ISSN : 2231-0711

Sandeep Shinde et al | IJCSET(www.ijcset.net) | August 2015 | Vol 5, Issue 8,301-303

Traceback Mechanism for DDoS Attacks Using Local Flow Monitoring in MANET

Mr. Sandeep Shinde [#1], Dr. J. W. Bakal *[2]

[1#]*Dept. of Information Technology, Pillais Institute of Information Technology, Mumbai University, India*

*[2]*Principal, S.S. Jondhale College of Engineering, Dombivali-west, Mumbai University, India*

***Abstract*—Mobile ad-hoc network is integration of node which is scatterd around the network. Every node in mobile ad-hoc netowk is configured by own, it also decentralized and less secure. Due to mobability properties of mobile ad-hoc network every node in mobile network move around the network. The DDOS attack is the major security in the mobile ad-hoc network. The DDOS attack it generate huge unwanted traffic so that authorized user not able to access service or resource efficiently. In this paper, we introduce new technique local flow monitoring system based on entropy variable for detecting DDoS attack .**

Index Term- MANET, DDoS, Network traffic

1. INTRODUCTION

In mobile Ad-hoc Network is independently configured itself which does not have any framework network and interconnected through wireless protocol. In mobile ad-hoc network it allows the node free to move any direction. The open nature, dynamic topology, some security issue and other issues due to mobile ad-hoc network easily vulnerable to different attacks. Now days, Mobile ad-hoc network are affected by different attacks like impersonation, message distortion, eavesdropping, DoS and Distributed denial of service etc[1].

Denial of service (DoS) attacks, which are initiated for avoiding to authorized user from accessing or use of network various services. The research community knows this attack since the early 1980s. The denial of service attack creates unwanted traffic towards victim so that the authorized user not able accesses the resources of network. It also reduce the degree of performance of the system.

The first Distributed DoS attack incident reported by the Computer Incident Advisory Capability (CIAC) in mid of 1999. After this all DoS attacks have lunch in distributed nature [2][6].

Currently DDoS attacker is lunched the attack victim from remote location. The attacker first search compromised computer (those compute are have less security). Compromised computer are also called as Zombies. It create a network of compromised computer is called botnet network. And attacker lunch attack through is botnet network by sending huge amount of unwanted traffic towards the victim. Through the zombies the attacker are control the attack on victim. So the attacker are install worms, Trojan horse or backdoors. Attacker are lunch the DDoS attack remotely and use very large and complex network due to that it is very difficult to detecting and controlling.[3][4]

2. DISTRIBUTED DENIAL OF SERVICES ATTACK IN MANET

In Mobile ad-hoc network, the DDoS lunches using malicious node. Distributed and large scale of compromised or zombies or malicious user are generate huge amount of traffic towards the targeted network with number of infected packet which consume bandwidth , battery power and services. Due to this victim or targeted network cannot provide service properly to its intend or authorized network or user.[4][5]. In distributed denial of service attack , the attacker lunch attack using the number of different network path. To victim it is very difficult to compare authorized traffic or unauthorized traffic.

3. PROPOSED WORK

In this section we introduce our defense scheme with algorithm through which we can detect the DDoS attack.

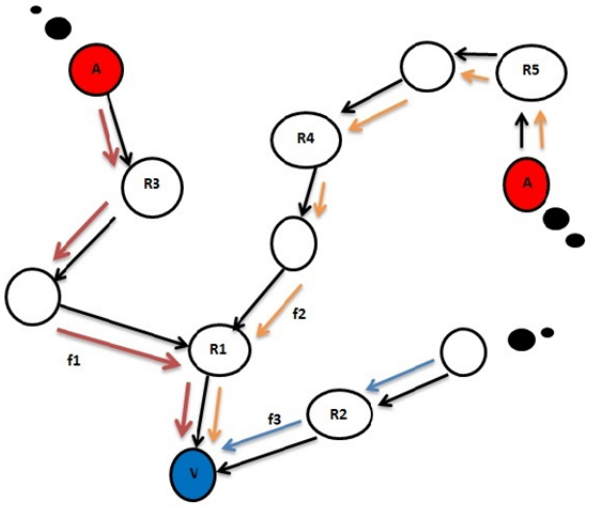
DDoS Detection Scheme using Local Flow Monitoring based on Entropy Variation

A. DDOS attack Detection Scheme

A simple mobile ad-hoc network with DDoS attack to demonstrate our proposed detection scheme. We here categorize the packets that are passing through a router into flows. Flow is defined by pair the upstream router where the packet come from and the destination address of the packet. Entropy is an information theoretic concept, which is a measure of randomness. We use entropy variation to measure of changes of randomness of flows at a router for a given time interval. We notice that entropy variation is only one of the possible metrics in fig1. [13][15].

4. OPERATION OF DDOS DETECTION FRAMEWORK.

In a DDoS attack scenario, as shown in Fig 2, the flows with destination as the victim include legitimate flows, such as f3, and a combination of attack flows and legitimate flows, such as f1 and f2. Compared with no attack cases, the volumes of some flows increase significantly in a very short time period in DDoS attack cases. Observers at routers R1, R4, R5, and V will notice the dramatic changes; however, the routers who are not in the attack paths, such as R2 and R3, will not be able to sense the variations. Therefore, once the victim realizes an ongoing attack, it can push back to the networks, which caused the changes based on the information of flow entropy variations, and therefore, we can identify the locations of attackers.



	Mobile nodes		Data flow
	Attack traffic		Legitimate traffic
A	Attacker	V	Victim

Fig 1: Proposed DDoS Detection framework

In these it calculate threshold (local threshold parameter δ) by differentiating current flow probability distribution and entropy distribution and according calculate the mean and changes the threshold value for next flow many times it wastes resources or over exceeds by threshold value considering only current flow.

To overcome this drawback it is important to consider current differences i.e. current probability distribution, cumulative distribution of all the flow and best probability distribution between the flow i.e. called as recommended probability distribution. Compare all these three probability distribution and according decide threshold for next flow.

Calculate direct probability distribution between current and previous flow

$$\delta_1[t] = \delta_1[t] - \delta_1[t-1] \quad \text{------ (1)}$$

Calculate cumulative probability distribution of all previous flows.

$$\delta_2[t] = \sum_{f=1}^{n} \delta[f] \quad \text{----- (2)}$$

Calculate recommended probability distribution by comparing all flows.

$$\text{Rec}\delta 2[\text{t}] = \max(\delta \text{f}) \quad \text{------ (3)}$$

We are comparing flow for value of f=1, 2, 3 …n

Compare $\delta 1$ and $\delta 2$ and Rec$\delta 2$ .Choose best sigma as final probability distribution.

Where t=1, 2, 3, 4, 5 to number flows.

After detecting the attack traffic and using traceback mechanism we easily find the source node of attacker.

Algorithm

Initializtion

Local flow monitoring

Intialization

1. Local threshold parameter C
2. Another local threshold parameter δ
3. Next local threshold parameter for sampling time period ΔT

Step1. Label first flow as f1 and set packet sixe as 100 bytes.

Step2. Execute first flow for first time ie, x1=1 (we have to execute first flow f1 (every flow) for 5 times.)

Step3. Wait till ΔT is over or not.

Step4. Once timer is equal to. then calculate probability distribution as follows.

$$p_i = x_i \left(\sum_{i=1}^{n} x \right)^{-1}$$

Step5. After getting probability distribution, calculate entropy distribution as follows…

$$H(F) = -\sum P_i \log P_i$$

Where i is 1, 2, 3,4,5 times execution of each flow.

Step6. Then save H(F) for 5 times execution of each flow. So H(F) is for each flow.

Step 7. Check weather absolute value of | H(F)-C| of current flow is less than or equal to δ

7.1 Calculate mean as follows

$$C[t] = \sum a_i \; C\,[t-1], \sum a_i = 1$$

7.2 Calculate standard deviation as follows.

$$\delta[t] = \sum \beta_i \;\; \Delta\,[t-1], \sum \beta_i = 1$$

Step8. Calculate direct probability distribution between current and previous flow.

$$\delta_1[t] = \delta_1[t] - \delta_1[t-1]$$

Step9. Calculate cumulative probability distribution of all previous flows.

$$\delta_2[t] = \sum_{f=1}^{n} \delta[f]$$

Step10. Calculate recommended probability distribution by comparing all flows.

$$Rec\delta_2[t] = \max(\, \delta f)$$

Where f=1, 2 ,3, 4 ,---n

Step11. Compare $\delta 1$ and $\delta 2$ and Rec $\delta 2$ .Choose best sigma as final probability distribution.

Where t=1, 2,3,4,5 to number flows

Step12. Go for next flow.

5. CONCLUSION

Now days the security of mobile ad-hoc network is major topic for research community. In these paper we introduced new local flow monitoring algorithm which is detect the DDoS attack which attack on victim through large number of distributed in network. Tradition traceback mechanism like PPM and DPM which gone through number drawback. In our scheme the attack is identify in first visited routers when infected or unwanted flows came towards and so it will issue the traceback request to the connected all routers to first router in network. This procedure is continue still the victim is known. In scheme we are added recommended the probability for purpose is it for deciding the threshold of flows. We are expecting to improve false positive rate for allowing the authorized traffic access by network.

REFERENCES

[1] Minda Xiang, Yu Chen, Wei-Shinn Ku, Zhou Su, "Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc networks" Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , DEC. 5 - 9, 2011.

[2] P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[3] R. K. C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial, Computer J. IEEE Commun. Magazine,Vol. 40, no. 10, pp. 42-51, 2002.

[4] CERT, Denial of Service Attacks, June 4, 2001[online], http://www.cert.org/tech tips/denial of service.html

[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state of the art,"Computer Journal of Networks, vol. 44, no. 5,pp. 643-666,Apr.2004.

[6] T. Peng, C. Leckie, and R. Kotagiri, "Proactively detecting DDoS attack using source ip address monitoring," in Proceedings of the Third International IFIP-TC6 Networking Conference, 2004, pp.771–782.

[7] R. R. Talpade,G. Kim, and S. Khurana, "Nomad: traffic based network monitoring framework for anomaly detection," in the Fourth IEEE Symposium on Computers and Communications, 1999, pp. 442–451

[8] Y Kim,J.-Y. Jo, and K. K. Suh, "Baseline profile stability for network anomaly detection," in Proceedings of the 3rd International Conference on Information Technology: New Generations, 2006, pp. 720–725.

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

[10] Ping Du Nict,Tokyo, Japan Nakao A. "DDoS Defense Deployment with Network Egress and Ingress Filtering" in Communication (ICC), 2010 IEEE International Conference, 23-27 May 2010.

[11] Chao Gong, Sarac,K. "IP traceback based on packet marking and logging" Communications 2005. IEEE International Conference 2005 page 1042-1047.

[12] Chao Gong, Sarac, K."A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking" Parallel and Distributed Systems, IEEE Transactions, Page 1310-1324.

[13] Shui Yu and Wanlei Zhou, "Traceback of DDoS Attacks Using Entropy Variations", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 3, March 2011.