ISSN:0975-9646
Ghanshyam Prasad Dubey et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,3879-3883

Network Performance investigation in Presence of Multiple Vital Node and IDS in MANET

Ghanshyam Prasad Dubey [1], Prof. Amit Sinhal [2], Prof. Neetesh Gupta [3]

[1]M.Tech Scholar, Information Technology, T.I.T, Bhopal, India.
[2] Professor of Computer Science & Engineering, T.I.T, RGPV, Bhopal, India.
[3] Asstt. Professor of Information Technology, T.I.T, RGPV, Bhopal, India.

Abstract **— A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructure less, multi-hop network. The wireless and distributed nature of MANETs poses a great challenge to system security designers. Although security problems in MANETs have attracted much attention in the last few years, most research efforts have been focused on specific security areas, such as establishing trust infrastructure, securing routing protocols, or intrusion detection and response, none of the previous work proposes security solutions from a system architectural view. In this paper we proposed multiple vital links finding technique that finds vital links and then we apply IDS module on these vital links only and analyze network performance in Denial of service attack and IDS time. Our simulation tested through NS-2 and deploys mobile node structure with resultant value.**

Keywords— AODV, **IDS, routing overhead, packet delivery ratio, NS-2, Multiple Vital Links, Throughput.**

I. INTRODUCTION

Ad hoc network is a wireless network without having any fixed infrastructure. Each mobile node in an ad hoc network moves arbitrarily and acts as both a router and a host [1]. A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. In these and other applications of ad hoc networking, security in the routing protocol is necessary in order to guard against attacks such as malicious routing misdirection, but relatively little previous work has been done in securing ad hoc network routing protocols. Secure ad hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power (energy) of each individual node in the network. Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information quickly as conditions change, requiring more rapid and often more frequent routing protocol interaction between nodes than is typical in a traditional (e.g., wired and stationary) network. Expensive and cumbersome security mechanisms can delay or prevent such exchanges of routing information, leading to reduced routing effectiveness, and may consume excessive network or node resources, leading to many new opportunities for possible Denial-of-Service attacks through the routing protocol.

II. RELATED WORK

The security problem and the misbehavior problem of wireless networks including MANETs have been studied by many researchers, e.g., [2], [3], [4], [5]. Various techniques have been proposed to prevent selfishness and misbehavior in MANETs. Here we describe some security mechanism previously done by the researchers.

Albers et al. proposed a distributed and collaborative architecture of IDS by *using mobile agents* [6]. A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS. Two types of data are exchanged among LIDS: security data (to obtain complementary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion). In order to analyze the possible intrusion, data must be obtained from what the LIDS detect on, along with additional information from other nodes.

Sterne et al. proposed a dynamic intrusion detection hierarchy that is potentially scalable to large networks use clustering.

This method is similar with Kachirski and Guha, but it can be structured in more than two levels [7]. Thus, nodes on first level are cluster heads, while nodes on the second level are *leaf nodes*. In this model, every node has the task to monitor, log, analyze, respond, and alert or report to cluster heads.

B.Sun Proposed Zone Based IDS (ZBIDS). In the system, the MANET is spitted into non overlapping zones (zone A to zone I) [8]. The nodes can be categorized into two types: the intra zone node and the inter-zone node (or a gateway node). Each node has an IDS agent run on it. This agent is similar to the IDS agent proposed by Zhang and Lee. Others components on the system are data collection module and detection engine, local aggregation and correlation (LACE) and global aggregation and correlation (GACE). The data collection and the detection engine are responsible for collecting local audit data (for instance, system call activities, and system log files) and analysing collected data for any sign of intrusion respectively.

III. ARCHITETURE OF PROPOSED SCHEME

In the field of mobile ad hoc networks routing protocols, there are lot of problems to be tackled such as Quality of service, power awareness, routing optimization and security issues. My main interest is in the security issues related to routing protocols in MANETs. Here we work on the multiple vital node detection [1]. The vital (critical) node test detects nodes whose failure with malicious behavior spread over the network that disconnects or significantly degrades the performance of the network (i.e. introduces unacceptably long alternative paths). Fig 1 represents the attacker free network by that numbers of nodes are communicate with each other though a common link for example if A3 want to send their data to C3 then data first come to B then C then C3. In this fig number of nodes are depends on a single node and a single path through that node. These nodes are the vital or critical nodes and the link between them are called critical link. Attackers or malicious nodes jam that type of network by sending the huge number of data and routing packets through a common link then congestion occur in the network. Single attacker not affect the network easily but multiple critical nodes are easily destroyed that type of network. Fig 2 show the network affected by malicious nodes.

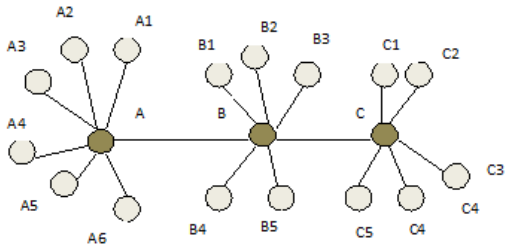

Figure 1 Simple attack free communication among the nodes

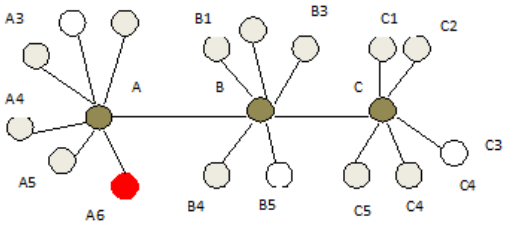

Figure 2 Communication in the presence of attack on critical nodes.

In this figure the nodes A, B and C are the critical nodes. The link A to B and B to C or vice versa having a capacity to forwarded maximum amount of data suppose 2 megabytes/sec. And the capacities of sending data of connected nodes are also limited and each and every node in the network is do their work under limitation. Now the malicious nodes are uncertainly deliver routing packets and data packets in the network by that congestion occur in the network.

IV. PROPOSED SOLUTION

As nodes in mobile ad hoc networks have a limited transmission range, they expect their neighbors to relay packets meant for far off destinations. These networks are based on the fundamental assumption that if a node promises to relay a packet, it will relay it and will not cheat. The reputations of the nodes, based on their past history of relaying packets, can be used by their neighbors to ensure that the packet will be relayed by the node. Here we present an intrusion detection scheme (IDS) to detect and defend against malicious nodes' attacks in MANET. The IDS are apply on the critical nodes because it is the perfect location to identify misbehavior of connected nodes. If the possibility of congestion will occur in the network then senders are reduce their sending rate. If the channel continues to be congested because some sender nodes do not reduce their sending rate, it can be found by the destination. It checks the previous sending rate of a flow with its current sending rate. When both the rates are same, the corresponding sender of the flow is considered as an attacker.

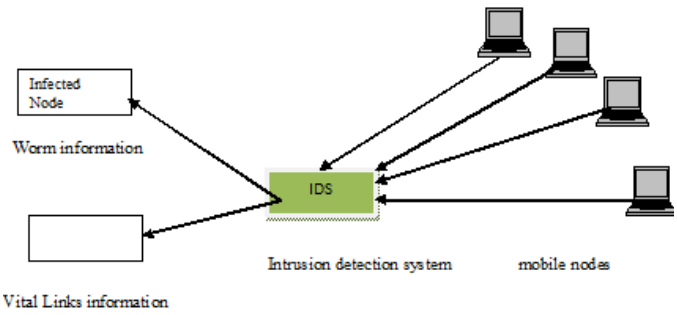

Figure 3 Architecture of intrusion detection system

Once the malicious nodes are identified kill those nodes. This type of node/s are continuously sending the control packets and data packets in the network, due to that neighboured nodes are not establish strong connection in the network.

V. SIMULATION OF IDS

In simulation part there are seven modules which are ns-simulation, trace file, nam file, x-graph, packet receive, packet loss, C++ package, awk utility. Ns-Simulation module simulates the scenario of the wireless network, where antennas of different frequencies are simulated, connections are established and the traffic flows as given in the instructions. Trace file is generated after running the simulation; two files are created trace file and nam file after the simulation ends.

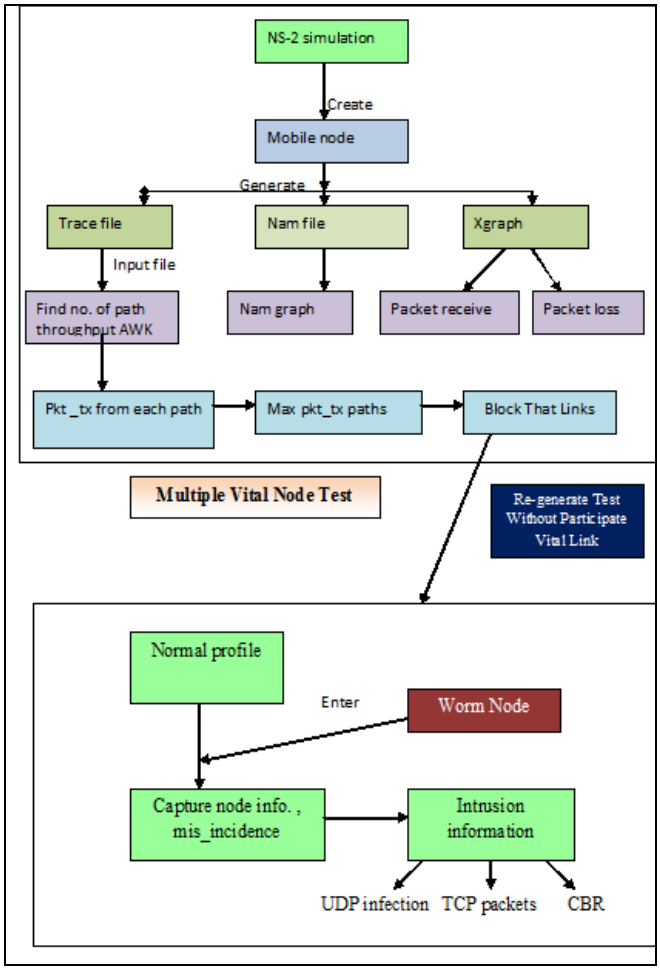

Figure 4 Simulation Architecture

A. Simulation Environment

The simulator we have used to simulate the ad-hoc routing protocols in is the Network Simulator 2 (ns) [9] from Berkeley. To simulate the mobile wireless radio environment we have used a mobility extension to ns that is developed by the CMU Monarch project at Carnegie Mellon University.

B. Simulation Parameter

We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc.

Simulator Used	NS-2.31
Number of nodes	50
Dimension of simulated area	800m×600m
Number of critical nodes	4
Number of malicious nodes	2
Routing Protocol	AODV
Simulation time	35 sec.
Traffic type (TCP & UDP)	CBR (3pkts/s)
Packet size	512 bytes
Number of traffic connections	5,30
Node movement at maximum Speed (m/s)	random
Transmission range	250m

Table 1 Simulation parameter

According to above table 1 we simulate our network.

C. *Performance Evaluation*

There are following different performance metrics have showed the results on the basis of following:

*Routing overhead***:** This metric describes number of routing packets transmitted for route discovery and route maintenance need to be sent so as to propagate the data packets.

*Average Delay***:** This metric represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It is measured in seconds.

Throughput: This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps. It can also be defined as the total amount of data a receiver actually receives from sender divided by the time taken by the receiver to obtain the last packet.

Packet Delivery Ratio: The ratio between the amount of incoming data packets and actually received data packets.

VI. SIMULATION RESULT

A. Infection Percentage in the Presence of Malicious Node

Here is analysis of infection percentage spreading on network, basically malicious node enter on network at 1st second and send malicious packet to network, if any node receive that infected packet so that mobile node infected

through attacker activity. In this simulation after 19th second network infected via malicious activity.

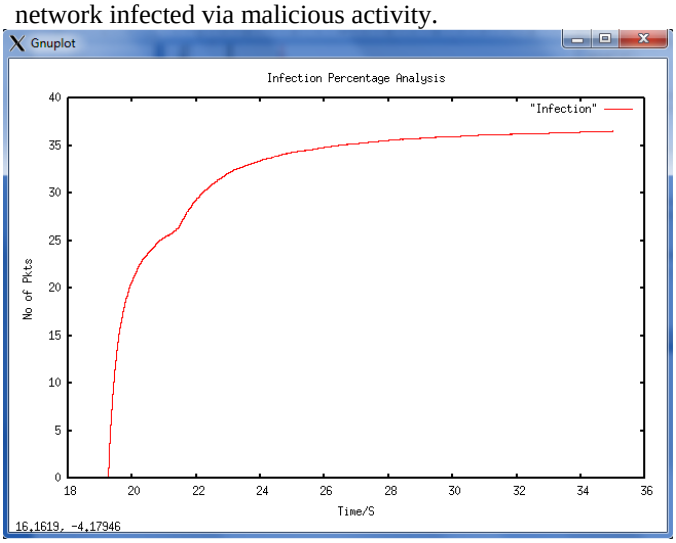

Figure 5 Infection Percentage Analysis

B. Throughput Analysis Normal, Malicious and IDS Case

In wireless communication networks, such as packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain wireless network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. Here is throughput result at normal , malicious and IDS time, if malicious node come into network so no data packet transmitted in that case result will be zero but after applying IDS module on to the network so the throughput become same as normal time.

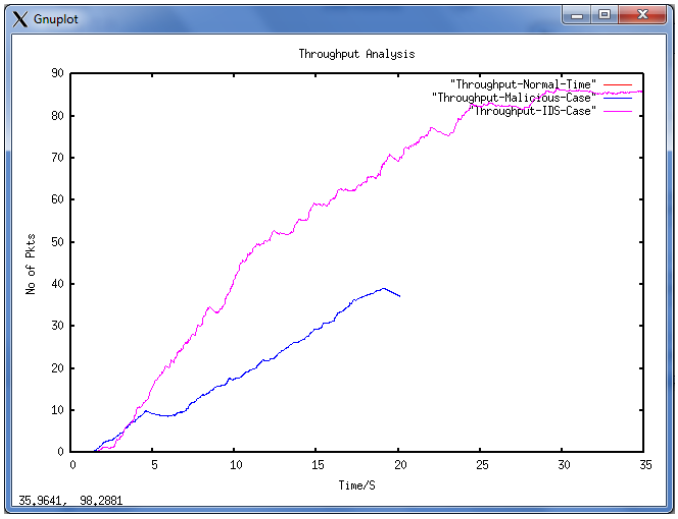

Figure 6 Throughput Analysis

C. Packet Delivery Ratio Analysis

Packet delivery ratio means ratio between data receives per unit out of transmit packet at particular time unit. Our result provide good result from start to till end of simulation time that result give average packet delivery ratio 90%. At IDS case but malicious node time PDF value nearly 80% at 19th second.

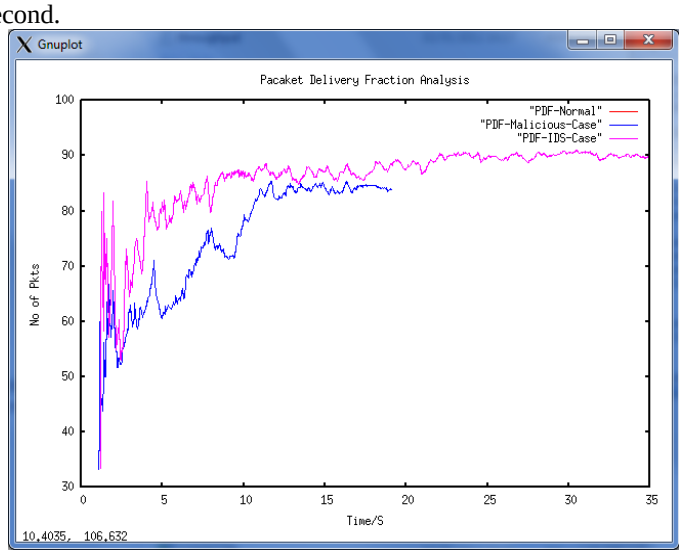

Figure 7 Packet Delivery Ratio Analysis

D. Routing Overhead Analysis

Graph 8 shows routing load before Malicious, after Malicious and after IDS module, here red lines a show routing overhead in the case of before Malicious that is minimum, in the presence of malicious node the routing overhead is maximum. Since the malicious is attack the network at the time of 19 sec. so the routing load is tend to increase. These results show that the original data can't be transmitted. When IDS modules attached with bottleneck nodes, routing overhead is decrease while malicious node present. And also our original data transmitted by the genuine sender to genuine receiver.

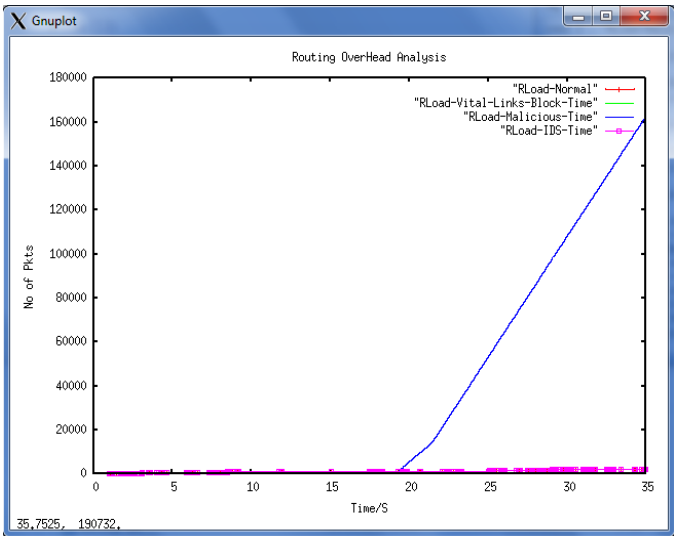

Figure 8 Routing Overhead Analysis All Cases

E. Cost Effectiveness

As per local IDS scheme to obtain cost difference between previous and proposed methods are:

According set theory

$M = \{m_1, m_2 \ldots\ldots m_n\}$ // Number of mobile nodes

I = {i_1,i_2……i_n} // Number of IDS in case of local IDS
M and I both set is equal and cost of i_1 is c_1 , cost of i_2 is c_2
Hence total cost of IDS
C = {c_1 + c_2 + c_3……c_n} // for n nodes

$$\textbf{i.e. } C = \sum_{i=1}^{n} c_i \text{……. (1)}$$

After applying IDS at only vital links so that IDS is not requires each and every node
V = {v_1, v2, ……..., v_k} // number of vital links
V⊂ M and k < n, and cost of each IDS is c_1
So total cost at the time of vital link is
C_V = {c_1+c_2+……+c_k} // k times

$$\textbf{i .e. } C\_V = \sum_{i=1}^{k} c_i \text{……. (2)}$$

'k' is less than 'n' every time
Than C > C_V
Hence the total cost difference given by

$$C_{Reduce} = 100\ (1 - C\_V/C)$$

VII. ABOUT THE DEMONSTRATION

In this demo, we analyze network performance on the basis of network parameter like throughput, routing load, packet delivery ratio and average end to end delay etc. in our simulation we check network behavior in presence of a attacker node and intrusion detection system.

VIII. CONCLUSION

Finally number of analysis base in MANET environment, we conclude following points:-
1. It provides secure communication between senders to receivers.
2. Our IDS recover 100% data in presence of attacker node and block malicious node through IDS.
3. IDS are implemented in vital links only that reduces the cost of IDS.
4. End to end delay is increased by 50 percent in presence of attacker node.
5. Routing overhead is increased drastically in presence of attacker node.
6. We also analyze infection is spreads over the network near by 36 percentage till the end of simulation.

Here we show the conclude result table 3.

Overall Summery					
Parameter		Normal Case	Vital-Link-BlockTime	Malicious Time	IDS Case
SEND	=	1162	51	708	1162
RECV	=	1044	0	531	1044
ROUTINGPKTS	=	2380	252	162874	2380
PDF	=	89.85	0	75	89.85
NRL	=	2.28	0	306.73	2.28
Average e-e delay(ms)	=	507.81	0	762.99	507.81
No. of dropped data (packets)	=	111	32	115	111
No. of dropped data (bytes)	=	85508	12776	91332	85508

Table 2 Conclude result table

REFERENCES

[1] Kamlesh Chandravanshi , Mukesh Bathre" Intrusion Detection System for Wireless Ad-hoc network" COMPUTER AND NETWORK TECHNOLOGY Proceedings of the International Conference on ICCNT 2009, *Chennai, India, 24 - 26 July 2009*
[2] L. Zhou and Z.J. Haas, "*Securing Ad Hoc Networks*," IEEE Network Magazine, vol. 13, no. 6, Nov./Dec. 1999.
[3] F. Stajano and R. Anderson, "*The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks*," Proc. Seventh Int'l Workshop Security Protocols, 1999.
[4] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "*Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks*," Proc. IEEE Int'l Conf. Network Protocols (ICNP '01), 2001.
[5] I. Aad, J.-P. Hubaux, and E-W. Knightly, "*Denial of Service Resilience in Ad Hoc Networks*," Proc. MobiCom, 2004.
[6] P. Albers, O. Camp, et al. "*Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches*". Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002
[7] D. Sterne, P. Balasubramanyam, et al. "*A General Cooperative Intrusion Detection Architecture for MANETs*". Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005
[8] B. Sun, K.Wu, and U. W. Pooch. "*Alert Aggregation in Mobile Ad Hoc Networks*". The 2003 ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003
[9] The Network Simulator – ns-2 http://www.isi.edu/nsnam/ns