Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

DDoS Attack Detection & Protecion Mechanism in MANET

Mr. Ranjit Mane[1], Prof. B. W. Balkhande[2],
[1]*Department of Computer Engineering, BVCOE, Navi Mumbai,*
[2]*Department of Computer Engineering, BVCOE, Navi Mumbai*

Abstract— In DDoS attack, the general functionalities of network like bandwidth, speed of delievery, throughput, battery power,computational power gets disabled. Bandwidth of any link of any node gets consumed or flooded due to flooding attack so that victim node is not able to provide services to expected node. DDoS detection technique for detecting DDoS attack has been introduces as follows. In this we also introduce techniques for detecting and controlling flooding attack. The results obtained from NS–2 based simulations of proposed technique shows that the techniques can detect and control attacks effectively. MANET is network of all type of mobile nodes which are dyanamic in nature and communicate with each other dynamically because of changing topology. There are many chances of attacks on MANETs as they are wireless technology. Attacks can be DDoS attack and flooding attack.

Keywords: *MANET, DDoS attack, Flooding attack*

I. INTRODUCTION

Distributed denial-of-service attack (DDoS Attack) is a attack on network link or bandwidth by sending overwhelming amount of requests to victim. DDoS attacks is considered the most easy way to access and attack a network. MANET is a collection of wireless nodes that dont require any preexisting infrastructure. Nodes in MANET can be host or simply a router MANETs are mostly used in disaster, emergencies, military or civil situation in metro cities mostly, doe to its effective feature of dyanamic deployment and adaptation [6]. The features like mobility, high speed, flexibility,highly traffic tolerent and no preexisting infrastructure makes it better than wired network. Vulnerability of MANET is more due to its wireless nature. The major security attacks on MANET are 1)DDoS 2) flooding attack. The DDoS attak make bandwidth unavailable to nodes who are communicating with victim, so that original messages and packets can't reach to victim. There are some techniques a)distance estimation DDoS detection technique for detecting DDoS attack b)bandwidth control technique for controlling DDoS attack c) dyanamic counter based technique for detecting and controlling flooding attack in network simulator NS-2 [8]. The distance estimation DDoS detection technique gives results in term of throughput , packet drop rate , end to end delay,packet delievary ratio. The dynamic counter based technique determines minimum and maximum number of neighbours as per varied netework with different node speeds.

II.DDoS attacks in MANETs

A DDoS attack is a wireless attack which floods network links with large amount of data packets. It makes victim's link unavailable to expected senders Because of it network becomes inefficient and works slowly. Its performance gets decreased. Attacker plans the attack in some steps, first finds insecure machine i.e. easily vulnerable machine in network. Second attacker attack the discovered machine with infected code Then infected machine further used to find and spread malicious code to another machine in network and so on. Thus attacker stepwise prepares an attack. DDoS attack basically target victims computational resources such as bandwidth, memory, battery power,

computational power etc. Types of DDoS attack are ping of death, SYN Flood, Rflected Attack and nuke attack.

III. Proposed System

3.1 The distance estimation DDoS detection method:

The distance estimation DDoS detection technique used to identify abnormal changes of mean distance values, maximum distance values and minimum distance values based on the prediction model [6,8]. Distance value means number of hops required for packet to reach from source to destination. The distance information of packet can be taken from TTL value of IP header. The prediction technique the mean, maximum, minimum value of distance, mean absolute deviation (MAD), maximum absolute deviation(MaxAD) and minimum absolute deviation (MinAD) value at next time interval. Therefore, we can provide a clear scope for a legal value at the next time interval. Any values which are out of the legal scope can be considered as anomalous. The MAD-based deviation prediction model defines the scope of normality to detect abnormal changes of the mean distance value. The MaxAD-based deviation prediction model defines the scope of normality to detect abnormal changes of the maximum distance value and The MinAD-based deviation prediction model defines the scope of normality to detect anomalous changes of the minimum distance value.Central to this technique is the computation of the distance

1) Computing Distance: Based on the TTL field of IP header the distance has been calculated. During transfer, each intermediate router deducts one from the TTL value of an IP packet. Therefore, the distance of the packet is the final TTL value subtracted from the initial value. The challenge in distance calculation is how the victim derives the initial TTL value from the final TTL value. Fortunately, most of the operating systems use only a few selected initial TTL values: 30, 32, 60, 64, 128, and 255, according to [6]. Most of the Internet hosts can be reached within 30 hops. Therefore, the initial value can be determined by choosing the smallest initial value of all the possible values which are larger than the final TTL value. For example, if the final TTL value is 100, the initial TTL value is 128 which are the smallest of 128 and 255.

Adaptive distance based DDoS detection algorithm :

1.After receving packet p ;
2. If interval <ϒ then Add d of packet p with old d;
Otherwise CalculateAvg; MaxDist; MinDist; MAD; MaxAD; MinAD;

Predict AvgP; MaxP; MinP; MDP;//for average MaxDP;// for max MinDP;// for min

3. If ((Avg>(AvgP+ thr* MDP))OR (Avg<(AvgP- thr* MDP)))
then Set anomaly flag;

4. Elseif ((MaxDist>(MaxP+ Maxthr* MaxDP))OR (MaxDist<(MaxP-Maxthr* MaxDP))) then Set anomaly flag;
5. Elseif ((MinDist>(MinP+ Minthr* MinDP))
OR
(MinDist<(MinP-Minthr* MinDP)))
Then Set anomaly flag; Otherwise Forward packet;

3.2The Bandwidth control of DDoS attack technique:

To drop attack packets relatively, a distance-based attack traffic rate limit control will be triggered in the source-end edge network after receiving an alert message from the defense system of the victim-end edge network[6]. The operation of defending against DDoS attack is as follows.

Alert messages between a victim end and a source end includes three types: Request messages, Update messages, and Cancel messages. These messages are used in different phases of defeating a DDoS attack.

Request messages: Once DDoS attack is detected victim provides suggested rate limit value to a source end by sending request message.

Update messages: If attack traffic still increases then victim sends an update message to the source end again. Based on the requirements in the message, the source-end defense system will decrease the rate limit value exponentially. After the traffic at the victim end has returned to normal for a while, an update message sent to the source end asks it to increase the rate limit value linearly.

Cancel messages: Finally, if the defense system has not found any anomalous changes in the victim end since the update message, a cancel message is sent to remove the rate limit at the source end.

Bandwidth control of DDoS attack algorithm:

1.On hearing anomaly flag set;
2. Initialization of sending rates of source end routers;
Ratelimit = (lowerloadlimit + upperloadlimit) / 2;
3 Initialize configurable small constant C;
4 Multicast current rate limit information to source end routers;
5 Monitor current traffic rate at victim end;
6 If currenttrafficvictim >= upperloadlimit Then
6.1 Set constant as lowerloadlimit;
6.2 Find difference between current traffic at victim end and constant c;
6.3 Calculate decrease rate factor by taking quotient factor of small constant c and difference calculated in previous steps 6.2.
6.4 For (each node i at distance d)
6.4.1 Find drop rate for node i;
6.4.2 Find rate limit for node i;
6.5 End for;
7 Else
7.1 If currenttrafficvictim <= upperloadlimit then
7.1.1 Find difference between current traffic at victim end and previous traffic at victim End;
7.1.2 If difference calculated in previous step 7.1.1 is less than configurable small constant Then 7.1.2.1 remove threshold;
7.1.3 Else
7.1.3.1 Keep upperloadlimit value in constant c;
7.1.3.2 Keep current traffic at victim as previous traffic rate at victim end;
7.1.3.3 Calculate increase rate factor;
7.1.3.4 Calculate rate limit for node i;
7.1.4 End if;
7.2 Else
7.2.1 Break;
7.3 End if;
8 End if;

IV. Simulation and Results

4.1 Simulation implementation and evaluation for DDoS attack

The performance of our proposed scheme against DDoS attack is analyzed in MANET with and without defense scheme. To evaluate performance of our proposed techniques following performance matrices are used.

Throughput: - Throughput is the number of packets transmitted per unit time

Packet drop rate: - Packet drop rate is ratio number of packets dropped to the total number of packets sent.

End to End delay: - End to End delay is the delay experienced by a packet from the time it was sent by the source till the time it was received at the destination.

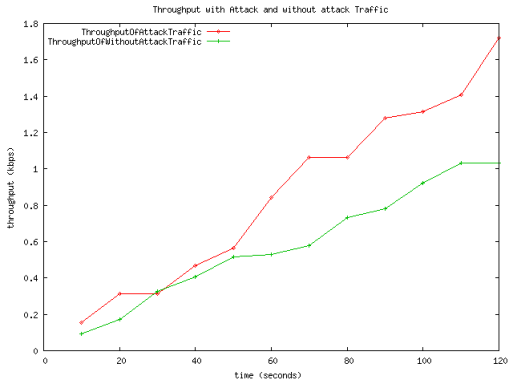

Figure 1.” with and without attack traffic versus time Throughput”

As shown in Figure 1 at the initial stage there is miner difference between throughput of attack traffic and legitimate traffic but as time increases and attack comes in picture then our proposed approach works on attack and filters traffic using bandwidth control mechanism and hence attack traffic throughput increases.

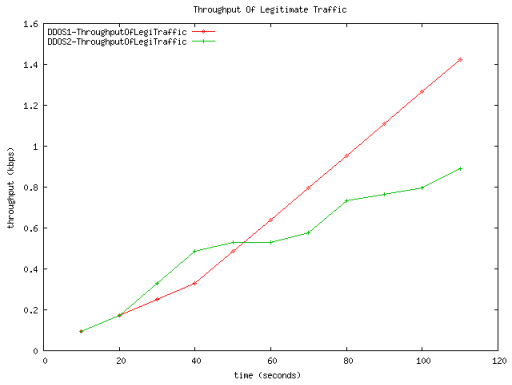

Figure 2. “Throughput of genuine traffic versus time”

Figure 2 shows in existing system throughput of legitimate traffic is consistently increases where as throughput of legitimate traffic in proposed approach is decreases because of various control mechanisms applied at source and destination end.

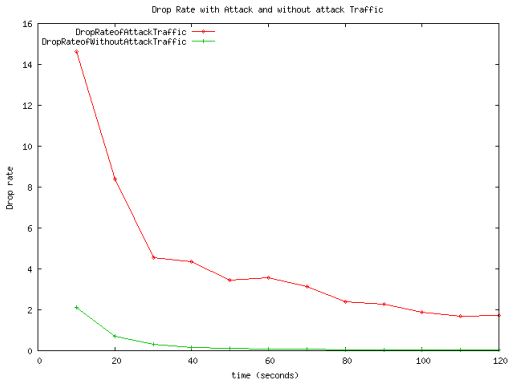

Figure 3. "Packet drop Rate with and without attack traffic versus time"

Figure 3 Shows the Packet Drop Rate with and without attack traffic versus time, it indicates at initial stage more percentage of attack traffic is delivered to destination but when time increases then proposed approach works on traffic and drop rate slowely decreases and drop rate without attack traffic given cinsistency with minar changes.

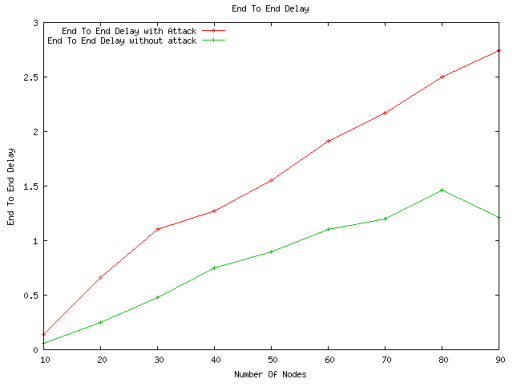

Figure 4. "Impact of End to End Delay versus Number of Nodes"

Figure 4 shows Impact of End to End Delay Versus Number of Nodes, it indicates when attack traffic comes in existance it altimatly affects on delivery time of traffic at destination causing delay hence end to end delay increases with attack traffic. The difference between end to end delay with and without attack traffic is increases as simulation time increases.

V. Conclusions

As the use of MANETs increases, the security is becomes critical issue. In this paper, we have discussed the various security issues and security attacks in MANET and proposed a defense schemes against DDoS and flooding attacks in MANET. We have also simulated some DDoS attacks in MANET, with and without defense schemes and understand the effects of such attacks on performance of network.

References

[1] Chang and R.K.C., "Defending against flooding-based distributed denial of- service attacks: a tutorial," IEEE Communications Magazine, vol. 40, no. 10, pp

[2] Chang wang Zhang, Jian ping Yin. "Low-rate DoS attack detecting and filtering method based on distributed congestion participation", Computer Engineering and Science,2010

[3] Jie ren Cheng, Jian ping Yin, "DDoS attacks detection based on ARMA prediction model", Computer Engineering and Science,2010,

[4] Jie ren Cheng, Jian ping Yin, "Distributed denial of service attack detection method based on address correlation", Computer Research and Development,2009,

[5] B. Soujanya, T.Sitamahalakshmi and C. H.Divakar, "Study of Routing Protocol in MANET", International Journal of Engineering Science and Technology, Vol. 3, No. 4, pp. 2622-2631, 2011.

[6] Rachana Yogesh patil . "A Rate Limiting Mechanism for Defending Against Flooding Based Distributed Denial of Service Attack"

[7] Krishan Kumar Saluja, Parveen Kakkar, "The DDoS Attacks in MANET- A Review" Journalof Information Systems and Communication, Vol. 3, Issue 1, 2012, pp.-310-314.

[8] Hwee-Xian Tan,WinstonK.G.Seah "Framework for statistical filtering against DDoS attacks in MANET."Proceedings of second international conference on embedded software and systems (ICESS)

[9] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39–53, Apr 2004.

[10] Yun Liu, Jian ping Yin. "A distributed denial of service attack detection based on K-Means algorithm".Computer Engineering and science.2008.

[11] Y. You, M. Zulkernineand A. Haque "Detecting flooding-based DDoS attacks," Proceedings of the IEEE International Conference on Communications, Glasgow.

[12] NishuGarg, R.P.Mahapatra. "MANET Security Issues".IJCSNS.InternationalJournal of Computer Science and Network Security, Volume.9, No.8, 2009.

[13] Krishan Kumar Saluja, Parveen Kakkar, "The DDoS Attacks in MANET- A Review" Journalof Information Systems and Communication, Vol. 3, Issue 1, 2012, pp.-310-314.

[14] M. BaniYassein, A. Al- Dubai, M. OuldKhaoua and Omer M. Aljarrah. "New Adaptive Counter Based Broadcast Using Neighborhood information in MANETS", IEEEConference on Parallel and DistributedProcessing Pages 1-7, May 2009.

[15] Ping Yi ,ZhoulinDai,Yi-Ping Zhong , Shiyong Zhang "Resisting Flooding Attacks in Ad Hoc Networks" International Conference on Information Technology: Coding and Computing, ITCC pp.657-662.

[16] K. Kumar, R. Joshi, and K. Singh, "An integrated approach for defendingagainst distributed denial of service attacks," IRISS-2006, IIT Madras. [Online].Available:http://www.cs.iitm.ernet.in/~iriss06/paper.html.

[17] M. Robinson, J. Mirkovic, M. Schnaider, S. Michel,and P. Reiher, "Challenges and principles of DDoS defense,"Computer Journal of ACM SIGCOMM,vol. 5, no.2, pp. 148-152,2003.

[18] Ahmad Sanmorino1, Setiadi Yazid2." DDoS Attack Detection Method and Mitigation Using Pattern of the Flow"2013

[19] Wang H.,Zhang D. and Shin K."Detectingsynflooding attacks,in IEEEinfocom".

[20] MahaAbdelhaq,SamiSerhan,RredAlsqour and Rosilah Hassan(2011) IEEE sponsored international conference on Electrical Engineering and informatics.

[21] J. Jung, A. Berger, and H. Balakrishnan, "Modeling TTL-based internet caches," in Proceedings of the Twenty-Second Annual Joint Conference of theIEEE Computer and Communications Societies, 2003, pp. 417–426.

[22] T. Gil and M. Poleto, "Multops: a data-structure for bandwidth attack detection," in Proceedings of 10thUsenix Security Symposium, 2001, pp.23–38.