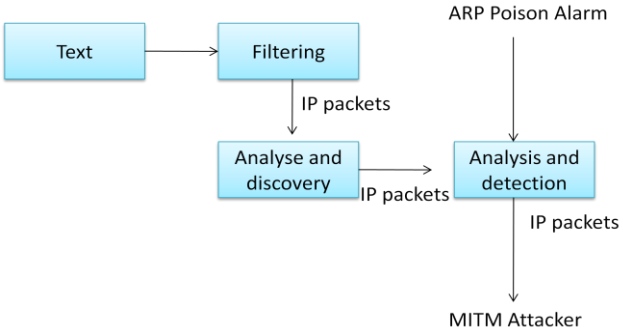

Figure 4 . DL2MITM Attack detection

Step 1 : Monitors packet headers of network traffic at regular intervals

Step 2 : Generates report of this packet header data.

Step 3 : Analyze the data to check for any Abnormalities

Step4 :Correlate the observed traffic with previous normal states of traffic

Figure5. Algorithm of proposed DL2MITM attack

Algorithm for explicit data request

Step1 Text file is taken and passed as an input file

Step 2 Filtering techniques are applied

Step 3 Nodes are created

Step 4 Connection is established

Step 5 The data is passed between the nodes

Step 6 If attacker occurs by using behavioral analysis attacker is detected

Figure 6. Process in DL2MITM through explicit request

Third party in the middle attack is where the attacker intrudes into the communication between the endpoints on a network to misuse the data path and to inject false information between the source system and the destination. This raises a ARP poison alarm. This is a type of attack where the attackers intrude into an existing connection to intercept the packets and change the packet data and thus injects false information.[4][8] It involves eavesdropping attack type over a connection, intrudes into a connection, intercepts the data and injects false data on the data path. This attack is possible in various domains and accordingly has different names with respect to the domain like monkey in the middle attack, fire brigade attack, session hijacking, TCP hijacking or TCP session hijacking. This attack happens like this. Basically attacker checks for communications between client and server. Then he uses a program in which appears like a server for the client or vice versa.

1. Consider a wired / wireless Network.
2. Establish links connection with traffic from agents as UDP and TCP
3. Provide estimations of bandwidth, delay, queue type etc.
4. At UDP, CBR(constant bit rate) agent is created and at TCP, FTP (file transfer) agent is created
5. Timeline the events in the communication network and raise ARP poison alarm
6. The agents that are created for the connections are to be released.

Figure 7: Sample steps to identify DL2MITM (Data link layer man in the middle attack)

IV. IMPLEMENTATION

For black hole attack, DSR routing protocol is focused. Every node in an ad hoc network maintains a routing table, which contains information about the route to a particular destination [2]. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and send back an RREP (Route Reply) packet. If not, it checks routing table to evaluate a possible route to the destination. Or else it relays the RREQ packet by broadcasting it to its neighboring nodes. Since DSR has less security mechanisms, malicious nodes can perform many attacks by their anomalous behavior.

Parameters considered in simulation

Area of size : 1000 × 584
Channel : wireless channel
Propagation model : Two Ray Ground
Mac : IEEE 802_11
Queue : DropTail and Pri Queue
Antenna : Omni Antenna
Ifqlen : 50
Number of nodes : 4-15
Routing protocol : DSR

Figure 8. Arguments considered

A malicious node x can carry out many attacks against DSR. This paper provides identification of 'Black Hole' attacks. [6]Implementation in NS-2 is described. To implement our contribution we have used the details explained in this paper. In our work, we have used the nodes that exhibit black hole behavior in wireless ad-hoc network that use DSR protocol. Some of the nodes behave as a Black Hole and had to use a new routing protocol, they can involve in messaging. In our simulations, we use CBR (Constant Bit Rate) application, UDP/IP, IEEE 802.11b MAC and physical channel based on statistical propagation model. Random waypoint model is used for scenarios with node mobility. The selected pause time is 10s. A traffic generator was developed to simulate constant bit rate (CBR) sources. The size of data payload is 512 bytes. Here 4-15 nodes were considered among which node 2 is a malicious node and remaining are normal nodes. The metrics used to evaluate the performance are given below.

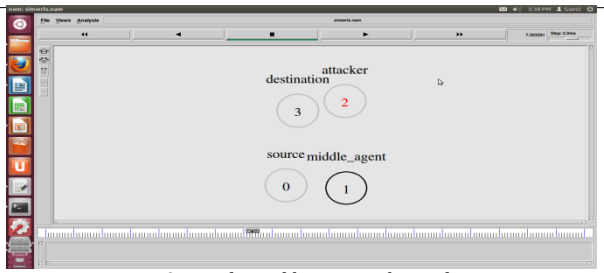

Figure 9. Wireless ad hoc network simulation

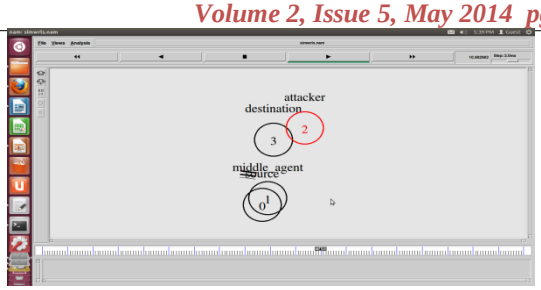

Figure 10. Node 2 is the attacker

MITM Attack : Nodes creation is shown with simulator. Node 0 is the client and node 3 is the destination. Nodes 1, 2 and 4 are the intermediate nodes, out of which node 4 is the opponent trying to hijack the data on the network. Data path is identified as with flows between UDP and TCP. The connections between the nodes are with approximations of bandwidth, delay etc. If UDP data path exists, an agent at constant bit rate is created.

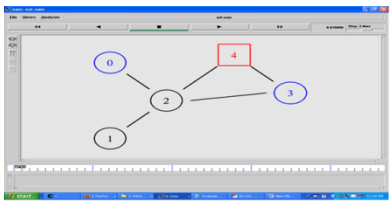

Figure 11. client(N0),destination(N3)

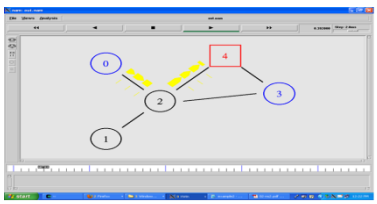

Figure12. N0-N2path hijacked by N4

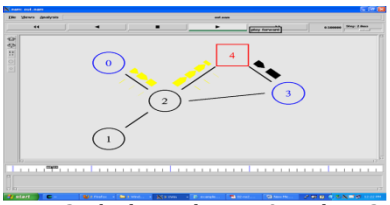

Figure13. Third party decrypts & send to N3

V. CONCLUSION

In this paper we have studied the routing security issues of MANETs and described the cooperative black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the DSR protocol. The proposed solution is applied to Identify multiple black hole nodes cooperating with each other in a MANET and to identify secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. NS2 implementation is simulated that runs on Linux, Windows with cygwin,Mac OS X,Solaris etc. Regarding MITM attack detection, developed a solution based system to trace for anomalies, their detections, the existing attacks etc in a network based system. Within the anomaly based, behavioural method is our approach because certain intrusion detection systems failed with signature and statistical based techniques. In this paper, we highlighted only third party in the middle attack, most common type of attack in global reach standards.

References

1. Pooja Vij, V K Banga and Tanu Preet Singh. Article: Broadcast ID based Detection and Correction of Black Hole in MANETs. International Journal of Computer Applications 56(17):6-11, October 2012.
2. Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly Detection: A survey, ACM Computing Surveys, 09 2009.
3. C.E.Perkins and E.M.Royer, “Ad Hoc On Demand Distance Vector Routing,” Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.
4. Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly Detection: A survey, ACM Computing Surveys, 09 2009.
5. D.E.Denning. An intrusion detection model. IEEE Transactions on Software Engineering, SE-13:222-232, 1987.
6. Virendra Singh Kushwah “Implementation of New Routing Protocol for Node Security in a Mobile Ad Hoc Network” (IJCSIS) International Journal of Computer Science and Information Security,Vol. 8, No. 9, December 2010
7. Abderrahmane Baadache, Ali Belmehdi “Avoiding-Black-Hole-and-Cooperative-Black-Hole-Attacks-in-Wireless-Ad-hoc-Networks ”IJCSIS) International Journal of Computer Science and Information Security,Vol. 7, No. 1, 2010
8. ns-2 Tutorial exercise , Multimedia Networking group, UVA
9. C.M barushimana, A.Shahrabi, “Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks,” Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.
10. Suhasini Sodagudi, Varun Manchikalapudi, K.Rajasekhara Rao,”An approach to identify anomaly with network data analysis”, IEEE Xplore Digital library, 2012
11. Suman S Chandran, Brajesh Patel, Amit kumar Chandanana, “Detection of suspected nodes in Manet”, ACEEE Int.J. on Network security, Vol.03, No.01, Jan 2012
12. Janvon Mulert, Ian Welch and Winston K. G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV", Journal of Network and Computer Applications, Volume 35, ppt: 1249-1259, Issue 4, July 2012.

