ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Denial of Service Attacks Implementation and Detection Approach for MANET

Hemant Pareek[1], Vishal Shrivastva[2]

M.Tech., Computer Science & Engineering, Arya College of Engineering & I.T., Jaipur,Rajasthan,India [1]

Professor, Department of Computer Science & Engineering, Arya College of Engineering & I.T.,Jaipur,Rajasthan,India [2]

Abstract: This paper implement and analyze two most common very effective Denial of service attacks known as Explicit packet dropping attack (EPDA) and implicit packet dropping attack (IPDA). The effects of both of these attacks are measured during data communication through a reactive MANET routing called Ad-hoc on-demand distance vector routing protocol (AODV). In Explicit packet dropping attack (EPDA), the attacker first explicitly gain access over the newly establish route between a source destination pair during the route discovery process and then drop all the packets that goes through it. On the other hand, in case of the implicit packet dropping attack (IPDA) the attacker does not know that at what time during the data communication process and of which data flow it is going to attack. Therefore the attacker implicitly caught on some data communication route and once it is on the route it will drop all the data packets that it receives for forwarding towards the destination node. To prove the effectiveness and correctness of the attacks and their detection methods, compare simulation results for various metrics over various MANET scenarios.

Keywords: AODV, DoS Attacks, EPDA, IPDA, MANET

I. INTRODUCTION

MANET routing protocols in general lack security mechanisms. For proper operation of routing protocol, it is assumed that intermediate nodes included in routing paths are trustworthy and follow protocol rules. It is required that each node in the network generate and forward routing control traffic according to protocol specifications. Absolute trust on intermediate nodes is a significant issue in networks that are characterized by dynamic topology. It is comparatively easy to eavesdrop wireless communication and to physically capture and compromise legal nodes. Without appropriate network level or link-layer security provisions, routing protocols are susceptible to many form of malicious activity that can freeze the whole network. In this chapter various attacks that can be launched on MANETs by exploiting the vulnerabilities inherent in routing protocols are discussed. It explains how basic routing protocol functions like packet or message forwarding and routing can easily jeopardize the whole network.

It is imperative to secure networks - wired or wireless for its proper functioning. Wireless ad hoc network is more vulnerable to security threats than wired network due to inherent characteristics and system constraints. The nodes are free to join, move and leave the network making it susceptible to attacks - both from inside or outside the network. The attacks can be launched by nodes within radio range or through compromised nodes. The compromised nodes exploit the flaws and inconsistencies present in routing protocol to destroy normal routing operation of the network. A compromised node may advertise nonexistent or fake links or flood honest nodes with routing traffic causing Denial of Service (DoS) attacks[1][2] that may severely degrade network performance. Thus it is seen that routing protocols are one of the main areas of vulnerability. There is a need to study the vulnerabilities in routing protocols that may be exploited by malicious nodes to launch attacks.

In this paper, two types of denial of service attacks over mobile ad hoc networks are implemented and their impact is analyzed on data communication process when using a reactive routing protocol for data communication. The reactive routing protocol used is well known Ad-hoc on-demand distance vector (AODV)[3] routing protocol. In the Implemented attacks, a malicious node i.e., attacker will drop data packets that it receives for forwarding towards the destination of the packet. The attacker can do the attack by either making itself one of the intermediate nodes on the active route. The attackers can be one of the intermediate nodes in two ways. In the first method the attacker is waiting that some route discovery process will select it as one of its intermediate node and then it will drop all the data packets it receives for forwarding to destination. In the second method the attacker uses the dissemination of the false information to become the part of an active route. Due to the wrong information spread by the malicious nodes the routing tables of the source node enters a route for the destination that will surely includes the attacker in the route. Results are drawn using graphs to show the impact of the attack on data communication. Finally, a mechanism is proposed through which both the attack and attackers can be detected during the data communication and can be avoided in further communication process.

II. RELATED WORK

In this Section, various types of attacks that are proposed in the recent years by various researchers working on the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

areas of attacks over MANETs with their detection methods (if given and available in the literature) are discussed.

Various attacks on MANETs given in literature are as follows:

(i)Jamming attacks

A node may generate considerable interfering radio transmissions (white noise [4]) that hinders legitimate traffic (control, data) to access the communication channel. Jamming prevents reception, resulting in massive amount of control traffic being lost. This prevents routes to be constructed in the network and accurate view of topology cannot be maintained.

(ii)Incorrect Traffic Generation attacks

A malicious node may generate incorrect control traffic and affect network connectivity in two ways.

Identity spoofing: A malicious node assumes the identity of some other node in the network and generates control messages. This causes incorrect topology view in nodes in the network.

Link spoofing: A misbehaving node may advertise an incorrect or non- existent link. As control messages are flooded into the network, all nodes receive and record information of the spoofed link. This causes incorrect routing tables or topology view of the network.

(iii)Incorrect Traffic Relaying attacks

Nodes in MANET forward both control traffic and data traffic. A misbehaving node may choose not to forward any type of traffic correctly. This misbehaviour may take the following forms:

Incorrect forwarding: In MANETs, each node acts as a router that forwards control traffic for diffusion into the network. A node may choose not to forward traffic resulting in missing connectivity. This leads to generation of incorrect routing tables or network topology. Similarly, a node may not forward data traffic correctly resulting in loss of data.

This also results in loss of network connectivity as data traffic is not forwarded to intended destination.

Replay Traffic: A node may first accumulate control traffic and later forward it as new set of control messages. During this period network topology may have changed. Replayed control traffic results in incorrect view of topology.

Based on the above three categories the following attacks are given in the literature:

(a)Wormhole Attack [5]

This attack is one of the most serious attacks on MANETs. In wormhole attack at least two attackers are required to perform the attack very effectively. These two attackers resides on different areas of the network makes a tunnel through the network to communicate with each other. The attackers broadcast the wrong information to the other nodes in the network that the destination is only one hop away from them. Sometimes they also broadcast the wrong information that they are true neighbours of each other due to this the attacker one which is near to source node is easily selected on the route between the source destination pair when the route is discovered on the basis of lowest number of hops on the route. It is very difficult to detect the worm hole attack as it is not modifying any data packet or generating any false traffic in the network.

(b)Gray Hole Attack [6]

In this attack the attacker when receives a route request (RREQ) message it modifies the sequence number in the RREQ message to perform the attack. The attacker increases the sequence number more than the usual number and reply back to the source to make it believe that it has the better and fresher route to the destination node. Once the source node got this reply it start the transmission of data packet on the route which consists of the attacker i.e., one of the intermediate node of the established route is the attacker. Till now half of the attack is performed by the attacker by spreading the false information and making himself the part of the route. Now when the data communication is started using the route, the attacker will drop all the data packets that reach to it without forwarding any of the data packets. In the literature many solutions are given to detect and then avoid the black hole attack. Another attack which is very close to the black hole attack in its implementation and attacking process is known as gray hole attack. In this attack the attacker does not try to get on the path between the source destination node but it also does not forward any data packets that goes through it.

(c)Flooding Attack [7]

Flooding attack is the simplest attack to implement but it is one of the most dangerous attacks. In this attack, the attacker broadcast the false control or data packets in the network due to which the network bandwidth is wasted largely and the legitimate packets are not able to reach their destinations. This attack is implemented on the reactive protocols by broadcasting the false data packets and RREQ messages. On the other hand, this attack can also be implemented on proactive routing protocols when the attacker node uses lower time to send the periodic updates. The methods to detect and avoid such nodes from the network are given in the work.

III. PROPOSED METHODOLOGY

The DoS attacks that are implemented in this paper are Explicit Packet Dropping Attack (EPDA) and Implicit Packet Dropping Attack (IPDA). The effects of both of these attacks on routing process and received data quality are measured during and after data communication through a reactive MANET routing protocol called Ad-hoc On-demand Distance Vector(AODV). In first DoS attack i.e. explicit packet dropping attack (EPDA), the attacker first explicitly gain access (i.e. become an intermediate node of the established route) over the newly established route between a source destination pair using the false information dissemination during the route discovery process of AODV and then drop all the packets that goes through it. On the other hand, in case of our proposed second DoS attack i.e. implicit packet dropping attack (IPDA) the attacker does not know that during the data communication process to which data flow it will attack. Therefore, the attacker implicitly

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

caught on some data communication route and once it is on the route it will start dropping all the data packets that it receives for forwarding towards the destination node.

3.1 Proposed Implementation of Denial of Service (DoS) Attacks

The working and proposed implementation process of two denials of service (DoS) attacks is described in this section.

3.1.1Explicit packet dropping attack (EPDA):

In the Explicit packet dropping attack (EPDA), when a source node receives a data packet for routing it towards some destination node, the node checks its routing table and if the source routing table does not have any route for the destination node the source node initiates the RREQ message. The RREQ message is a broadcast message and it contains following fields:

<source _addr, source_ sequence_no, broadcast_ id, dest_ addr, dest_ sequence_no, hop _cnt>

The <source _addr , broadcast_ id> is unique for each RREQ. Whenever the source sends a new RREQ then broadcast_ id is incremented. If the node that receives the RREQ is neighbor node it checks it for the duplicity by using a data structure called SEEN TABLE. If the received RREQ is not a duplicate it is re-broadcasted into the network by decrementing the TTL and increasing the hop count field. On the other hand, the RREQ is discarded without broadcasting. If an intermediate node has a fresh route for the destination then the node creates the RREP message sent it back to the source node. The destination sequence number field in the received RREQ message is used to calculate the freshness of the route. If the node receiving the RREQ message has route for the destination whose seq_no is greater than the sequence number given in the received RREQ message then the node can initiates a RREP message. On the other hand if none of the intermediate nodes has fresh route for the destination then the RREQ is finally received by the destination which then replies with the route reply message (RREP). The RREP is traveled in the unicast way from destination to source and creates the forward route when it reaches the source node.

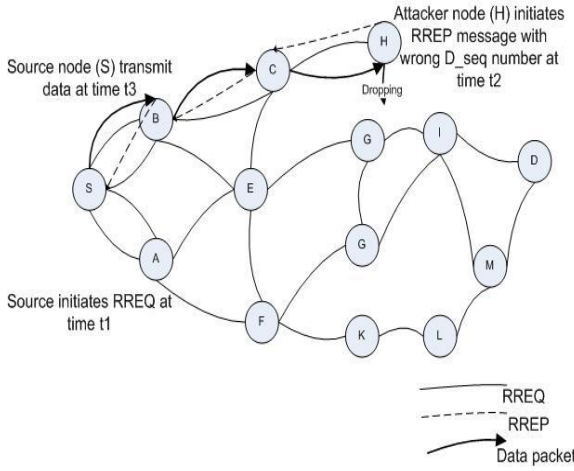

Fig 3.1 Working process of Explicit Packet dropping attack during route discovery phase

The attacker node will exploit the above mentioned route discovery process of the AODV routing protocol to make himself an intermediate node of the selected data communication route in the following way. When the attacker node receives the broadcast RREQ message from the source node it will create an RREP message with very high increased destination sequence number and send that RREP message to the source node. When the source node receives the RREP message from the attacker node it has no way to detect that this is the fabricated RREP message and it is generated by the attacker node.

Therefore, the source node updates its routing table for the destination node and starts the data transmission process. The source node will discard any other RREP messages that it receives from other network nodes or destination. In this way the attacker node make itself the part of an active route and drop all the data packets that it receives from the source node instead of forwarding them to the destination node.

The above mentioned approach of attack is also explained with the help of Figure 3.1. In the Figure 3.1 the source node is S, the destination node is D and the attacker node is H. The timing instants used in the Figure are such that where t1 < t2 > t3. The Figure 3.6 clearly shows how the attacker node H gains access on the newly established route and performs the packet dropping attack.

3.2.2Implicit packet dropping attack (IPDA):

In this attack, the attacker node will behave like a selfish or non-cooperative node which will not forward the data packets of other nodes that goes through it. The attacker will not do anything to disrupt the data communication in the network as long as it is not the part of any data communication path. Therefore, in this kind of attack finding the attacker node becomes difficult task as it is not harming the network by any other means than not forwarding the data packets. To properly explain this attack an example is used as given in Figure 3.2.

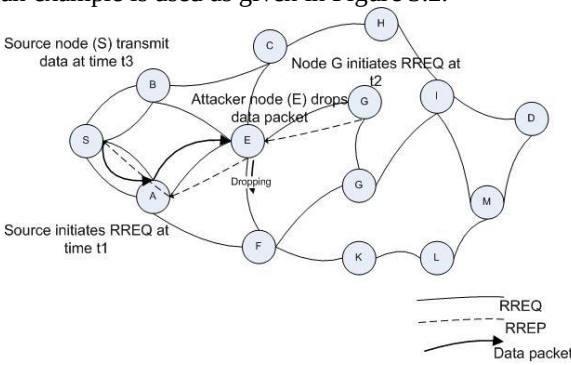

Fig 3.2 Working process of implicit packet dropping attack during route discovery phase

In Figure 3.2 node S is the source node and Node D is the destination node. When node S starts the route discovery phase at time t1, the broadcasted RREQ is received by the node G which has found a fresh route in its routing table for node D. Therefore, node G will reply the RRP on behalf of node D. This RREP will travel towards the source node through the unicast route from which node G has received

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

the RREQ message. If the node E is a malicious node in the network and it has forwarded the RREQ message that has been replied by node G then the RREP message will also go through node E. Therefore, when node S starts the data transmission after it receives the RREP message then all the data packets are received by the malcious node E as it is one of the intermediate node on the selected route between the node S and node D. When node E receives the data packets for forwarding it will intentionly drop them instead of forwarding them towards the destination. As, we can see from the example given in Figure 3.7 that node E has not any additional effort to get on to the route selected between the node S and D. This is why this attack is named as implicit data packet dropping attack.

3.3 Proposed Detection Method for EPDA and IPDA Attacks

The concept of Data packet Routing Information (DPRI) table is proposed in order to combat with the EPDA Attack. This proposed mechanism works as follows:

•In this every node maintains a DPRI table. This table consists of two fields knows as from and through corresponding to other nodes.

•Here from means the node whose table it is has routed any packets coming from the corresponding node in the table. And Through means if the node has routed any packets through the nodes listed in the table.

•For both the fields '0' stands for false and '1' stands for true.

•Now let's consider an example given in Figure 3.3.

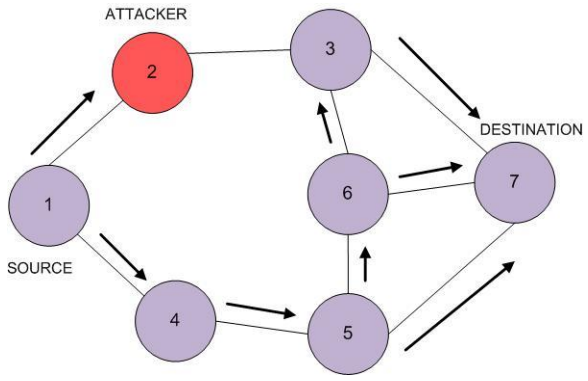

Fig 3.3 Example for detection method for EDPA

Here the FROM and THROUGH Fields for node 2 are '0' which indicates it as an attacker node.

The entire mechanism works as follows:

(i)First the source node broadcasts RREQ. When the source node receives RREP, it first checks if the RREP is from Destination node or an Intermediate Node. If it's from the destination then the route is considered secure and data packets are forwarded through that route. Else if, it's from an intermediate node, then the reliability of that node is checked.

TABLE 3.1
DPRI TABLE FOR NODE 3

DATA PACKET ROUTING INFORMATION		
NODE #	**FROM**	**THROUGH**
6	1	0
2	0	0
4	1	0

(ii)If the source has used this intermediate node before also for routing then it is considered reliable and hence data packets are routed through the provided route. Else it is an unreliable node.

(iii)The intermediate node that generates the RREP is supposed to reply with its Next Hop Node and its DPRI entry for the Next Hop Node.

(iv)The source node now generates FRq (Further Request) message to Next Hop Neighbor with the ID of the Intermediate node in question.

(v)The Next hop neighbor replies FRp(Further Reply)message with DPRI entry for Intermediate Node and the next hop node of current Next hop neighbor.

(vi)Now, the source checks if the THROUGH field of DIR table of Intermediate Node is TRUE for its next hop neighbor but the FROM field of DIR table of the Next Hop Neighbors Node is FALSE for the intermediate node, then it is declared as a attacker node, Else the node is considered reliable, The reliability of other nodes in the route is tested using the same procedure. This is done until the destination is reached.

But this method is suitable only in case of EDPA attack. For attacks like IPDA the DPRI table is modified-

(i) 3 different other fields known as CTR(COUNTER), Malicious node(MAL NODE) and TIMER is added. The DPIR table is now known as EDPRI Table (Extended Data packet Information Routing Table).

TABLE 3.2 EDPRI TABLE FOR NODE 3
DATA PACKET ROUTING INFORMATION

NODE#	**FROM**	**THROUGH**	**CTR**	**MAL NODE**	**TIMER**
6	1	0	0	0	0
2	0	0	3	1	2^4
4	1	0	0	0	0

(ii)And also 2 more types of packets are added which are Refresh packet and BHID Packet. Refresh packet is generated when a presence of malicious node in a route is detected. Each node that receives Refresh Packet deletes concerned path from its Routing Table.

(iii)CTR field keeps the count of how many times a node has behaved maliciously, MAL NODE are used to indicate if a node is an attacker or not by storing values 1 and 0 respectively. BHID packet is used to update this field. TIMER field, based on CTR value, is used to contain the time for which the node will be considered as an attacker.

Here the mechanism works as follows:

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

The detection of attacker node in EDPA is done in the same way as in the above process. But now after detecting the attacker the following steps are followed.

(i)After detecting the malicious node, the source now broadcasts a BHID packet and makes everyone aware of the attacker's identity.

(ii)Now all the other nodes mark this node as a black hole i.e. they set the MAL NODE field in the EDPRI table as 1corresponding to the attacker node. Also the value of CTR is increased by 1.

(iii)Each node now starts a timer (based on CTR value). This timer indicates the time for which the node is considered as an attacker.

(iv)After the timer expires this node is given one more chance and its MAL NODE field is again set to 0.

IV. SIMULATION RESULTS

This Chapter presented the detailed performance analysis and impact analysis of the Explicit Packet Dropping Attack (EPDA) and Implicit Packet Dropping Attack (IPDA) on different scenarios over mobile ad-hoc networks (MANETs). The network scenarios used in the simulation process are designed in such a way so that the effects of the wireless channel and environment can be obtained during the simulation process to replicate the real time scenarios. This is done to discover the exact impact of both the attacks over MANETs.

Performance Metrics

The following metrics are used in varying scenarios to evaluate the three different protocols:

(i)Packet delivery ratio (PDR): The ratio of the application data packets that are received without any error at destination nodes to the total data packets generated by the CBR sources are called Packet delivery ratio (PDR) of the network. Let's assume that S is the total number of packets send from source node and R represents the total number of packets received successfully at each destination node than the PDR is defined as follows:

PDR = R/S

(ii)Average end-to-end delay of data packets: This metric is calculated by the destination node whenever it receives a data packet. The destination node will calculate the delay of each received data packet by using its send timestamp and its received timestamp at the destination. At the end of the transmission the total time of the data packets received at the destination is divided by the total number of received data packets. Average end-to-end delay (EED) for packets received by each destination node is calculated as follows:

EED = delay of each packet received successfully / total number of packets received

(iii)Normalized routing load: The number of routing control messages that are transmitted for each data packet delivered at the destination node are called the Normalized routing overhead of a source-destination data flow. Normalized routing load gives a measure of the efficiency of the protocol by telling how much extra load is put by the proposed method to implement its working in the network.

Normalized routing load = Total number of control packets / (total number of control packets + total number of data packets in the network)

4.1 Simulation Result

In order to compare and evaluate performances of the three protocols (AODV, AODV with EPDA and AODV with IPDA) in different network conditions, one parameter are varied in the simulations:

• Number of Attackers

Simulations are carried out by keeping the number of sources constant and varying the mobility in the network. 5 sources are modeled respectively to study the effect of varying mobility in network. 4.1 Effect of network mobility on proposed attacks

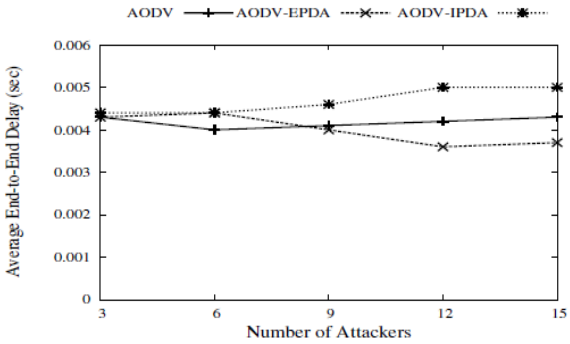

Figure 4.1 Average EED with increase in number of attackers

In Figure 4.1, the end-to-end delay of all the comparing routing protocols are shown with the increase in the number of attacker in the network. As it can be seen from the Figure 4.1 that as the number of attackers are increased in the network the end-to-end delay is not much affected. This is because the EED depends on the change in distance between source and destination during the route discoveries as with the change in the route length the EED is also changing. Here due to the attacks the EED actually decreases because the source is able to discover a shorter path for destination even if it is a wrong route with attacker on it.

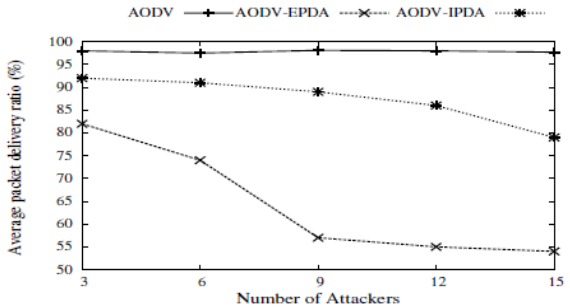

Figure 4.2 Average PDR with increase in number of attackers

In Figure 4.2 show the effects on network packet delivery ratio (PDR) with increase in number of attackers in the network for traditional AODV, AODV-EPDA and AODV-IPDA protocols. As it can be seen from the Figure 4.6 that as the number of attackers in the network increases

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

the PDR of the network starts decreasing. This is because as the increase in the network the probability that an active route will have an attacker on it increases. Due to this the data packets that are received by the attackers to forward to the destination nodes are increases and as the attacker will drop these data packets instead of forwarding them also increases. In this way the total network PDR decreases with increase in number of attackers in the network. As it can be seen from the figure that the PDR of AODV-IPDA is higher than the PDR of AODV-EPDA this is because in cas of AODV-IPDA the probability that an attacker will come on an active route is lower than it is in case of AODV-EPDA routing method.

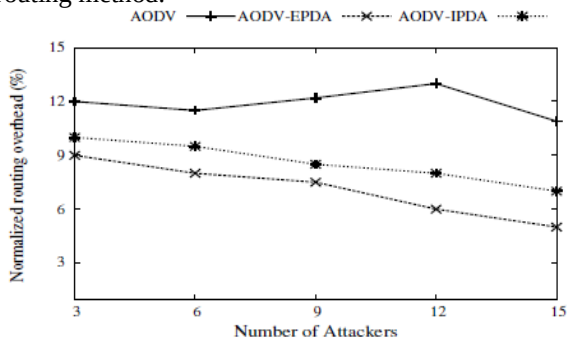

Figure 4.3 Average overhead with increase in number of attackers

In Figure 4.3 show the effects on network overhead with increase in number of attackers in the network for traditional AODV, AODV-EPDA and AODV-IPDA protocols. As it can be seen from the Figure 4.3 that as the number of attackers in the network increases the network overhead of the network starts increasing. As it can be seen from the figure 4.3 that overhead of the traditional AODV is lager than the other two with attacker protocols this is because in case of attack in the route the number of times route broken is decreased because the attacker will never initiate a route error message even if there is a route and it is broken. Due to this the number of route discovery processes is more in case of network without attack as compared to the case where there are attacks in the network.

V. CONCLUSIONS

The simulation results presented in the previous sections shows that the proposed attacks are implemented successfully and they causes the various forms of problems during the data communication process. the impact of the attacks on various network scenarios using various performance metrics (i.e., end-to-end delay, packet delivery ratio and routing overhead) to prove the correctness and effectiveness of the attack algorithms. It has been observed during simulations that due to attacks the performance of the underlying network decreases highly in terms of network throughput. Furthermore, proposed a possible detection method for the attacks and its theoretical study prove that attack can be detected with certain assumptions (such as each attacker causes unique type of misbehaviour). Although, it is very difficult to provide detection method with 100% efficiency and which also has a very low convergence time so that the effect of attack can be minimized or localized.

REFERENCES

[1] R.H. Jhaveri, S.J. Patel, and D.C. Jinwala “DoS attacks in mobile ad hoc networks: A survey. In Advanced Computing Communication Technologies (ACCT)2012”,Second International Conference on, 2012.

[2] Carl.G,Kesidis.G,Brooks,R.R.Rai,"Denial-of-service attack-detection techniques",Internet Computing, IEEE , vol.10, no.1, pp.82,89, Jan.-Feb. 2006.

[3] Yih Chun Hu Adrian Perrig and David B. Johnson Ariadne, “a secure on-demand routing protocol for ad hoc networks”, In Eighth ACM International Conference on Mobile Computing and Networking(MobiCom 2002), September 2002.

[4] Su.Ming-Yang and Chiang.Kun-Lin ”Prevention of Wormhole Attacks in Mobile Ad Hoc Networks by Intrusion Detection Nodes”, Wireless Algorithms, Systems, and Applications, Springer Berlin Heidelberg, 2010.

[5] Nait-Abdesselam.F "Detecting and avoiding wormhole attacks in wireless ad hoc networks" Communications Magazine, IEEE , vol.46, no.4, pp.127,133, April 2008.

[6] Chen Wei, Long Xiang, Bai Yuebin, Gao Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Communications and Networking in China, 2007. CHINACOM '07. Second International Conference on , vol., no., pp.366,370, 22-24 Aug. 2007.

[7] Ping Yi, Zhoulin Dai, Yi-ping Zhong, Shiyong Zhang "Resisting flooding attacks in ad hoc networks" Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on , vol.2, no., pp.657,662 Vol. 2, 4-6 April 2005.