International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-6, August 2020

Mitigation of DDoS Attack in MANET

Zalte S. S., R. K. Kamat, V. R. Ghorpade

***Abstract:** This paper discusses an improved mechanism to mitigate the DDoS attack in Mobile Ad-hoc Network (MANET) without compromising the packet delivery ratio. MANET inherently has geographically sparse mobile nodes more vulnerable to various attackers more radically the DDoS type. Moreover it emanates open medium, absence of centralized authority, lack of clear line of defense that leads to more vulnerability towards secure environment. Since there are no hindrances for non-legitimate nodes, which allows them to freely enter and exit from the network at anytime, various active attacks like black hole, gray hole, DDoS found to jeopardize the network. The DDoS attack discussed predominantly in to present paper, penetrates the network thereby constraining the resources like memory, battery and bandwidth by frequently transmitting fake packets after regular time span thereby starving the computing resources. This paper demonstrates the feasibility of defense mechanism to the DDOS attack in MANET.*

***Keywords:** MANET, active attacks, non-legitimate nodes, DDoS.*

I. INTRODUCTION

1.1 Problem Background, State of the art

The speedy explosion of peripheral wireless devices such as a pad, laptop, smart phones, sensors leads to popularity of MANET[1]. However given the popularity of MANNET touching increasingly widespread and diverse applications, the inherent secure routing is posing more pitfalls owing to MANET's unique characteristics like unpredictable topology, lack of a clear line of defense and secure communication, the movable position of the nodes, decentralized infrastructure, the vulnerability of wireless connections, varying topology and so on[2]. God number of research groups are working on the security issues pertaining to MANNET given the speedy explosion of applications of MANET that necessitates detecting malicious attacks and countermeasures to thwart them. It is without any doubt that the ever increasing MANNET application sphere relies solely on preserving confidentiality and secure delivery of data. Besides, if security is compromised the network performance hampers to a larger extent. Further the dependency of the mobile ad-hoc network such as MANNET infact leads to a negative tendency had any of the nodes misbehave due to tightly couples nature of the network, Scientific literature in this context report variety of misbehavior patterns, that floods the network by constantly sending fake packets within a particular time span or packet dropping or even pretending itself as a destination. Amongst all the Distributed Denial of Service (DDoS) is one of the most dangerous attacks in MANET extremely hard to detect and mitigate. Literature widely discuss the issues of DDoS attack that brings down the network performance in several ways[3].

Revised Manuscript Received on August 21, 2020.
* Correspondence Author

Dr. Sheetal S. Zalte*, Assistant Professor, Department of Computer Science, Pune University, India.
Dr.Vijay Ghorpade, Principal, Department of Computer Science, Bharti Vidyapeeth's College of Engineering, Kolhapur, India.
Dr. R. K. Kamat, Department of Electronics and Computer Science, Shivaji University, Kolhapur, India.

II. DDOS ATTACK IN THE CONTEXT OF MANNET

DDoS is a malicious activity to interrupt regular traffic of a targeted victim, service or network by flooding the fake traffic over the target network. This is generally achieved by involving multiple compromised nodes as sources of attack traffic; the mechanism well known as BOT shown in schematic diagram in Fig. 1. Victim nodes may be computers, PDA, laptops and even IOT devices are the potential targets of DDoS attack resulting in traffic clog up on highway, preventing normal traffic arriving at its desired location.

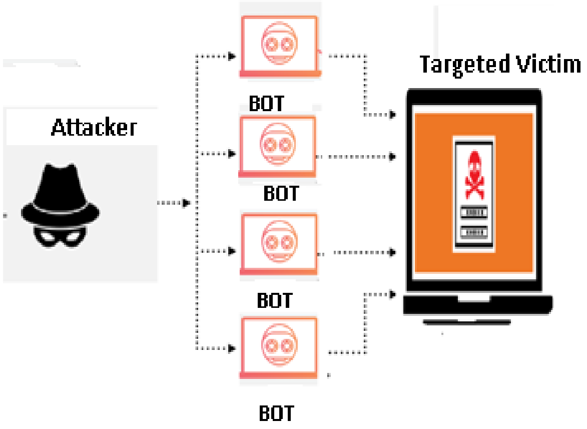

Fig. 1.Distributed Denial of Service

DDoS targets various system resources like energy, bandwidth, memory, and so on. The attacker launches this attack by flooding the network with a large volume of data packets with the help of a large number of nodes distributed throughout the network. This data traffic consumes the bandwidth and/or other resources like energy or battery and engages CPU so much, so that the node discards other legitimate request packets and also prevents transmission of packets from other legitimate nodes. The DDoS target in three scenarios: In the first attack scenario, it targets memory storage and processing resources. This is an attack that targets the memory, CPU by continuously sending fake packets to its neighbors to overload the storage space and consumes memory of the node. In the second scenario, attacker target the battery power of the node, while the third scenario targets bandwidth thereby disrupting the connectivity.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

Thus DDoS vulnerability leads to targeting the energy, memory, and bandwidth and ultimately results in network performance degradation. [4].

DDoS attack is generally accomplished at the application layer, while it uses the network layer to target network transmission.

Subsequently these attackers are harder to repel than DoS assaults. Attacker maliciously floods the network with a tremendous amount of packets; it not only prevents immediate neighbors from accessing wireless media but also denies nodes in 2-hop neighbors of network connectivity. The main symptoms of DDoS attack are:

Suddenly slowing down the network performance (low PDR, Throughput ,Packet Count), not reaching a particular website, non accessibility of data from the website and unusual spam mails.

III. METHODS

Several research groups are working on the techniques to mitigate the DDoS attack. One of the recent papers [5] proposed a machine learning approach in MANET that is Feed Forward Back Propagation Neural Network (FFBPNN) as a classifier and (AODV) routing protocol to mitigate DDoS attack. The author has taken energy consumption and delay of node, as against that of malicious node as a threshold value to identify the malicious node and discard it from the route.

Yet another technique proposed in [6] to prevent flooding attack uses two algorithm Flooding Avoidance and Attacker Isolation algorithm, In flooding avoidance algorithm, number of received requests are checked if it exceeds than the limit, the node is added to the suspicious list or else it is consider as normal node. Isolation algorithm further blocks and isolates any node that wants to flood the network with fake requests for different random IDs that do not exist in the network. DDoS attack can be detected at an initial stage as evidenced in [7] wherein the PDR is calculated for each node and ,if PDR is very high than the normal PDR then that node is marked as malicious and banned for transmission. An extensive review of such many techniques has been presented in [8].

Interestingly a smart Detection system is proposed in[9] which uses a machine-learning algorithm very similar to the Random Forest Tree to obtain classified network data from network devices using the sFlow protocol. One of the recent papers [10] reports the mechanism of monitoring node to detect DDoS attack by sending the Hello packet to the neighboring node and waiting for the reply. If a reply comes within set interval then the neighbor node is considered as ok. Otherwise, the neighbor node considered as victim node. By disabling nodes id, the malicious node can be prevented from network transmission. In view of the reviewed techniques, the mechanism proposed in this

IV. PROPOSED MECHANISM

This section of the paper discusses the solution. As reviewed in previous sections, the DDoS attacker continuously sends the packets without waiting for the reply. Normal node waits for Δt after sending a packet for the reply. But the attacker does not wait for the reply.

Δt=tr- ts

tr-Packet Receiving Time

ts-Packet Sending Time

If Δt< threshold time then attack is considered as DDoS, here threshold time is taken as 2 seconds.

In the implemented mechanism we have calculated request timestamp for each node. Request timestamp calculated by taking difference between current timestamp and last timestamp is as per equation 1.If it is less than threshold value i.e. 2 sec then we increase the malicious behavior count of the respective node.

If the count gets exceed more than 5 times then the respective node is categorized as malicious.

Once, the malicious node is identified then DDoS attack is alarmed the malicious node is banned for 30 sec from taking part in network transmission. The said mechanism expressed in terms of sequence of events is as follows:

I step

$$\text{Calculate RequestTimeStamp} = \int_{i=0}^{T} \text{Request[NodeID]} = \text{TimeStamp} -> \text{TimeStamp} - \text{LastTimestamp} < \mathit{2Sec} \rightarrow \text{DThreshold[NodeID]}{+}{+} \qquad (1)$$

II step

$$\text{if DDoS Attack} = \int_{i=0}^{\text{DThreshold}} \text{DThreshold[i]} > 5 \ \text{->} \qquad (2)$$

then Node is declared as malicious and alarm as DDoS

III step

set flag=0 indicate node is inactive and block particular node block=30 Sec

End if

The above referred steps have been implemented using NS3 simulator as detailed below:

V. RESULTS AND DISCUSSION

Network Simulator (NS3) is a discrete event simulator used to simulate and test the performance of the ad-hoc routing protocols. This is a free software mainly used by researchers and the people who are in education. In the ns-3 simulation, files are used for the simulation, and trace file is generated as output.

Network traffic shows a communication file. Those files can be generated by generating a completely randomized movement and communication patterns with a script.

By giving trace files as input to awk script we plot Gnu plot graphs. The trace file can also be used to visualize the simulation run with a network animator.

As Table I shows, the simulated area consists of no. of mobile nodes. The topology is a flat rectangular area with 700m*700m. The duration of the simulation is 10 seconds.

We have used a constant bit rate (CBR) traffic sources and they distributed randomly within the mobile ad hoc network.

Table- I: NS3 Simulation Parameters

Simulator	NS3
Simulation Area	700 *700
Simulation time	10 Sec
No of Nodes	25,50,75,100,125
Packet size	512 bytes
Routing Protocol	Adhoc On Demand Vector
Attack	DDOS

Attackers	Randomly Attackers
Traffic Source	Constant Bit Rate

In the proposed mechanism, the Ad-hoc On-Demand Distance vector routing protocol is modified.

This routing protocol is more suitable for the MANET because in this protocol routes are created only on demands. In the NS3 simulation environment, we have implemented a DDoS attack in the AODV routing protocol. We have used simulation parameters as shown in Table-I. Here, attackers send useless traffic after some time interval frequently.

But, in the proposed mechanism Attack ratio is calculated by using equation no. (3).It is one, so we can say that almost 100% of attacks detected..

Attack ratio=Attack detected/no. of time attacked (3)

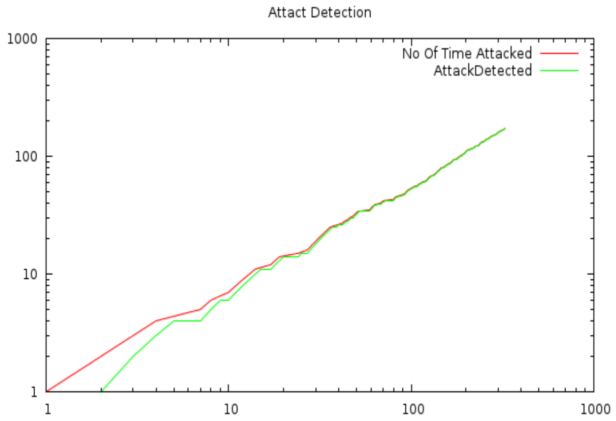

Fig. 2. Attack detected vs no.of times attacked

After detecting attacks, we have prevented them from network transmission. Table II contains PDR of attacked AODV and new AODV. It shows after implementing the proposed mechanism in attacked AODV, we get a 50% increased PDR.

During simulation we have varied no. of nodes from 25 to 125.In fig.3. we have compared attacked AODV vs. NewAODV.

Packet Delivery Ratio:-It is calculated by the ratio of a Total number of successfully captured packets to the number of packets sent by CBR sources.

PDR = Total Packet Received/Total Packets Sent. (4)

Table- II: PDR for Attacked AODV and New AODV

Nodes	Packet Delivery Ratio	
	Attacked AODV	*New AODV*
25	11.17	24.6
50	23.86	40.11
75	27.63	53.66
100	34.47	64.17
125	33.4	60.45

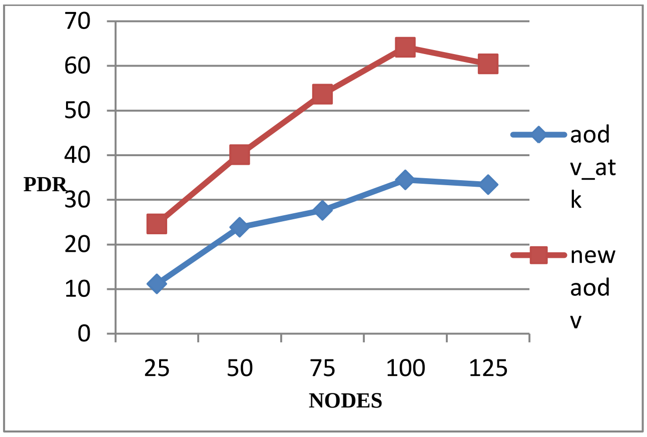

Fig. 3. No. of nodes vs PDR

This metric gives how proposed method works in attacked AODV securely and efficiently.

VI. CONCLUSION

DDOS is an extremely severe and brutal attack in the network. By injecting useless traffic in the network, it slowdowns performance and suspends network services. If it is not detected and prevented in the initial stage, it would cause damage for sensitive data, network services, and legitimate users. Once the DDOS attack implements in routing, it breaks down network performance like decreased Packet Delivery Ratio count. In this paper, we have used threshold timestamp to detect DDOS attack and attacker and we have successfully prevented malicious attackers by blocking them from network transmission. After mitigating the DDOS attack in the AODV routing protocol, we have received a marginally increased Packet Delivery Ratio..

ACKNOWLEDGMENT

I am gratified to my Head of the department Dr. R.K. Kamat, who is always, supported and encourages me to do research work. I am also thankful to my guide Dr.Vijay R. Ghorpade.

REFERENCES

1. D.Djenouri, L.Khelladi, N.Badache,: A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys and Tutorials Journal 7(4), 2-29, December 2005.
2. Deng, H., Li, W., Agrawal, D.P.: Routing security in wireless ad hoc networks. IEEE Communications Magazine 40(10), 70-75, October 2002 .
3. V.V. Timcenko," An Approach for DDoS Attack Prevention in Mobile ad hoc Networks", ELEKTRONIKA IR ELEKTROTECHNIKA, ISSN 1392–1215, VOL. 20, NO. 6, 2014,pp-150-153.
4. Y. Chaba, Y. Singh and P. Aneja, "Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET," Journal of Networks, Vol. 4, No. 3, 2009, pp. 178-183.
5. Jasmine Batra, C. Rama Krishna," DDoS Attack Detection and Prevention using Aodv Routing Mechanism and Ffbp Neural Network in a Manet", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019,pp- 4136-4142
6. Mahmoud Abu Zant and Adwan Yasin," *Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV)"*, Hindawi Security and Communication Networks, Article ID 8249108, Volume 2019,pp-1-12.

7. *Kanchan Kaushal, Varsha Sahni," Early Detection of DDoS Attack in WSN", International Journal of Computer Applications (0975 – 8887) Volume 134 – No.13, January 2016,pp-14-18*
8. Sonali Swetapadma Sahu et.a. “Distributed Denial of Service Attacks: A Review”, I.J. Modern Education and Computer Science, 2014, 1, 65-71 Published Online January 2014 in MECS.
9. Francisco Sales de Lima Filho,1 Frederico A. F. Silveira ,"Smart Detection:An Online Approacher for DOS/DDOS Attack Detection Using Machine Learning" Hindawi Security and Communication Networks Volume 2019, pp-1- 15 pages
10. Dr.Amar Almomani,"A Novel Solution to Handle DDOS Attack in MANET", Research Gate, Journal of Information Security, 2013, 4, 165-179

AUTHORS PROFILE

Dr. Sheetal S. Zalte pursued Bachelor of Computer Science from Pune University, India in year 2002 and Master of Computer Science from Pune, India, in year 2004. She earned her Ph.D. in Mobile Adhoc Network at Shivaji University. She has 11 years of teaching experience in computer science. She is currently working as assistant professor in Computer Science Department at Shivaji University. She has published research papers in reputed international journals and conferences including IEEE and it’s also available online. Her research areas are MANET, VANET ,Blockchain Security.

Dr. Vijay Ghorpade pursed B.E. degree and M.E. degrees in Computer Science and Engineering from Marathwada University, Aurangabad, and Shivaji University, Kolhapur, India, in 1990 and 2001 respectively. In 2008, he earned his PhD degree at SGGSIET, Nanded, India. Presently he is working as Principal at Bharti Vidyapeeth’s College of Engineering, Kolhapur, India. His research interests include network security and ad hoc network. He has published more than 20 research papers in reputed international journals including IEEE.

Dr. R. K. Kamat was born in India 1971.He received his both B.Sc. and M.Sc. in Electronics with distinction in 1991 and 1993 respectively.Further he completed Mphil and PhD in electronics at Goa university. Presently, he is working with Department of Electronics and Department of Computer Science in Shivaji University,Kolhapur. He has published more than 150+ research papers in reputed international journals including IEEE and authered 12 books.