 ISBN:978-93-5254-640-4

Mitigation of Data Flooding Attacks in Ad Hoc Networks: An NS-2 Simulation Study

Dr.S.N.Lokhande
School of Computational Sciences, SRTM University, Nanded , MS,431606, India
lokhande_sana@rediffmail.com

Dr.N.K.Deshmukh
School of Computational Sciences, SRTM University, Nanded, MS,431606,India
nileshkd@yahoo.com

Dr.P.U.Bhalchandra
School of Computational Sciences, SRTM University, Nanded, MS, 431606, India
srtmun.parag@gmail.com

Mr.S.R.Mekewad
School of Computational Sciences, SRTM University, Nanded, MS, 431606, India
satishmekewad@gmail.com

Dr.S.D.Khmaitkar
School of Computational Sciences, SRTM University, Nanded, MS, 431606, India
s.khamitkar@gmail.com

Dr.G.B.Kurundkar
Dept of Computer Science, SGBS College, Purna, Dist Parbhani, MS, 431606, India
gaju_k@rediffmail.com

Abstract— Network security is a weak link in wired and wireless network systems which if breeched then the functionality of the underlying network is impaired by malicious attacks and causes tremendous loss to the network. Denial of Service (DoS) attacks is one such most harmful network security threat. Ad Hoc networks are even more vulnerable to such attacks as they are infrastructure less and without any centralized authority. This paper narrates part results of an undertaken research work whose objective was to study the impact of Data Flooding DoS attacks on the performance of Ad Hoc networks. The gained knowledge is used to design and develop a security framework to detect intrusion and perform response actions. The validations of proposed defense system are carried out using statistical approach. All Simulations were carried out in NS-2.

Keywords— Security in Ad Hoc Networks, DoS Attacks, Simulation , Intrusion Detection

INTRODUCTION

In recent years, the explosive growth of mobile computing devices has impelled a revolutionary change in the computing world. This lead to emerging ubiquitous computing [1] which merely does not dependent of capability provided by the personal computer and has been a research hot spot in last few years. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method. In wireless networks, nodes transmit information through electromagnetic propagation over the air, making it cost economic and suitable for voice & data transmission. Wireless networks broadly fall into two main categories, infrastructure based called wireless through wireless Access Point (AP) and AdHoc network, where the nodes communicate with each other without having a central access point [2] . Our study centers on the later on. The Ad Hoc wireless Network is an autonomous system of mobile nodes. Such networks are known as infrastructure less network because no any per-existing infrastructure is required for communications [3]. Here mobile nodes form a time being network without help of centralized administration. These nodes generally have a limited transmission range and each node seeks the assistance of its neighboring nodes in forwarding packets [4]. This is the basic reason the nodes in an Ad Hoc network can act as both routers and hosts. Wireless Ad Hoc networks have wide range of applications including military applications, disaster management, business environments for cooperative & collaborative computing and sensor networks. It is witnessed that the computing scenario is drastically changed due to applicability of wireless communications. Today we have number of application areas where wireless networks can play important role. However, the risk also increases of getting harmed by intrusions and threats as the network is open and without centralized coordinator. According to [5], a threat can be defined as the potential possibility of a deliberate unauthorized attempt to access information, perhaps manipulate information and render a system unreliable or unusable. Since the prime concern of this research is security in Ad Hoc networks, an attempt is made herein to discuss the various security related attacks in the Ad Hoc networks. These attacks can roughly be classified into two major categories, namely passive attacks and active attacks [6]. In the passive mode of attack, data being exchanged is obtained without affecting the communication process. An active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of an Ad Hoc network. Eavesdropping, traffic monitoring, traffic analysis are few examples of passive attacks. Radio signal jamming, data modification, impersonating, denial of service (DoS) and message replay are examples of active attacks. According to the sphere of influence the attacks can also be classified as external attacks and internal attacks [7].When an attack is carried out by a node which is not in the domain of the network is referred as external attack. When a node within the domain of network is compromised and performs the

malicious activity is referred as internal attack. As compared to the external attacks, internal attacks are more severe due to fact that the insider has privileged access rights and knows valuable and secrete information. Further, the attacker can launch attacks on different protocol layers. On the basis of this, attacks can also be classified as per the network protocol stacks. We choose Denial of Service (DoS) attacks as they can be external as well as internal. These attacks attempts to prevent the victim from being able to use all or part of his/her network connection [8]. Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' access to a service provider. These are very easy to generate but are very difficult to detect and hence they are popular choice of hackers [9]. These can easily be applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the network. These attacks can be active or passive [11,12]. As compared with wired networks, DoS attacks in wireless Ad Hoc networks may not only bring damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be congested due to the limited bandwidth available as compared to fixed networks [10]. We have chosen two Dos attacks for our study, viz, data flooding attack and Black hole attack [11]. In data flooding attack, massive amount useless data packets will exhaust the communication bandwidth in the network and in black hole attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [13,14,35].

LITERATURE REVIEW

It is evident from the literature reviewed in the context of research hypothesis that there are numbers of intrusion detection and prevention systems proposed for traditional wired networks as we need to monitor central monitoring devises only [16]. The same is not true with Ad Hoc network as they do not have physical ambiance or central monitoring devices. Case drastically changes in wireless Ad Hoc networks where the communication medium is widely open and shared among different users [2, 3]. This highlights chances of being accessed by both legitimate and malicious users. This also gives scope to intruders as there is no clear severance between normal and abnormal activities in a mobile environment. In Ad Hoc network, nodes can move randomly in any direction and at any movement a node can leave or join a network. If a node is compromised, it will generate false routing information. Many intrusion detection systems have been proposed to suit these characteristics of Ad Hoc network [15]. Numerous architectures have been evolved over the time and they have implicit considerations of intrusions [15,17]. We have chosen Distributed and Cooperative Intrusion Detection Systems for the underlying study. In this architecture each node has an IDS and every node participates in intrusion detection and responses by their IDS agent. To determine the possible intrusion and initiating a response, an IDS agent is responsible for detection and collecting local events and data. If the data evidence is uncertain for intrusion detection, then neighboring nodes IDS agents cooperatively participates in global intrusion detection actions. This architecture is more suitable for flat network infrastructure, not for multi-layer network. The following section reviews some of the important methods and we try to investigate to what extent the proposed hypothesis can help to test all possible considerations. Preventing DoS attacks has got severe attention in past decade. The Sun B. et al.[18] proposed neighborhood based and route recovery scheme and the detection and prevention of black hole attack is done on the basis of neighboring node information. In another study Shurman et al.[22] proposes redundant route and unique sequence number schemes for preventing black hole attack. The Tamilselvan L et al. [19] proposed a time based threshold detection method by enhancing the original AODV routing protocol and Glomosim simulator as proposed by Shurman et al.[14, 34] . The study of Djenouri D et al.[14] proposed a Bayesian approach and Glomosim simulator for node allegation that enables node deliverance before decision. Other similar study designed a novel solution named Bait DSR (BDSR) scheme [34] to avoid the collaborative black hole attacks. A hybrid routing protocols is proposed by combining proactive and reactive methods. On demand DSR routing protocol is used as a base routing protocol. All above surveyed literature is helpful in augmenting the defense mechanism for selected attacks in wireless Ad Hoc networks. In case of Ad Hoc network, every node works as router for other, nodes and thus a mobile node depends on neighboring nodes to forward packets to its destination. A neighboring node may be selfish or it may be compromised by an external attacker. This compromised node may cause of DoS (Denial of Service) attack by denying services to the legitimate nodes. As the nodes of Ad Hoc network may have less processing power as well as battery life and consequently would try to preserve these resources [33]. Actions of a selfish node could lead to congestion, lower throughput and denial of service. The Buttyan et al. [20] have shown by simulation that a selfish node does not participate actively in packet forwarding in order to conserve electrical energy. The Buchegger, et al. [21] study the vulnerabilities exposed by selfish nodes in Ad Hoc networks by introducing new technique. After reviewing contemporary work on attacks and network security issues, it was found that the routing strategy was not been considered. If a fault is detected in the primary route, nodes can switch to an alternate route provided they are able to find multiple routes. We have come across some novel methods of intrusion detection which forced us to go for statistical analysis. The Huang et al.[23,26], have proposed a detection algorithm scheme that uses the statistics of packets, namely, the relation between different features such as the correlation between the number of packets dropped and the percentage of change in routing table. Tseng et al.[26,33], have proposed an IDS system where the normal behavior of critical objects in the network is constructed with the normal specification first. Then the actual behavior is compared to the normal specification. IDS Model proposed by Brutch and Ko [25,33] is a statistical anomaly detection algorithm. It was our basic observation that the most of the surveyed models use packets and network traffic related information such as updates in routing table or request-reply flow in the network. IDS Model as described in [26] utilizes the statistics derived from packet or traffic related statistics, for instance, the correlation between the number of packets dropped and the percentages of

updates in routing table. Above cited literature review highlights novelties and contemporary research investigations in detection of DoS attacks. Since our research hypothesis deals with mitigation and prevention of DoS attacks, it is need of hour to address issues regarding responses related to specific attacks. Many studies, as cited above, have incorporated prevention and mitigation of such attacks. Such attempt needs understanding of Intrusion detection and intrusion response framework. The framework components are relevant and coexist with each other. It was our critical observation that while designing IDS, intrusion response framework has given less attention than intrusion detection framework [27]. After a rigorous analysis all above related issues, a common finding came in picture that the IDA for Ad Hoc network must work with localized and partial audit data. It is more difficult for IDA in Ad Hoc network to distinguish between normal and intrusion traffic [15]. In wireless network, there is often no clear line between normal or abnormal activities. In wireless network the connection is not stable and mobile nodes can join and leave the network at any time. In addition, the communication between nodes for IDA purpose should not use much bandwidth resources. The communication between IDA on different nodes must be secure to not allow attackers gain the access to such communication. However, encryption in Ad Hoc network is a difficult task itself as compared to wired network mainly because of requirement of physical connection for access. Unlike in a wired network, Ad Hoc network nodes can be very easily compromised and hence the proper IDA must not take it granted that any node is secured. Therefore, in cooperative algorithm, the IDA must not assume that any node can be fully trusted. IDA must address high false alarm rate problem. It is difficult to obtain enough audit data to make an intrusion detection decision, because the bandwidth of Ad Hoc network is much restricted compared with wired network. As a result, IDA in Ad Hoc network can easily result in either having too much false alarm or missing many attacks [28]. Thus, the most important requirement feature is to find an appropriate architecture of IDA that will fit the mobile and Ad Hoc aspects of the wireless network. For a proper security mechanism we need to sketch out efficiently a way to use the audit data source since the audit data in wireless network is often partial and local. Further enough concentration should be given to find another efficient way to distinguish attack traffic from normal traffic. In many cases, the normal traffic that seems abnormal due to numerous factors like poor network connections, contradicts our assumptions and the IDA will have a high false alarm rate [15]. On the backdrop of all above discussions and research findings, the goal of this research study is to observe the impact of combination of prevention and mitigation of selected DoS attacks in Ad Hoc networks. The findings of the research clearly state that the implementations of such unified mechanisms have a significant impact on the overall network positively. On the other hand, the implementation of such mechanisms does not only mitigate the attack effects, it also increases the overall performance above the normal state of the network. When we investigated above facts and tried to establish proposition for our research hypothesis, it was seen that there are several open issues in the models that were reviewed. The important among them must be highlighted before our experimental setup is established.

PROPOSED MODEL

It was understood from earlier two sections of this paper that the data flooding and black hole attacks will affect the significant parameters as well as the performance of the Ad Hoc network. It was also understood that cooperative distributive framework is necessary for IDS designing. This fact is used as base for our intrusion detection and prevention framework. The proposed framework will monitor different significant parameters for the detection of intrusive activity in Ad Hoc network. If these parameters change rapidly, the appropriate threat is detected and intruder is identified. Later a corrective action is taken. The challenge here is the identification of sensitive parameters and their threshold values to predict the intrusion correctly. Many researchers' uses parameters and their threshold values for the intrusion detection in Ad Hoc network [29,30,31] . The parameter Threat (T) is used by detection framework to detect an attack or vulnerability. Threat is a number, which takes values between 0 to 3, when there is no attack, the network is in the normal state (NS) and this is indicated by the T range 0; when there is an attack, the network is in the vulnerable state (VS) and is indicated by the T range from 1 to 3; The threshold value of Threat (T) for the normal and vulnerable state are obtained by measuring the values of the significant parameters. When the network is in operating state the values of parameters are measures and the new value of Threat (TI). By comparing the computed TI with the T threshold, the node is classified as being in the normal or vulnerable state and this classification detects the attack. Each step of the threat detection framework, whose objective is to calculate the Threat to detect an attack, is explained below. Steps of the proposed framework are shown in figure 1. We refer to the terminology in [32] for the sketching of the response and prevention mechanism which gets triggered when an attack is detected by the detection framework. The significant parameters identified and the thresholds for these significant parameters in the detection framework are used by the response and prevention framework to defend the attack. When detection framework detects an attack, each neighboring source node to the node under threat is examined by the response framework and different action plans are initiated based on the identification of the nature of the intrusion nodes [32]. On the basis of threshold values, the node is reputed using the counters and flags on their behavior, which is achieved by monitoring significant parameters of node. The reputation counter is updated by comparing the values of the significant parameters against an expected norm. Based on the reputation counter, the reputation flag is asserted as Normal, or Vulnerable. If the reputation flag is Normal, no action is necessary. If the reputation flag is Vulnerable then response action is executed. The response action may isolate, block or deny further connections to malicious nodes. This framework works on the basis of the network parameters and performing response action on the basis of assertion of reputation flag. Such a framework allows for response to flooding and black hole attacks. Those malicious and selfish nodes that generate abnormal parameter values are identified

and isolated. The following action plans [32] are used in the response framework.

a) Action Plan 1: If a neighboring node to the node under threat is flagged as "normal", no action is needed.

b) Action Plan 2: If a neighboring node to a node under threat is flagged as "abnormal", action plan 2 is executed which may isolate or block the attacking node to protect the system.

Thus, with the help of the intruder identification mechanism and action plans, malicious nodes that create threat in the network will be isolated or blocked from the activities in the network. The Intruder Identification and Response process of our model is as follows in figure 2.

EXPERIMENTATIONS, OBSERVATIONS AND RESULTS FOR DATA FLOODING ATTACKS

We have carried out experimentations for DoS attacks. They are narrated briefly herein. As the first objectives of this study is to measure the impact of data flooding DoS attack on server node. In the first stage, the simulated network runs the under the normal operation where the nodes are communicated by sending and receiving the data packets normally. A set of random and moderate Constant Bit Rate (CBR) traffic is generated over the simulated normal network. In the normal run the basic network performance parameters are measured and referred to as the baseline of the normal network behaviors. These include total packet sent, total packet received, total no. of packets forwarded, total number of packets dropped end to end delay. These parameters are then used to measure average packet delivery ratio, network throughput etc. of the network under normal operation using the AWK script. In the second stage, multiple attacking nodes are launched , which performs data flooding DoS attack over the service provider node in the simulated network during normal network operation. The data flooding DoS attacker nodes generates huge amount of data packets which are generally larger than the normal packet size. The impact of this attack and changes in networks/nodes performance parameters are measured. In the third stage, the proposed intrusion detection and prevention framework is launched in the network. The defense framework will identify the attacking nodes on the basis of nodes parameters by comparing it with the values of normal and under the data flooding attack. This will confront the flooding DoS attack going over the service provider node and will be identified the attacking nodes for isolation so as to stop all the further requests from this attacking node. The network performance parameters are recorded and compared to the values against the attacked phase.

A. Experiment 1 : Normal network

In this experiment, the wireless Ad Hoc network of varying numbers of nodes was simulated in NS-2 (15, 25, 35 and 50) and varying numbers of connections. The wireless nodes are moving randomly in the topographic region. These different simulation scenarios are run to extract the behavior patterns of network. The log data (trace file) of these scenarios is processed by using the AWK script. The output of the AWK script yields the values of network parameters like total packet sent (TPS), total packets received (TPR), total packets dropped (TPD),total packets forwarded (TPF), which are then used to calculate the throughput (THR), packet delivery ratio (PDR), end to end delay (E2ED) etc. Following table 1 shows the results of different simulation scenarios with respect to the network performance parameters. The bar graph in Figure 3 shows the values of packet sent, received and packet dropped ratio for varying network size. As the size of network is increased then ultimately the parameters values of network are increased, this may be due to the increased numbers of nodes and numbers of active connections. Also a graph of PDR (Packet Delivery Ratio) is plotted for the varying sized network. The packet delivery ratio of the network in the normal operation is lies between the 85 to 93 % as shown in the figure 4.

B. Experiment 2: Data Flooding Attack on Service Provider Node

In this set of experiments the performance of network under the data flooding attack on service provider node is evaluated. Comparison of the Normal Operation, Data Flooding Attack at Service provider node and Proposed Defense frameworks response to this attack are measured as result. The service provider is node 4 and the service requesters are node 1 and node 5 respectively. There is one attacker node 6, sending continues data packets towards service provider node 5, as shown in the screen shot of Nam output of NS-2. In the normal operation of network the service provider node is able to send data packets towards requester nodes 1 and 5; also both the nodes are receiving the data packets normally without any interruption as shown in Figure 5. Once the simulation starts, all nodes, including the service provider node and service requester nodes are randomly moving at constant speed of 8 m/s in the topographic region. The simulation experiment is carried over 900 second and the log data of NS-2 trace file is collected. This log data of trace file is processed and analyzed using the AWK script to find the values of network performance parameters like total number of packets send, total number of packets received packet delivery ratio, end to end delay and throughput. Table 2 shows the values of network parameters in the normal network operation. As the objective of this experiment is to evaluate the performance of service requester nodes against the data flooding attack, so the parameters of the requester node 1 and node 5 are measured. Following bar graph in figure 6 shows the packet sent and received ration of node 1 and node 5 under normal operation. In the second stage of data flooding attack on service provider node, an intruder node is configured in the network. In the simulated network node 6 is placed near the service provider node, which then sends the useless data packets/traffic towards node 4 to exhaust the memory of node 4 and its queue will full with this useless data packets , due to this the service provider node cannot process or receive the further requests from requester nodes. This affects the communication between service provider and service requester nodes. From the screen shot of NAM output of Figure 7 it is clearly seen that, once the data flooding attack is started by node 6 on node 4 at that time node 4 is unable to communicate and transfer data towards genuine request by

node 5. Due to the huge amount of this useless data traffic node 5 cannot receive its intended service over the network. This causes the severe impact on the performance of network by affecting the parameters values. The log data from the trace file after the data flooding attack on the service provider node is processed and the results obtained are shown in the following Table 3. From the data its witnessed that the flooding DoS attacks decreases the parameters values as the throughput of the node1 decreases from 77.90 to 22.30 and for node 5 decreases from 68.501 to 18.906 and there is increase in the end to end delay time from 0.359 to 0.754. When we compared the results of these two scenarios we can say that the data flooding attack on the service provider node has drastic impact on the performance of the network. The parameters those are affected due to this attack are packet delivery ratio, end to end delay and throughput of the network as well as node 1 and node 5. In other experimentation, multiple data flooding attackers are implemented and launched in the network. In this scenario the service provider node and service requester nodes are same as in the previous scenario. The nodes 6, 7, 8 and 9 are data flooding nodes in the network. All the four attacker nodes are placed around the service provider node 4. All the four attacker nodes simultaneously send useless data packets towards service provider node. Table 4 shows the values of parameters affected by the multiple data flooding attack on service provider node. As from the Table 5.4 is it observe that the huge amount of data packets are transmitted in the network. Due to this huge data traffic there is congestion in the network which affects the performance of network. The PDR (Packet Delivery Ratio) is measured as 18.85 and THR (Throughput) of the network is decreased as 58.72, similarly the E2ED (End to End Delay) is increased to 10.14. From this it is concluded that the multiple data flooding attack affects the performance parameters and also the performance of the network. In the next step of experiment, the proposed intrusion detection and response framework is launched in all the genuine nodes including the service provider node. The intrusion detection and response framework identifies the attacking nodes on the basis of parameters identified as sensitive parameters and blocks the attacking nodes. The defense framework helps the network to gain more useful packet delivery ratio, throughput and improves the overall performance of network under the data flooding DoS attack which targeted directly at the service provider node. The Throughput of receiver is measured which is a ratio of the first and last data packet received over the time difference between them. Average throughput is the average of per receiver throughput. Table 5 shows the network throughput comparison of normal network operation, under data flooding attack at service provider node and in the presence of proposed defense framework. From this graph it is seen that the throughput of the network under normal operation without the data flooding attack is 71.96 kbps where as under the data flooding attack it is decreased to 16.38 kbps means the throughput is decreased by 76.82 % . When the proposed framework is launched it countermeasures the attack and helps to improve the throughput to 58.35 , as compared to under data flooding attack it is improved by 41.97 kbps. The overall delivered packets for service requester node 1 and node 5 in the normal operation, under the data flooding attack at service provider nodes and in the presence of proposed defense framework to data flooding attack at service provider node over 900 seconds are illustrated in Table 6. The defense system improves the delivery rate of the individual and overall service traffic by eliminating the attacking packets while transmitting the legitimate packets. From the Table 6, we can conclude that the defense framework helps to increase packet delivery rate. In this case, the delivered packets of node 1 in 900 seconds are improved by 32.64% and the delivered packets of node N5 are improved by 52.33%.

C. Experiment 3: Data Flooding Attack at Service Requester Node:

In this experiment, service provider is node 4 which transmits the packets towards the services requester nodes node 1 and node 5. Node 6 is launched in the simulated network which performs the data flooding attack on requester node 5. During the data flooding attack scenario, the attacker node is deployed nearby the requester node 5, and sending the useless data packets towards the node 5. Once the simulation run starts, all nodes, including the service provider node, service requester nodes and attacker nodes are randomly moving in topology region. When the attacker nodes start the data flooding attack, it results in a traffic congesting and dropping packets around the requester node 5.Table 7 shows the statistical data of node 5 during the normal operation, under the flooding attack and in the presence of proposed security framework. It is seen that the E2ED which is doubled under the data flooding attack as compared to the normal operation and is decreased up to 2 ms when the proposed framework is launched in the network. Similarly the comparison of packet delivery ratio and throughput under the data flooding attack clearly shows that the values of network parameters are decreased under the data flooding attack drastically and under our proposed framework the values are decreased which helps to maintain the network its normal state. In another experiment multiple data flooding attackers are launched in the network. The service provider is node 4 which transmits the packets towards the services requester nodes node 1 and 5. There are four attacker nodes are node 6, 7, 8 and 9. During the data flooding attack, the attackers are deployed nearby requester node 5 and they start sending the useless data packets towards the node 5. Once the simulation runs starts, all nodes, including the service provider node, service requester nodes, and attacker nodes are randomly moving in topology region. When the attacker nodes start the data flooding attack, it results in a traffic congesting and dropping packets around the requester node 5. Table 8 shows the statistical data of node 5 during the normal operation, under the flooding attack and in the presence of proposed security framework. We plot graphs for PDR , Delay and YHR as shown below in figures 8,9 and 10 .From these graph we can conclude that the multiple data flooding attackers will decreases the network performance, whereas our proposed framework helps the network to acquire its normal state by suppressing the excessive data traffic, which increases the values of packet delivery ratio, throughput and decreases the valued of end to end delay.

TABLE 1: PARAMETER VALUES BEFORE DATA FLOODING ATTACK

Expt. Setup	TPS	TPR	PDR (%)	E2ED (ms)	THR (kbps)
Normal N1 N5	**78187 6046**	**48196 3205**	**61.60 53.01**	**0.187 0.359**	**77.90 68.50**

TABLE 2: NETWORK PERFORMANCE PARAMETERS

No. of Nodes	TPS	TPR	TPD	PDR (%)	THR (kbps)	E2ED (ms)
15	10773	8809	1970	89.76	49.16	0.1725
25	21513	18526	3378	85.99	102.88	0.2276
35	35899	33380	4806	92.63	184.71	0.118
50	43085	38041	9049	88.28	211.30	0.1653

TABLE 3: PARAMETER VALUES AFTER DATA FLOODING ATTACK

Expt. Setup	TPS	TPR	PDR (%)	E2ED (ms)	THR (kbps)
Under Data Flooding Node 1 Node 5	67268 4058	31956 1928	47.50 47.51	0.459 0.754	22.306 18.906

TABLE 4: PARAMETER VALUES AFTER DATA FLOODING ATTACK ON NODE N4

Expt. Setup	TPS	TPR	PDR (%)	E2ED (ms)	THR (kbps)
Service Provider Node (4) Under Multiple Flooding Attackers	560594	105713	18.85	10.14	58.72

TABLE 5: OVERALL THROUGHPUT COMPARISON

Experiment Runs	Overall throughput
Normal Operation	71.96
Under Data flooding attack	16.38
In presence of defense framework	58.35

TABLE 6: OVERALL DELIVERED PACKETS COMPARISON

Experiment Run	Successfully Delivered Packets (over 900 sec.)	
Service Requester Nodes ⇨	Node N1	Node N5
Normal Operation	48196	3205
Under data flooding on service provider	31956	1928
With defense framework	42387	2937

TABLE 7: OVERALL NETWORK STATISTIC UNDER SINGLE DATA FLOODING ATTACKER

Expt. Setup	TPS	TPR	PDR	E2ED	THR
Normal	257002	240793	93.69	1.49	225.24
Under Flooding On Node 5	355210	132021	38.42	3.10	73.35
In Presence of Proposed Framework	242085	206513	85.30	2.03	122.14

TABLE 8: OVERALL NETWORK STATISTIC UNDER MULTIPLE DATA FLOODING ATTACK

Expt. Setup	TPS	TPR	PDR	E2ED	THR (kbps)
Normal	257002	240793	93.69	1.49	225.24
Under Multiple Flooding attack on requester node 5	560594	105713	18.85	10.14	58.72
Proposed Framework	24185	20653	86.99	2.03	122.14

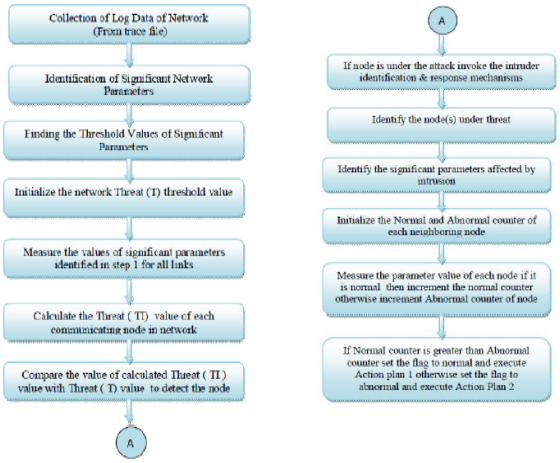

Fig. 1. Steps in Intrusion Detection & Prevention Model

1. Let N1, N2,...Nk be the nodes which are detected to be under threat based on intrusion detection algorithm.
2. Let $x_1, x_2,...x_n$ be the significant parameters which have been identified .
3. For each node under threat
   3.1. For each adjacent node to the node under threat
      3.1.1 Initialize its normal and abnormal counter
      3.1.2 For each significant parameter
         i. Measure the parameter values of the adjacent node.
         ii. If the parameter value is in normal state increment the normal counter
         Else increment the abnormal counter of the adjacent node.
   3.2. For each adjacent node
      3.2.1. If its normal counter is greater than abnormal counter
         set the flag of node to normal and execute the Action plan 1
         Else set the flag for node to abnormal and execute the action plan 2
4. Stop

Fig. 2. Proposed Intruder Identification and Response Process

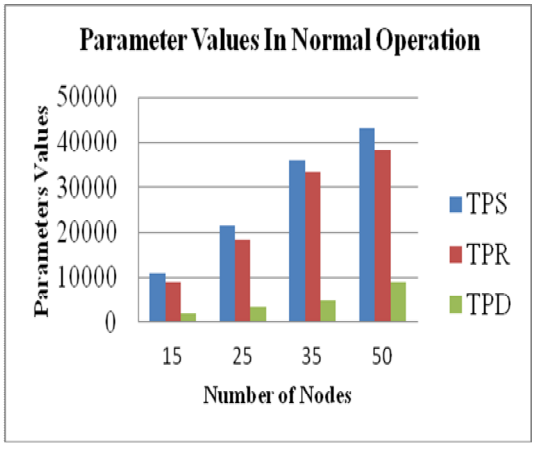

Fig. 3. Graph of Parameters in Normal operation

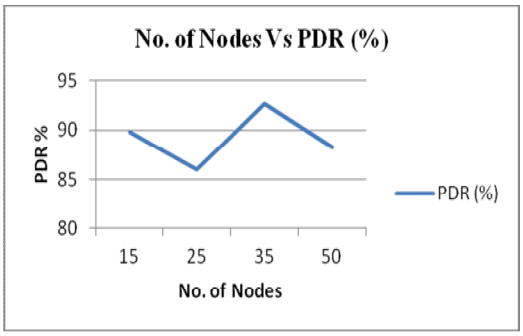

Fig.4 . Ratio of PDR Vs Number of Nodes

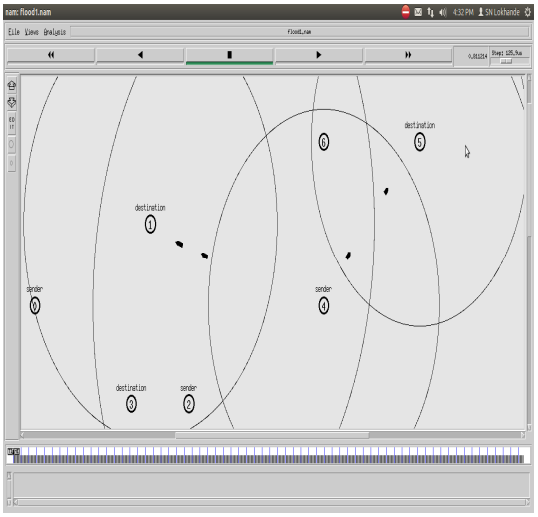

Fig. 5 . Simulated Network for Data flooding attack

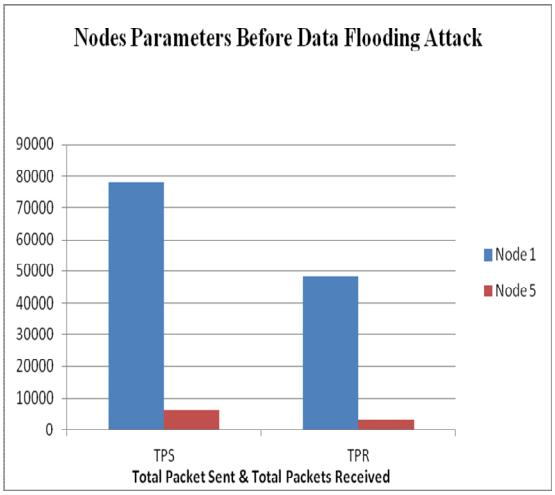

Fig. 6. Parameters before data flooding attack

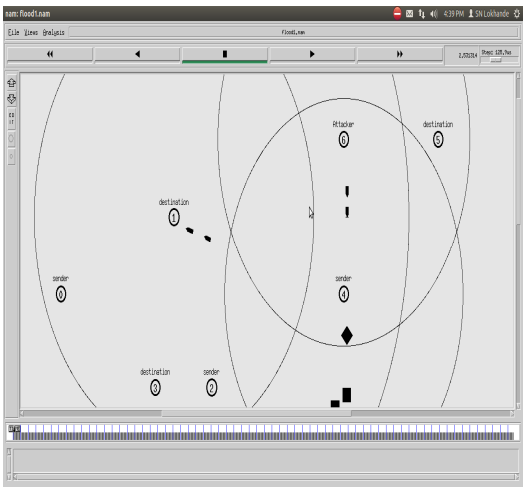

Fig. 7. Simulated network after data flooding attack

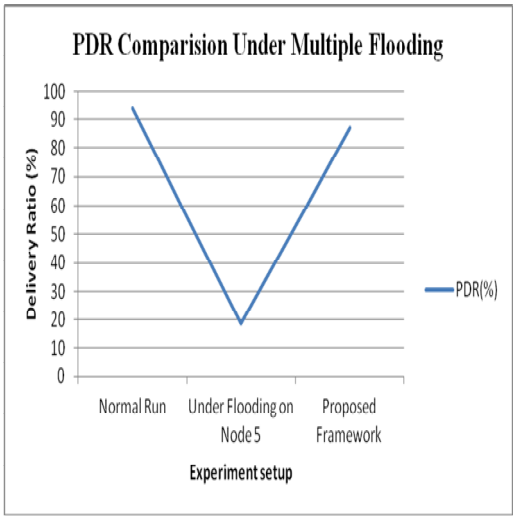

Fig. 8. Packet Delivery Ratio

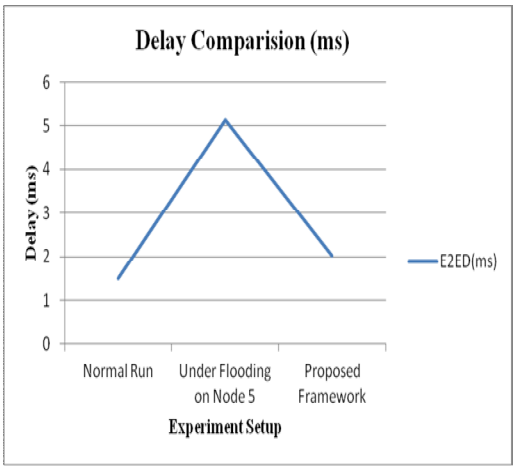

Fig. 9 . End to End Delay

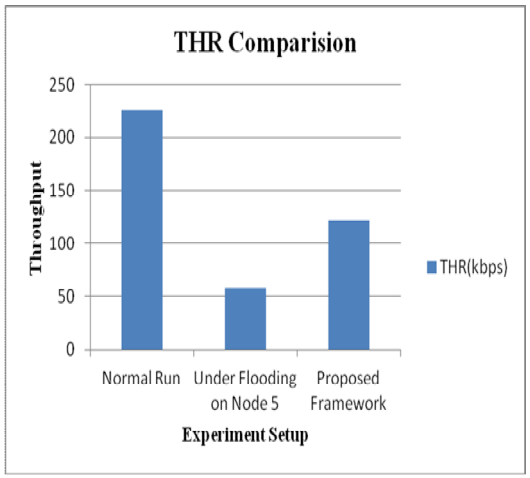

Fig. 10. Throughput Comparison

CONCLUSION

This research paper narrates creation, deployment and cross validation of an intrusion detection and response model for Ad Hoc network against data flooding DoS attack. Extensive simulations were performed to evaluate the performance of proposed framework in NS-2 simulator. The statistical validations are also carried out with the help of Chi-square approach. The fitness of our proposed framework is tested under the various scenarios and the results obtained prove that our proposed framework is good for the intrusion detection and prevention in the Ad Hoc network.

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2] M. Ilyas, The Handbook of Ad Hoc Wireless Networks, CRC Press, 2003.

[3] W. Stallings, Wireless Communication and Networks, Pearson Education, 2002.

[4] J. Schiller, Mobil communication. Addison-Wesley, 2000.

[5] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance", James P. Anderson Co., Fort Washington, 1980.

[6] Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer, Vol. 17, 2006.

[7] Vinay P.Virada , "Intrusion Detection System (IDS) for Secure MANETs: A Study", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 6, ISSN 2250-3005(online) October 2012.

[8] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET", International Symposium on Autonomous Decentralized Systems (ISADS '09), pp.1-6, 2009.

[9] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, 2004.

[10] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", Proceedings of the international multi conference of engineer and computer science, Vol. 2, 2010.

[11] Imad Aad, Jean-Pierre Hubaux, Edward W. Knightly, "Denial of Service Resilience in Ad Hoc Networks" , in Proceedings of the 10th annual international conference on mobile computing and networking , pp. 202-215, 2004.

[12] John Bellardo and Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", in Proceedings of the 12th Conference on USENIX Security Symposium – Vol.12.

[13] Safdar Ali Soomro,Sajjad Ahmed Soomro, Abdul Ghafoor Memon, Abdul Baqi, "Denial of Service Attacks in Wireless Ad hoc Networks" , Journal of Information & Communication Technology , Vol. 4, No. 2, pp.1-10

[14] Minakshi Bhardwaj ,G.P. Singh , "Types of Hacking Attack and their Countermeasure" , International Journal of Educational Planning & Administration. Volume 1, Number 1, pp. 43-53.

[15] IAad, J.P, Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks", ACM , MOBICOM, Philadelphia, PA, USA, 2004.

[16] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[17] Mukherjee, L. Heberlein, and K. Levitt, "Network intrusion detection" , IEEE Network, Vol. 8, No. 3, pp. 26-41, May 1994.

[18] Y. K. Chan et al., "IDR: An Intrusion Detection Router for Defending against Distributed Denial-of-Service (DDoS) Attacks" , Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'04), pp. 581-586, May 2004.

[19] B. Sun, K. Wu, U. W. Pooch, "Alert Aggregation in Mobile Ad Hoc Networks", Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe'03) in conjunction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003.

[20] Raj P N, Swadas P B, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issue, Vol. 2, pp 54-59, 2009.

[21] L. Buttyán , J. P. Hubaux, "Stimulating cooperation in self-organizing mobile Ad Hoc networks" , ACM journal for Mobile Networks (MONET), Vol. 8, No. 5, pp. 579-592, October 2003.

[22] H. Luo, S. Lu, "Ubiquitous and robust authentication services for Ad Hoc wireless networks", Department of Computer Science, UCLA, Technical Report TR-200030, 2000.

[23] Brinkley , W. Trost, "Authenticated Ad Hoc routing at the link layer for mobile systems", Wireless Networks, Vol. 7, No. 2, pp. 139-145, March 2001.

[24] Y. Huang, W. Fan, W. Lee, P. S. Yu, "Cross-feature analysis for detecting Ad Hoc routing anomalies", in Proceedings of 23rd International Conference on Distributed Computing Systems, pp.478-487, 2003.

[25] C. Tseng, P. Balasubramanyam, "A specification-based intrusion detection system for AODV", in Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 125-134, 2003.

[26] P. Brutch , C. Ko, "Challenges in intrusion detection for wireless Ad Hoc networks", in Proceedings of Symposium on Applications and the Internet Workshop, pp.368-373, 2003.

[27] O. Kachirski , R. Guha, "Effective intrusion detection using multiple sensors in wireless Ad Hoc networks", in Proceedings of 36th International Conference On System Sciences, pp.57-64, 2003.

[28] N. Stakhanova, S. Basu, J. Wong, "Taxonomy of intrusion response systems", Computer Science, Lowa State University, Technical Report 06-05, 2006.

[29] Kong, H. Lou, K. Xu, D. Gu, M. Gerla, S. Lu, "Adaptive security for multilayer ad hoc networks", Special Issue of Wireless Communication and Mobile Computing, Vol. 2, pp. 533-547, August 2002.

[30] N.Ye , Q.Chen, "An Anomaly Detection Techniques based on a CHI-SQUARE Statistics for Detecting Intrusion into Information System", Quality and Reliability Engineering International, 2001.

[31] N.Ye, X.Li, M.Emran, M.Xu, "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data", IEEE Transaction on Systems, Man & Cybernetics, 2001.

[32] S. P. Alampalayam et al, Intruder Identification and Response Framework for Mobile Ad hoc Networks, Conference proceedings , Conference: 22nd International Conference on Computers and Their Applications, CATA-2007, Honolulu, Hawaii, USA, March 28-30, 2007.

[33] S. P. Alampalayam, classification and review of security schemes in mobile computing, wireless sensor networks, 2010, 2,419-440

[34] Fan-Hsun Tseng et al, A survey of black hole attacks in wireless mobile ad hoc networks, Human-centric Computing and Information Sciences 2011, 1:4 doi:10.1186/2192-1962-1-4

[35] Syed Atiya Begum , Techniques for resilience of Denial of service Attacks in Mobile Ad Hoc Networks, International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.