International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Detection & Prevention of DDoS and Flooding Attacks in Ad hoc Network

P. D. Kadam[1], R.M.Khaire[2]

Department of Electronics & Telecommunication, Bharati Vidyapeeth University C. O. E., Pune-43, Maharashtra, India

Abstract: ***Many organizations are using LAN (local area network) to access the internet, this enable the work in many industries easy and comfortable. Flooding and D-DOS are the two major threats to WLAN because these two effects causes huge amount of interchange. The two threats are very difficult to detect and resolve because it involves huge network traffic, In this paper we are introducing a broadcast technique to overcome and prevent flooding attack. We are using two techniques to overcome these problems. This work involves two techniques (AVERAGE DISTANCE ESTIMATION) and (RATE LIMITING).AVERAGE ESTIMATION involves estimation of distance and RATE LIMITING involves different controlling units to encounter (DISTRIBUTED DENIEL OF SERVICES) attack. Regular distance estimation technique study and examine the distance values for noticing the hidden solution for controlling D-DOS. The mean values of distance are forecast to define normality in (AVERAGE ESTIMATION). The mean absolute deviation method is used which includes (MAD) technique to distinguish normality from the abnormality.***

Keywords: WLAN, Flooding attack, D-DoS attack.

1. Introduction

MANET dyanamically form temprory networks which are capable of communicating with one network with other network with no use of preceeding framework of network.In such hierarchy, it is necessary for one mobile network to act as host which enters the assistance of different hosts in delvering the data to the required place because of the bandlimited frequency.

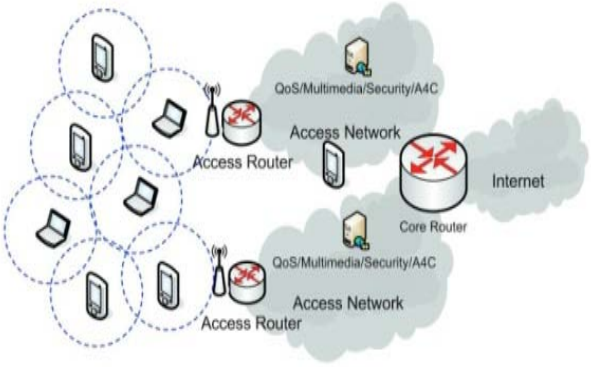

Figure 1.1: Mobile Ad Hoc Networks-MANETs.

Due to the accessibility of two major entities i.e ”MOBILE HOST” as well as “:NETWORKING HARDWARE” the networking becomes very smooth and due to this formation of internet is possible. But sometimes mobile users will communicate where there is no direct wired infrastructure is available because of many economical and physical constraints. We can take any day to day examples like sharing files on the airport between friends or during a road misshape calling an emergency. In these situations, a group of mobile hosts will form a wireless network and one can act as a host between them.

2. Related Work

Survey of DDoS Attack Detection Techniques
Our main objective in these DDOS attack detection I the network performance of LAN. Previously there has been some study on DDOS attack detection techniques and some of them are enlisted below.

2.1 Intermediate evaluation of distance using (DISTRIBUTED DENIEL OF SERVICES) technique.

Intermediate evaluation technique using DDOS is helpful in observing the exceptions in the average values of distance which uses a technique known as exponential smoothing estimation. The number of bounces required by the data from origin to particular direction is called as distance value. The notification of data can be obtained from(TRANSISTOR TRANSISTOR LOGIC) by defining the truth table for whole(INTERNET PROTOCOL).

The method called exponential smoothing is use to conclude two quantities known as mean deviation and average distance for latter interval of time. Hence we conclude the explicit picture of how the next interval of time is travelling. The values that are not synchronizing with this proper field decribed as abnormal.(MEAN ABOLUTE)structure define the areas which include normality and it also include those areas where abnormal changes are seen including traffic arrival rate.

2.1 Calculating Distance/Farness

Average distance or Mean distance is computed with the help of Transistor Transistor Logic field of IP host. While transmission, every router in between a source and destination will extract the Transistor Transistor Logic value from the IP packet. Packet distance can be calculated as the last Transistor Transistor Logic value deducted from its First value. Real problem in calculation of distance is to extract the first value from its Transistor Transistor Logic value. But most of the O.S uses first of its Transistor Transistor Logic values i.e. 30, 32, 60, 64, 128, and 255. Within 30 hops most of the Internet hosts can be reached. Thus first value can be computed by taking the finest possible value which is larger than final TTL.

2.2 Estimating Mean Distance

The estimation or prediction of any abnormality totally depends on the deviation and normalcy. The average value of distance D_{T+1} at time T+1 is calculated by using Exponential Smoothing Estimation model 1using the given equation.

$$D_{T+1} = D_T + W * (M_T - D_T)$$

where, D_T is a value of distance at time T calculated at time $T-1$, M_T is the distance measured at time T, W is a smoothing gain, and $M_T - D_T$ is the prediction error at T.

2.3 Calculating Deviation

Finding whether the distance is correct or incorrect, Mean Absolute Deviation (MAD) is calculated by using the given equation.

$$MAD = \frac{1}{N} * \sum |Et|$$

Where, N is no of previous errors and E_t is the Prediction error during time t . To have all the past errors is not possible. Thus, we compute MAD by using the Exponential Smoothing Technique based on approximation equation shown below.

$$MAD_{t+1} = R * |E_t| + (1 - R) * MAD_t$$

Where, MAD_t is the MAD value at given time T and R is a Smoothing Gain..

2.4 IP Characteristics Based Distributed Denial Of Service (DDoS) Detecting Technique

Abnormalities in any mobile n/w is predicted using any of these attributes, Transistor Transistor Logic , Internet Protocol add of source , and multiple attributes contribution. Jung *et al. uses* Transistor Transistor Logic for the synthesis of Internet Web for loading performance. Any D-DoS attack creates huge traffic which causes congestion which changes the statistical average distribution of above defined Transistor Transistor Logic attributes. On basis of this, Talpade*et al.* proposed a Transistor Transistor Logic -based statistical average model to observe any abnormality generated by D-DoS attack. Due to change in last Transistor Transistor Logic value, the result is not up to the level which cannot show the abnormal change in traffic topology. Our techniques uses due to the change in final Transistor Transistor Logic value compute distance value.

Kim *et al. designed* a prototype profile for number of attributes merge like Internet Protocol- type and size of packet, source Internet Protocol prefix and Transistor Transistor Logic values, port number of server and protocol - type. But this alone cannot enhance/improve performance of the traits which are not directly related with the abnormal change achieved during any D-DOS attack. However, merging these traits will make calculation more hard and will increment the false +ve rate as well.

2.5 Traffic Volume Based D-DoS Detection Technique

The two brilliant scientist “GIL” as well as ”POLELTO” come with a new invention of data structure known as (MULTOPS).MULTOPS stands for ”Multi-level tree .Both of them constructed a algorithm called “multi-level” tree which is used to accumulate the speed of data statics for logical subdivision of internet protocol network. A typical data speed is increase if the speed of host is increase or speed decrease if host’s speed decrease and same case happens for logical subdivision internet protocol network. Every such attack can be evaluated by MULTOPS finds a changing traffic rate. For detecting any change in rate of traffic, he designed a stationary traffic prediction system which can work in changing traffic rate. This approach is also used by Lee. but it also uses the exponential technique of smoothing to synthesis the rate of traffic and MAD to find any abnormal change in traffic. But these two approach are below satisfactory due to their simple prediction technique for complex and dynamic rate of traffic and other are very complex techniques available.

3. Proposed Work

3.1 D-DoS Defense Frameworks

Any network system is evaluated in two fields . The first domain is the core network and it have high speed core routers which are the real backbone network. The second field involves edge network which connects to a core network through edge routers. Usually, there is not much traffic which needs to be forwarded by edge routers.

As shown in figure 6.1, D-DoS prevention system is installed in every router of any protected network. While transmitting the D-DOS traffic towards the recipient , the recipient system will detect the attack because the traffic will process large amount of abnormalities at the victim end. This defense system cannot attacks when the traffic is more. Hence a second defense system is installed in the networks to act to these heavy traffic attacks. In any such framework, finding any of the D-DoS attacks will occur only for edge routers. An edge router has the resources.

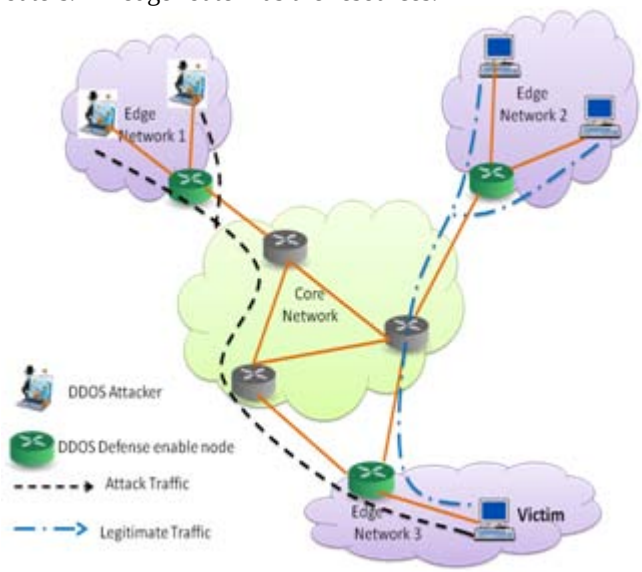

Figure 6.1: Distributed DDoS Defense Framework [10]

3.2 Operations of Defense Framework

Figure 6.2 shows the real time defending by the victim system during any DDOS attack. There are some alert

messages between the host and the receiver which are Update message, Cancel message, and Request message which are used in different phases of a DDOS attack. In the beginning of any attack, a request message from a recipient will give a suggest limit value to the sender. If the volume of D-DOS traffic further increases abruptly, an update signal about the same will be sent to the sender. Based on that update message, source will vary the rate limit exponentially. After the traffic return to normal, a refresh signal will be sent to the sender telling receiver to change the restricted speed linearly. If there is no abnormal change in the traffic a cancel message is send to the source end to remove such rate limit.

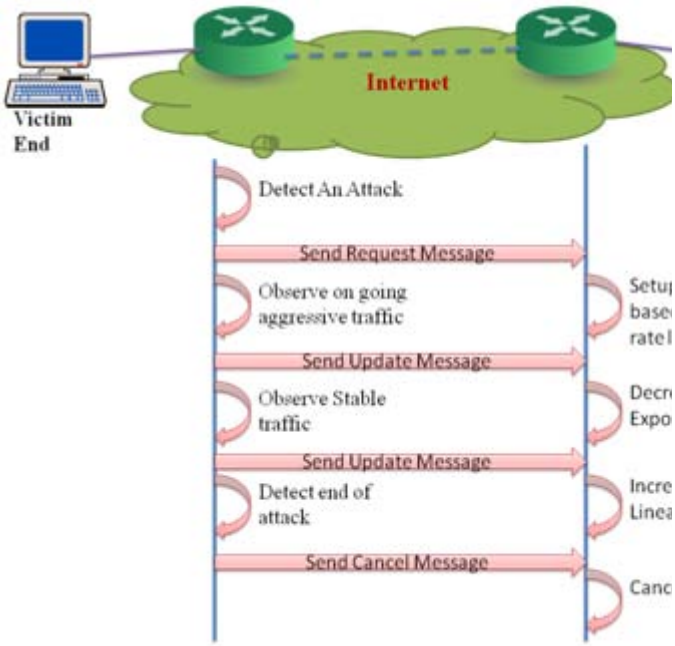

Figure 6.2: Illustration of distributed DDoS defense operation

4. Conclusions

Here we proposed some methods for the detection as well prevention of overloading and distributed denial of service attacks generally happen in WLAN network. In this we proposed a counter based method for the detection, prevention of overloading attacks, a fundamental method for analysing of any D-DoS attack and finally a speed restricted method for limiting the rate for any D-DOS incursion.

This dynamically counter broadcast method gives dynamic adjustment of its verge value which depends on where it has been located. This average prediction D-DOS detection method uses an exponential smoothing technique for the calculation of average value of distance for next period. Rate limiting technique exponentially nullify the sending rate from the source router towards the recipient

References

[1] Y.-C. Tseng,S.-Y. Ni,J.-P. Sheu and Y.-S Chen.'*The broadcast storm problem in mobile ad hoc network'*. ACM/IEEE Mobicom'99, August 1999.

[2] S.-Y. Ni, J.-P.Sheu Y.-C.Tseng,'*The broadcast storm problem in a mobile ad hoc network'*, Wireless Networks, 2002.

[3] R. Kotagiri, T. Peng and C. Leckie, *"Proactively detecting Distributed Denial of Service attack using source Internet Protocol address monitoring,"* in Proceedings of the Third International IFIP-TC6 Networking Conference, 2004, page. 771–782.

[4] R. R. Talpade, S. Khurana and G. Kim, *'Nomad- traffic based network monitoring framework for anomaly detection,'* in the Fourth Institute of Electrical and Electronics Engineers, Symposium on Computers and Communications, 1999.

[5] R. Brooks,G. Carl, and S. Rai and G. Kesidis *'DOS attack detection techniques,"* Institute of Electrical and Electronics Engineers Internet Computing, vol. 10, January 2006.

[6] K. K. Suh, and Y Kim,J.-Y. Jo *'Baseline profile stability for network anomaly detection'* in Proceedings of the IIIrd International Conference on IT: New Generations, 2006.

[7] A.Berger , J. Jung, and H Balakrishnan, *'Modeling TTL-based internet caches'* in Proceedings of the 22nd Annual Joint Conference of the Institute of Electrical and Electronics Engineers Computer and Communications Societies, 2003.

[8] M. Poleto and T.Gil 'Multops: a data-structure for bandwidth attack detection' in Proceedings of xth Usenix Security Symposium, 2001, pp.23–38.

[9] S. Papavassiliou and J.Jiang *'Detecting network attacks in the internet via statistical network traffic normality prediction'* Journal of Network and System Management, vol. 12, 2004.

[10] J. Na , J. Jang ,S. Lee and H. Kim *'Abnormal traffic detection and its implementation,'* Advanced Communication Technology, vol. 1, February 2005.

[11] http://en.wikipedia.org/wiki/Wireless_LAN