Pattern Based Detection of DDoS Attacks in MANET

Divya Gautam, Vrinda Tokekar

Abstract**:** ***A MANET is a decentralized form of ad hoc network which does not depend on any existent infrastructure such as routers or access points. Distributed Denial of service attack (DDoS) is defined as attacking routing function and taking down the entire operation of the mobile ad hoc network.***

The two primary victims of DDoS attacks are the functions of routing and the battery capacity. The DDoS attack can cause routing table overflow which in turn can potentially cause the infected node floods. The routing overflow is followed by creating a fake route packet to consume the available resources of the participating active nodes. This cause disrupts the normal functioning of legitimate routes. Battery capacity is targeted by keeping it engaged in routing decisions.

In this work the detection of DDoS attacks are done on the basis of patterns of packets incoming in the node. The simulation is carried out in NS2. The attack traffic and non attack traffic patterns are analyzed after simulation depending upon different parameters like bitrate, pdr entropy. The patterns obtained are clearly showing the difference between attack traffic and non attack traffic in MANET environment.

Index Terms**:** ***DDoS, MANET, NS2, bitrate, pdr, delay, entropy.***

I. INTRODUCTION

A MANET is a decentralized form of ad hoc network which does not depend on any existent infrastructure such as routers or access points. In these kind of networks the task of routing and forwarding of packets are taken up by each node participating in the network and packets are forwarded dynamically depending on connectivity and routing algorithms implemented. These networks have the ability to add more nodes anytime as there is no need for set up as in infrastructure based wireless networks. Thus these networks are also referred to as self-configuring, self-organized networks. The IEEE 802.11 Wi-Fi protocol supports ad hoc networks. MANETs have gained importance due to this decentralized mode that it facilitates.

Some of the challenges faced with MANETs are:

a) Constrained Bandwidth: As with other wireless networks, MANETs also face the problem of constrained bandwidth as compared to their wired counterparts.

b) Dynamic Topology: The dynamic topology can be a challenge as an attack on one node can disturb the trust relationship between the nodes in the MANET.

c) Hidden Terminal Problem: The hidden terminal problem can be referred to as the clash between the packets at the receiving node due to simultaneous transmission of the same packets which are not in the vicinity of the sender but are in range to the receiving node.

d) Loss of packets due to erroneous transmission: Due to existence of hidden terminals, network interferences etc. packets are lost in this type of network.

e) Constrained Physical Security: MANETs are more vulnerable to physical security threats than wired networks. Risks of eavesdropping, spoofing and Denial-of-Service (DoS) attacks are more in MANETs. Also due to its decentralized nature, detection of point of failure sometimes becomes a complicated.

II. ATTACKS ON MANETS

Every network tries to ensure the following goals when it comes to security of the network:

a) Confidentiality: Confidentiality in terms of network security means that the information contained in a packet which is transmitted through the network should only be accessed by the receiver and shall be kept secret from other intermediate nodes.

b) Authentication: Authentication of a node is the process of identifying the node based on certain credentials.

c) Integrity: Integrity means that data should be the same throughout its life cycle without any tampering or loss. In other it means the data should be consistent throughout.

d) Availability: Availability means information should be ready to be accessed as and when required by any node given that it is authorized to access it.

e) Non-repudiation: Non-repudiation gives a guarantee that information once sent cannot be denied later.

The primary obstacles are vulnerabilities in MANET system which is self-configured, infrastructure less distributed ad hoc systems. The chances of security threats are very high which makes it almost impossible for companies not to rule out the network security issues.

IT system securities have to stay vigilant 24/7 since DoS/DDoS attacks can take place anytime. Protection against DoS and DDoS can get very tedious due to the difficulty in differentiating fake requests from legitimate requests.

Preventing DDoS/ DoS attacks by detecting and filtering fake requests/ attacker’s requests is barely efficient in providing security.

There are many approaches like intrusion detection and prevention, firewalls which have been used to conquer DoS/ DDoS threats but none of these is capable of

Revised Manuscript Received on June 05, 2019.

Divya Gautam, Department of Computer Science and Engineering, Amity University Madhya Pradesh, Gwalior.

Prof (Dr) Vrinda Tokekar, Department of Information and Technology, Institute of Engineering, DAVV,Indore.

providing complete independent security against dos and DDoS attacks [2].

III. LITERATURE REVIEW

According a report generated by ZDNet in 2014 by Colm Gorey et. al. [3], there are more than 100 DDoS attack that flooded the network at speed of 100GBPS and is increasing at a speed of 20 GBP. A Spanish company was targeted by the single largest attack. Researchers determined the attack by using ATLAS system with data flooded at a speed of 154.69 GBPS.

Jin Ye et. al. [4] proposed a method to detect and mitigate the DDOS attack in large sized networks. This technique is not applicable to small sized networks. Author proposed DDOS mitigation method based on destination IP address, and valid or legitimate source. This method detects the attack using non-parametric cumulative algorithm by analyzing the unusual features of source IP address and destination IP address when an attack occurs on the network.

Mohammed Alenezi et. al. [5] proposed DoS detection mechanism via IDS (Intrusion Detection System). IDS are either software or hardware that detects the intruders that are trying to enter into the network against the network policies. IDS are classified into three categories 1. Host based 2. Network Based 3. Hybrid (combination of both). In host based IDS detection mechanism application and operating system database files are detected and is located on host machine. In network based technique network files are checked and is located on machine that is connected to host that it detects.

Goran Candrlic et. al. [6] proposes that the attack on Cloudfare Network in 2013 was very extreme with 120GBPS and hit the edge of cloudfare network. Report published by e-Security planet, Peak of the attack was 300 GBPS that hit the upstream providers.

K.Murali et. al. [7], a secure zone routing protocol is proposed to detect attacks in MANET. This routing protocol is important because security is provided by secure zone routing protocol (SZRP). SZRP depends on secure discovery of neighbors, Packet routing securely, suspicious nodes detection, and prevent the malicious nodes to disrupt the network and its services or resources. To achieve all this secure key management and secure neighbor discovery is proposed in this paper.

Dr. K.Rama et. al. [8] describes the various basic operations of MANET i.e. administration, routing and security. Both QOS and security has negative impact on the performance of the network. Both affect the performance and services that are required in MANET. This paper discusses two accomplishments i.e. security accomplishment and QOS accomplishment. The main point is to design a protocol to achieve both accomplishments for administration and techniques for IPsec in MANET.

Nitika Singhi et. al. [9] analyze key management issues in MANET. As MANET is using in large network i.e. military, health and weather forecasting. That's why a secure routing protocol is required. Due to dynamic topology of network and self configuring nature of network MANET is used in various applications that need high security. This paper proposes an identity key management protocol using cryptographic and information theoretic security.

IV. SOLUTIONS FOR SECURITY ATTACKS IN MANET

As MANET is used widely in various sectors like military, research and development and many more other areas. So security has become a priority to secure nodes in network for secure transfer of data between nodes. There are various factors that are responsible for alteration of security in network:

1. Dynamic Topology
2. Lack of central server
3. Unreliable Wireless links
4. Nomadic Environment

There are basically two ways to secure network in MANET (Fig 1).

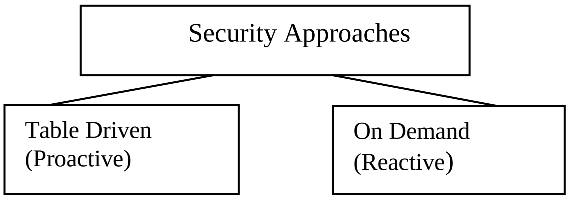


Fig 1: Security Approaches

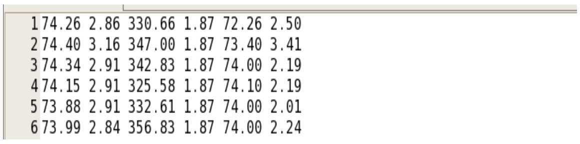
1. Table Driven (Proactive): In this method different cryptographic methods are used to provide security to the network. In this approach the encryption and decryption concept is used. At initial level it is tried to indentify that the coming traffic is normal or attacked traffic by analyzing the attack patterns.
2. On Demand(Reactive) : In this method first attack is identified then action is taken

In [10] Jaya Soni, Ravi Shanker Soni describe that SVM is supervised learning technique. Supervised learning technique is labeling technique. Input and output are previously known that are generated with various system parameters. Behavior of the node is identified by inserting input data with label and output is generated with some techniques. Various examples of technique are neural network, decision tree, and support vector machine (SVM).SVM identifies and detects the nodes which drop the packets on network. SVM classifies the nodes in two classes 1.Normal nodes 2.Malicious Nodes. Neighbors are assigned a trust value.

V. PROPOSED METHODOLOGY

To carry out this work NS2 simulator is used to simulate the MANET environment. The range of communication kept is 250 meters. Every time a trace file is generated when the simulation runs and is saved in the background. With the help of this trace file the six parameters are taken care viz; Bit rate, Packet Delivery Ratio, Delay, Entropy, Change in Bitrate and Change in Delay. These parameters are saved in text file. Total simulation run about 1000 times and then data is recorded every time. The Obtained dataset format (Fig 2) is used for SVM for further analysis of the traffic.

In this work LIBSVM tool is used to apply SVM on the dataset generated. LIBSVM is simple, easy-to-use, and efficient software for SVM classification and regression. It can solve C-SVM classification, nu-SVM classification, one-class-SVM, epsilon-SVM regression, and nu-SVM regression. It also provides an automatic model selection tool for C-SVM classification.



```
1 74.26 2.86 330.66 1.87 72.26 2.50
2 74.40 3.16 347.00 1.87 73.40 3.41
3 74.34 2.91 342.83 1.87 74.00 2.19
4 74.15 2.91 325.58 1.87 74.10 2.19
5 73.88 2.91 332.61 1.87 74.00 2.01
6 73.99 2.84 356.83 1.87 74.00 2.24
```

Fig 2: Format of generated text file

In figure 2 , various columns represent the 6 required parameters to detect the DDoS attacks are as column 1 represents packet delivery ratio, column 2 represents Delay, column 3 bit rate, column 4 Entropy, column 5 change in Bit rate and column 6 represents Change in Delay.

The values obtained for different 6 parameters after 1000 run of simulator, are plotted on GNU plot and obtained the different patterns in normal scenario and attack scnerio

VI. SIMULATION AND RESULTS

When attack is performed in simulated environment on NS-2 the traffic behaves unexpectedly. We analyse the traffic of the simulation. When there is no attack, the traffic found very smooth but when the attack is performed in the simulation the attack effects as follows:

Bit rate: As we perform attack in the simulation the bit rate of the network goes down.(Fig 3 a & b)

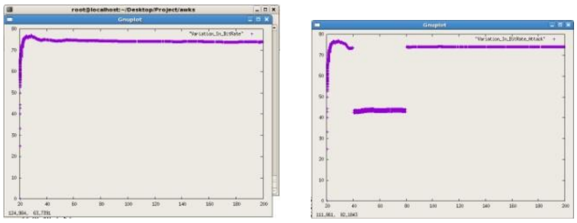


Fig 3 (a) Bit rate in Normal Traffic

Fig 3 (b) Bit rate in Attack Traffic

As we can see in Fig 3 (a & b) that the bit rate in normal scenario goes very smooth but in attack scenario the bit rate goes down (attack is performed from 40 sec to 80 sec).

Entropy: As we perform attack in the simulation the entropy of the network goes high.

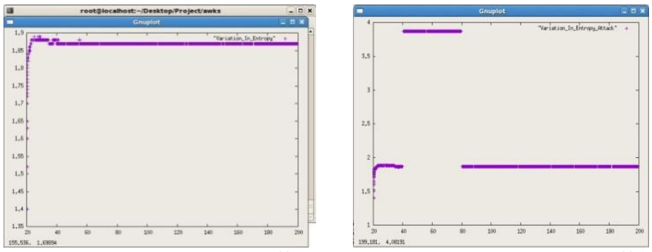


Fig 4 (a) Entropy in Normal Traffic

Fig 4 (b) Entropy in Attack Traffic

As shown in Figure 4 (a & b) the traffic goes unexpectedly low or high.

The attack is performed between time duration of 40 to 80 sec. Fig 5 shows the complete graph of the variation in three main parameters i.e. PDR, Bite Rate and Delay in normal and attack scenario.

It is clearly visible from the Graph if proper monitoring of the system is done on the given parameters then it is quite much possible to detect attack in earlier stages.

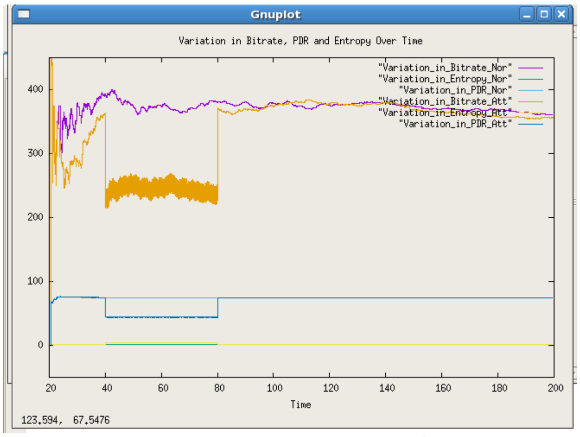


Fig. 5 Complete graph showing the deviation of parameters in attack and normal scenario (based on Bit rate, entropy, pdr).

VII. CONCLUSION

Early prevention of the DDOS attack is possible in this work. For early prevention we use traffic analysis in every 5 seconds. After each step of 5 seconds we hold the simulation and monitor the bit rate, entropy and pdr graph. If the values of bitrate, entropy and pdr go unexpectedly low or high then there could be some attacker nodes in the network. If such situation occurs, we can also apply SVM and PSO on the dataset generated till that moment.

In NS-2 if an attacker node is found then that particular node can be disabled by barring all the communication from that that node.

REFERENCES

1. Jesna. “MANET (Mobile Ad Hoc Network)- Characteristics and Features.” Exploria, 11 Dec. 2018, www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-ad-features/.
2. Giriraj Chauhan,Sukumar Nandi “ QoS Aware Stable path Routing (QASR) Protocol for MANETs”, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).
3. Colm Gorev ”Record number of DDoS attacks in first half of 2014”, 17 July 2014.
4. Jin Ye, Xiangyang Cheng, Jian Zhu, Luting Feng, and Ling Song “A DDoS Attack Detection Method Based on SVM in Software Defined Network”,Hindawi, Security and Communication Networks, Volume 2018, Article ID 9804061, 8 pages.
5. Mohammed Alenezi Martin J Reed School of Computer Science & Electronic Engineering University of Essex name, “Methodologies for detecting DoS/DDoS attacks against network servers” ,2012.
6. Goran candrlic, How Many DDoS Attacks Happen Each Day?September 24, 2013.
7. K.Murali , M.Rahul , G.Venkateshwaran , Dr.S.Pariselvam,” Detecting Attacks in MANET using Secure Zone Routing Protocol”, IJESC,2017.
7. Dr. K.Rama Krishna Reddy, “Improved Protocol Design with Security
8. and QoS over MANET”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology ,2018.
9. Nitika Singhi, Ravi Singh Pippal,” Analysis of Key Management Schemes in MANET”, International Journal of Applied Environmental Sciences (2018).

10. Jaya Soni, R. S. Soni, “A Comparative Study of Machine Learning Technique Based Intrusion Detection in Mobile Ad hoc Network”, International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 5, Issue 7 July 2016
11. M. Guarnera, MANET: Possible Applications With PDA In Wireless Imaging Environment,Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on. Vol. 5. IEEE, 2002.
12. C. Perkins and E. Royer, Ad Hoc On Demand Distance Vector (Aodv) Algorithm,in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99), (New Orleans, Louisiana, USA), 1999.
13. J. Broch, D. Johnson, and D. Maltz, The Dynamic Source Routing Protocol For Mobile Ad Hoc Networks, in Internet draft, IETF Mobile Ad Hoc Networking Working Group, Decembe1998.
14. M. Frodigh, P. Johansson, and P. Larsson, Wireless ad hoc networking -the art of networking without a network, Ericsson Review, no. 4, 2000.
15. Gupta, Anuj K., Harsh Sadawarti, and Anil K. Verma., MANET Routing Protocols Based On Ant Colony Optimization. International Journal of Modeling and Optimization 2.1, 2012.
16. AnjuRan, Sandeep Gupta, “Review on MANETs Characteristics, challenges, Application andSecurity Attacks”- International Journal of Science and Research (IJSR) 2015.
17. Harmanpreet Kaur, P.S. Mann, “Detection of Black Hole Attack in Mobile AD HOC networks a survey” International Journal of Science and Research (IJSR) 2014.
18. Aarti, Study of MANET: Characteristics, challenges,Application and Security Attacks-International Journal of Advance Research in Computer Science and software Engineering,2013
19. M. Corson and J. Macker, Mobile Ad Hoc Networking (Manet): Routing Protocol Performance Issues And Evaluation Considerations, in Request For Comments 2501, Internet Engineering Task Force, 1991.

AUTHORS PROFILE

Ms. Divya Gautam is currently a research scholar at Institute of Engineering and Technology, Devi Ahilyabai Vishwavidhyalaya, Indore and working as assistant professor at Amity University has obtained Masters in Engineering degree from at Institute of Engineering and Technology, Devi Ahilyabai Vishwavidhyalaya, Indore in Information Technology(Specialisation in Information Security) and Bachelor’s of Engineering from Madhav Institute of Science and Technology(Autonomous Institute), Gwalior. She is having 12 years of experience. 5 years as Head of Department –Information Technology at Malwa Institute of Technology, Indore

Prof. (Dr.) Vrinda Tokekar is currently Professor and Head, Dept. of Information Technology, Institute of Engineering and Technology (UTD) and Head, Information Technology Centre (IT Centre), Devi Ahilya University, Indore, (M.P.) (NAAC ’A’ Grade, has obtained Ph.D. (Computer Engineering), 2007, Devi Ahilya University, Indore (M.P.), M.E. (Computer Engineering), 1992, S.G.S.I.T.S., Indore (M.P.), B.E. (Hons.) (Electrical and Electronics Engineering), 1984, BITS, Pilani (Raj.). She has teaching experience of more than 29 years and specialized in the field of Computer Communication Networks, Wireless and Mobile Adhoc Network and Information Security. She has Guided many PhDs.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication