International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 24 Issue 9 – JUNE 2017.

PREDICTING AND PREVENTING THE DENIAL OF SERVICES ATTACKS USING TRUST BASED FUZZY LOGIC MECHANISM

T.Saraswathi#1, V.Umarani*2 and M.Kumaran$3

#Jaya Engineering College, Thiruninravur-602 204,Tamilnadu

*Jaya Engineering College, Thiruninravur-602 204,Tamilnadu, India

$ Jaya Engineering College, Thiruninravur-602 204,Tamilnadu, India

Abstract: Tremendous growth towards mobile devices and wireless networks has emerged into the new field of study, Mobile Adhoc Networks (MANET). MANET is a self-organized and reconfigurable environment that doesn't depend on any centralized system. Routing efficiency and data sharing are one of the significant parameters in MANET environment. In this paper, we have proposed trust based fuzzy logic mechanism to detect the Denial of Service attacks. Firstly, the nodes are randomly deployed and distributed in MANET environment using OLSR and ONION routing protocols. Multi-Point Relay (MPR) is used for controlling the packets throughout the network using two-hop neighbor's communication systems. Reputation value for each node is estimated. Based on the estimated value, the node's behavior is classified into low, medium and high priority class. The nodes reside at high priority is used for further analysis. After receiving the authorization from Trusted Authority (TA), the behavior of nodes is studied and detected the malicious nodes. Experimental study has shown the efficiency of the proposed system in terms of packet loss ratio and throughput.

Keywords: MANET, Routing efficiency, Data sharing, Trust and Reputation models.

I. INTRODUCTION

From the day the Internet has originated, the problems faced by the client and the server are existing in the wireless scenario. One of the most prominent attacks that still revolve around is Denial of Service (DoS) attacks [1]. DoS and Distributed Denial of Service (DDoS) are growing concerns as more people use on-line services for e-commerce, banking, and social networking. DoS attacks prevent authorized users to access the available resources and services. The attacker attempts to prevent legitimate users from accessing the information or services by sending large number of fake requests, whereas in a DDoS attack, the master owns millions of insecure machines called zombies which act according to the master command to overload the victim with huge volume of packets.

There are two general forms of DoS attacks: those that crash services and those that flood services. In most cases DDoS attacks involve forging of IP sender address so that the location of the attacking machines can't easily be identified. The Key feature of DDoS includes distributing the attack across hundreds or thousands of compromised hosts (often residing on different network) and coordinating the attack among the hosts. In the summer of 1999, the Computer Incident Advisory Capability (CIAC) reported the first DDoS attack incident and most of the DoS attacks since then have been distributed in nature [2]. Most of the DDoS flooding attacks launched have tried to make the victim's service unavailable.

Denial of service (DoS) attack is Distributed Denial of service (DDoS) attack since it is launched concurrently to numerous machines. DDos attacks are not new disturbance to internet, they came back late in August 1999 and after that incessantly their severity is growing. Some recognized DoS attacks are SYN Flood, teardrop, smurf, ping of death [3]. There have been large scale attacks targeting many high profile websites [4]. These sites include twitter, facebook, Amazon etc. There are varieties of DDoS attacks as classified in [5]. However, the most common form of DDoS attacks is a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination. DDoS attacks cannot be detected and stopped easily because forged source addresses and other techniques are used to conceal attack sources [6].

The rest of the paper is organized as follows: Section II depicts the related work; Section III depicts the proposed work; Section IV presents the experimental analysis and concludes in Section V.

II. RELATED WORK

Denial of Service attacks on servers is the major concern of network security in today's world. The DOS attacks aims at the HTTP request of the clients. The traffic sampling is a technique that bifurcate the network traffic on the basis of parameters such as number, average length of flow, identifying the traffic of interest, etc. The author in [7] use traffic sampling which samples arrived HTTP requests and registers the information of traffic characteristics by scheduled rules. The information such as source IP, source port, destination IP, destination port, protocol type, start and end time of the HTTP request packet is registered. With the help of the registered information the attacking traffic is classified by measuring the accessing time content. The author in [8]studied Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Sample-by-sample detection method is used for tackling the DOS attacks. Moreover the traffic can behave falsepositive or false-negative to confuse the server, need to detect and mitigate such type of behavior of network traffic. The author in [9] proposed a Rateguard system that deals with such types of attacks based on leaky-bucket based rate control technique. The author in [10]studied false-positive and false-negative rates for mitigating the model-based attacks.

Authentication is one of the major issues for the server to decide the legitimate user. Client puzzles helps server for authentication and association. Server sends the puzzle to the requesting client, after solving the puzzle successfully client is able to access the services on the server. The puzzle should be time dependent so that client can get only limited time to solve it. The author in [11] proposed a lightweight mechanism to defend against DoS attacks on 802.11 networks. Client puzzles are implemented on the access points in WLAN's in order to defend the resource depletion attacks. The author in [12] studied client puzzles based on partial collisions in hash functions. Due to which the fine-grained control over the puzzles is possible which is useful for the access control. The author in [13] proposed a client transparent technique. They embedded an authentication code in the port number field of TCP packet and used IP level filtering to counter the DOS attacks.

The DOS attacks also aims at the TCP, ICMP, UDP, etc. Mostly the flood attacks are sent on them. Thresholds are used to detect such type of flood attacks and defend against them. The author in [14] studied a Poseidon framework which mitigates the distributed denial of service attacks. Interest flooding in named data networks (NDN) which exploits the key architectural features of NDN is mitigated by setting up the threshold which limits the rate of incoming interests from the interface. The author in [15] studied a two-tier coordinated defense scheme against distributed denial of service attacks which uses flood detection by threshold and online monitoring is done.

III. PROPOSED WORK

This section depicts the working of proposed algorithm via modules.They are explained as follows:

a) Creation of the topology

Consider a group of nodes which are randomly and uniformly distributed in square size of 1000 * 800m. The transmission range of node is set to 250m with speed of 5m/ms. The data traffic is set to 100 packets per millisecond with queue length of 50 packets. The overall network performance is investigated using fuzzy logic system. The proposed algorithm consists of three processes, namely,

i) Detection of misbehaving nodes based on the observed evidences.
ii) Introduction of geographic routing and greedy algorithm to transfer the data via selected shortest path. And also to retrieve the data securely from present position of node's.
iii) Simulations on set of nodes to estimate the effectiveness and efficiency of the trust.

b) Denial contractions with fictitious node mechanism

Each node in the network communicates with other nodes based on the given information. Using Multi-point Relays (MPR), the optimization of node is done for control packets throughout the network. MPR operates in both one-hop neighbors and two-hop neighbors. By minimizing its MPR selections, anode is able to transmit messages to all two-hop neighborswith minimal duplication. Thus, both topology controlmessages and data packets are only forwarded by this mini-mal MPR set, allowing for fewer duplicate messages whilemaintaining network-wide coverage.

c) *Trusted fuzzy logic with fictitious nodes:*

Trust is an important factor in the MANET environment. In order to select the trustworthy node for secured transmission process, we have adopted a trust based fuzzy logic mechanism.Firstly, the behavior of the nodes is observed and its pattern is recorded. The behavioral pattern is studied using fuzzy logic mechanisms. The reputation values of each node is calculated and classified into three classes, namely, low, medium and high. The aim of this classification process is to minimize the relay and to maximize the packet delivery ratio. The nodes which are classified under high class are treated as the trusted authority nodes.

High classes of nodes contain authorized evidences from delegation history and forward history.Then, the greedy algorithm is applied over the nodes of high classes. The task of greedy algorithm is to transfer the data under selected shortest paths. When a node is misbehaving iTrust introduces a periodically available Trust Authority which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then, Trusted Authority (TA) could punish or compensate the node based on its behaviors.

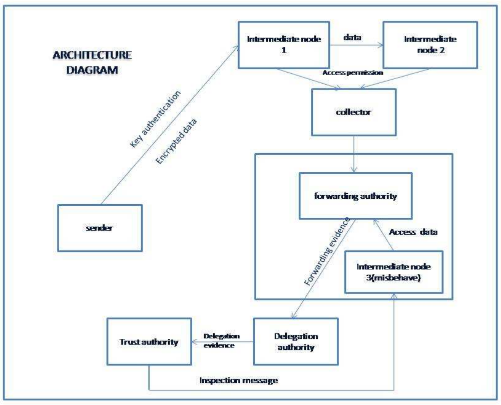


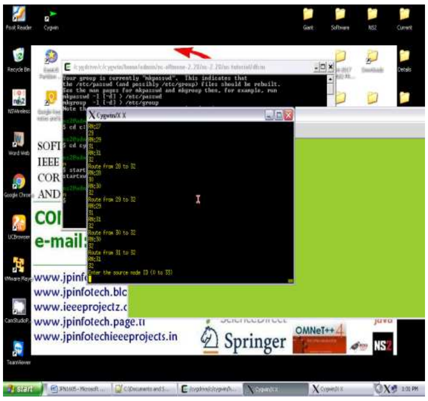
Fig.1. Proposed architecture

IV. EXPERIMENTAL RESULTS

This section depicts the simulation analysis of our proposed technique. Simulation study is carried out in NS2 programming language.The simulation parameters are listed in table 1.

No. of Nodes	50 nodes
Transmission range	250m
Transmission speed	5m/ms
Data traffic	100 packets/ms
Queue length	50 packets
Protocols	OLSR and ONION routing protocols

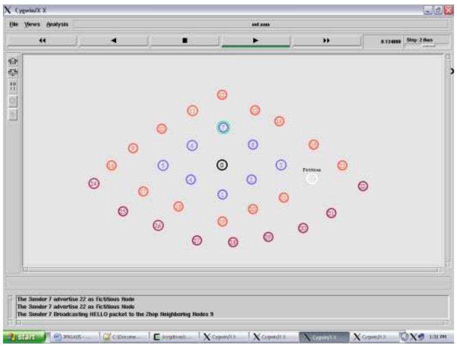
Table 1. Simulation parameters



```
Your group is currently "mkpasswd".  This indicates that
the /etc/passwd (and possibly /etc/group) files should be rebuilt.
See the man pages for mkpasswd and mkgroup then, for example, run
mkpasswd -l [-d] > /etc/passwd
mkgroup  -l [-d] > /etc/group
```

```
RN:27
29
RN:29
31
RN:31
32
Route from 28 to 32
RN:28
30
RN:30
32
Route from 29 to 32
RN:29
31
RN:31
32
Route from 30 to 32
RN:30
32
Route from 31 to 32
RN:31
32
Enter the source node ID (0 to 33)
```

Fig.2. Initialization of the nodes



```
The Sender 7 advertise 22 as Fictitious Node
The Sender 7 advertise 22 as Fictitious Node
The Sender 7 Broadcasting HELLO packet to the 2hop Neighboring Nodes 9
```

Fig.3. Determination of the fictitious nodes

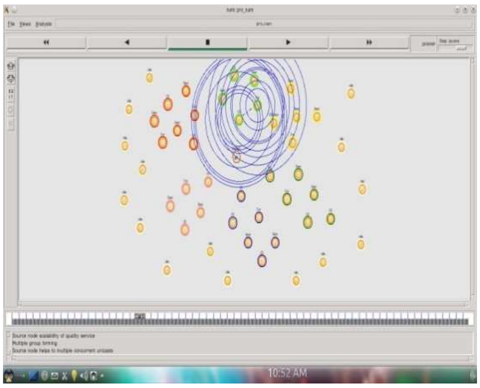


Fig.4. Distribution of channel frequency using ONION routing protocol

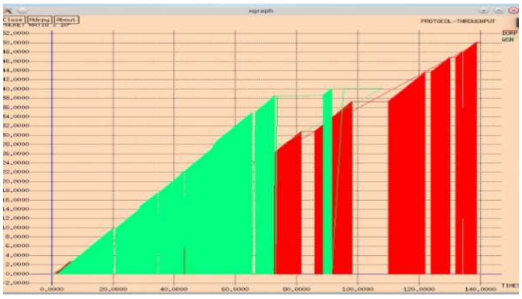


Fig.5. Packet loss ratio analysis

From the fig.5., it is estimated that our proposed technique significantly reduces the packet loss ratio than the existing works.

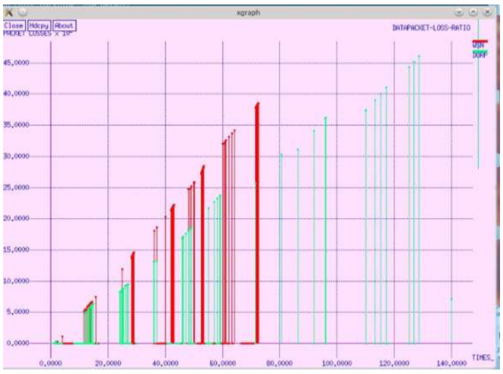


Fig.6. Throughput analysis

From the fig.6, it is inferred that our proposed technique significantly increases the throughput rate than the existing techniques.

V. CONCLUSION

With the rapid development made in wireless technologies, the research on mobile computing has gained much interest among the researchers. Mobile Ad-hoc Network usually has a dynamic shape and a limited bandwidth. Routing is one of the key issues in MANETs due to their highly dynamic and distributed nature; the use of mobile networks is growing very fast. The performance of a mobile ad-hoc network depends on the routing scheme employed, and the traditional routing protocols do not work efficiently in a MANET. In this paper, we have proposed trust based fuzzy logic mechanism to detect the malicious nodes that causes denial of service attacks. The nodes are randomly deployed using OLSR and ONION protocols. The reputation value of each node is estimated. After receiving the authorization from Trusted Authority (TA), the behavior of nodes is studied and detected the malicious nodes. Experimental study has shown the efficiency of the proposed system in terms of packet loss ratio and throughput.

REFERENCES

[1] Nadav Schweitzer et al, “Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes”, IEEE Transactions on Mobile Computing, 15 (1), 2016.

[2] Claudio A. Ardagna, Mauro Conti, Mario Leone, and JulindaStefa, “An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments’’ July- Sept 2014.

[3] Robinpreet Kaur &Mritunjay Kumar Rai, A Novel Review on Routing Protocols in MANETs, Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012.

[4] Perkins CE, Bhagwat P (1994) Highly Dynamic DestinationSequenced Distance-Vector Routing (DSDV) for Mobile Computers. Proceedings of ACM SIGCOMM 1994:234–244.

[5] Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989) A Loop Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review, Volume 19, Issue 4:224–236.

[6] Chiang C-C, Wu H-K, Liu W, Gerla M (1997) Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. Proceedings of IEEE SICON:197–211

[7] Johnson. D and Maltz. D. A, “Dynamic source routing in ad hoc wireless Networks” in Mobile Computing (Imielinski and H. Korth, eds.), Kluwere Academic Publishers, 199

[8] Perkins CE, Royer EM, Chakeres ID (2003) Ad hoc On-Demand Distance Vector (AODV) Routing. IETF Draft, October, 2003, available at http://tools.ietf.org/html/draft-perkins- manet-aodvbis- 00. Accessed 21

[9] Toh C-K (1996) A Novel Distributed Routing Protocol to Support Ad- Hoc Mobile Computing.Proceedings of the 1996 IEEE 15th Annual International Phoenix Conference on Computers and Communications:480–486

[10] Pearlman MR, Samar P (2002) The Zone Routing Protocol (ZRP) for Ad Hoc Networks. IETF draft, July 2002, available at http://tools.ietf.org/id/draft-ietf-manetzone-zrp-04.txt. Accessed.

[11] February 2008 94 A.-S.K. Pathan and C.S. Hong Haas ZJ, Pearlman MR, Samar P (2002) Intrazone Routing Protocol (IARP). IETF Internet Draft, July 2002.

[12] Ramasubramanian V, Haas ZJ, Sirer, EG (2003) SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks. Proceedings of ACM MobiHoc 2003:303–314.

[13] Juan A. Sanchez and Pedro M. Ruiz, “ LEMA: Localized Energy-Efficient Multicast Algorithm based on Geographic Routing,” in Proceedings. Of 2006 31st IEEE Conference on Local Computer Networks in 2006.

[14] J.-E. Garcia, A. Kallel, K. Kyamakya, K. Jobmann, J.-C.Cano and P. Manzoni, “A Novel DSR-based Energy-efficient Routing Algorithm for Mobile Ad-hoc Networks,” in vehicular technology conference 2003 IEEE.

[15] KMwrugan, S. Balaji, P. Siasanka and S.Sbanmugavel , “Cache Based Energy Efficient Strategies in Mobile Ad-hoc Networks,” in 2005 IEEE.

BIOGRAPHY

[1]**T.saraswathi**, received B.Tech(IT) from Veltech Engineering College, affiliated to Anna University. Currently pursuing post graduate in CSE in Jaya Engineering college affiliated to Anna University.

[2]**V.Umarani**, received B.E degree and M.E degree in computer Science and Engineering from Arulmigu Kalasalingam college of Engineering affiliated to Madurai Kamaraj University and Anna University respectively. She has more than 13 years of teaching experience in the field of computer Science and engineering. She is presently working as a Associate professor in computer science and engineering department of Jaya Engineering college, Chennai. Her research interest includes wireless sensor network and network Security.

[3]**Prof.M.Kumaran**, received his under graduate from university of madras and post graduate from Anna University. He has 18 years of experience in teaching. Currently, he is working as HOD/Professor CSE department in Jaya Engineering College. His area of interest is open source system developments, information security and protocol management.