DDOS TRAFFIC CONTROL USING DSA ALGORITHM WITH STRUCTURE INFORMATION IN SDN

PUNITHA JILT A

AP, DEPT OF CSE, ST.ANNES COLLEGE OF ENGINEERING AND TECHNOLOGY, TAMILNADU, INDIA

Abstract –

Nowadays, computer network is very important because of the many advantages it has. However, it is also vulnerable to a lot of threats from attackers and the most common of such attack is the ***DNS based Distributed Denial of Service (DDoS)*** *attack. A detection and defense algorithm against DDOS attack is very important. Many of the proposed DNS based DDoS solutions try to prevent/mitigate such attacks using some intelligent non- "network layer" (typically application layer) protocols. This can be analyze DNS based Distributed Denial of Service (DDoS) attack detection and prevention measures using software defined policies. DDOS is an attack overloads the firewall by malicious scripts. In this paper provides efficient prevention method named* ***Digital Signature Algorithm (DSA)*** *to prevent DDOS attack. It provides automatic intrusion detection and prevention.*

Key Words: DDOS, DNS, DSA, detection, defence, intrusion firewall, and software defined policies

1. INTRODUCTION

The current prevalent DNS based DDOS solutions are for application layer, and not directly implemented at the network layer. So, via this proposed doctoral research it is intended to utilize flexibility of SDN and make underlying network intelligent enough to prevent DNS based DDOS attacks. More specifically, it is intended to design, develop, and validate SDN based framework which will introduce "appropriate intelligence" to enhance the functionality of Openflow enabled L2/L3 switches so that underlying network itself can prevent and mitigate DNS based DDoS attacks. For each incoming or outgoing packet, a firewall decides to accept or discard it based on its policy. A firewall policy is composed of a sequence of rules, where each rule specifies a predicate over five different fields: source and destination port, source and destination IP address, and IP protocol. Typically, firewall policies do not check the source port field. The rules in a firewall policy may overlap and conflict.

1.1EXISTING SYSTEM

There is no deployed technology that has successfully defended against DDOS attacks. Most of the approaches focus, perhaps understandably, on protection of customer sites against incoming attacks. This turns out to be very difficult to do with today's Internet architecture and protocols. Thus in existing system, both firewall security for servers and application security are not efficient and highly secure.

1.2 PROPOSED SYSTEM

It provides efficient prevention method named **Digital Signature Algorithm (DSA)** to prevent DDOS attack. DSA algorithm avoid botnet intrusion and validate each user by key based authentication system.Our proposed system provides automatic intrusion detection and prevention against DNS based DDOS attack using SDN based programmability. Also our proposed system provides the infrastructure details before and after attacks.

2. MODULES:

DDOS Attack

2.1 PREVENTION MEASURE:

- ✓ DEEP PACKET INSPECTION (DPI)
- ✓ Digital Signature Algorithm (DSA):
- ✓ Filter Based Approach
- ✓ Software Puzzle Based Approach
- ✓ Key seed mechanism

3. ALGORITHM:

The DDoS identification is then based on the detection of anomalies in the characteristics of the packet attributes. Description of the botnet identification algorithm, it is worth commenting on a possible limitation of the proposed approach.

Step 1: Collect network traffic packets and flow information in real-time.

Step 2: Pre-process network traffic by cumulatively averaging it as in (2)

Step 3: By using AR model, predict the network traffic.

Step 4: Find out the prediction error by (4)

Step 5: Detect the abnormal traffic by analyzing prediction error based on chaos theory

Step 6: Detect DDoS by using trained neural network.

4. ARCHITECTURE

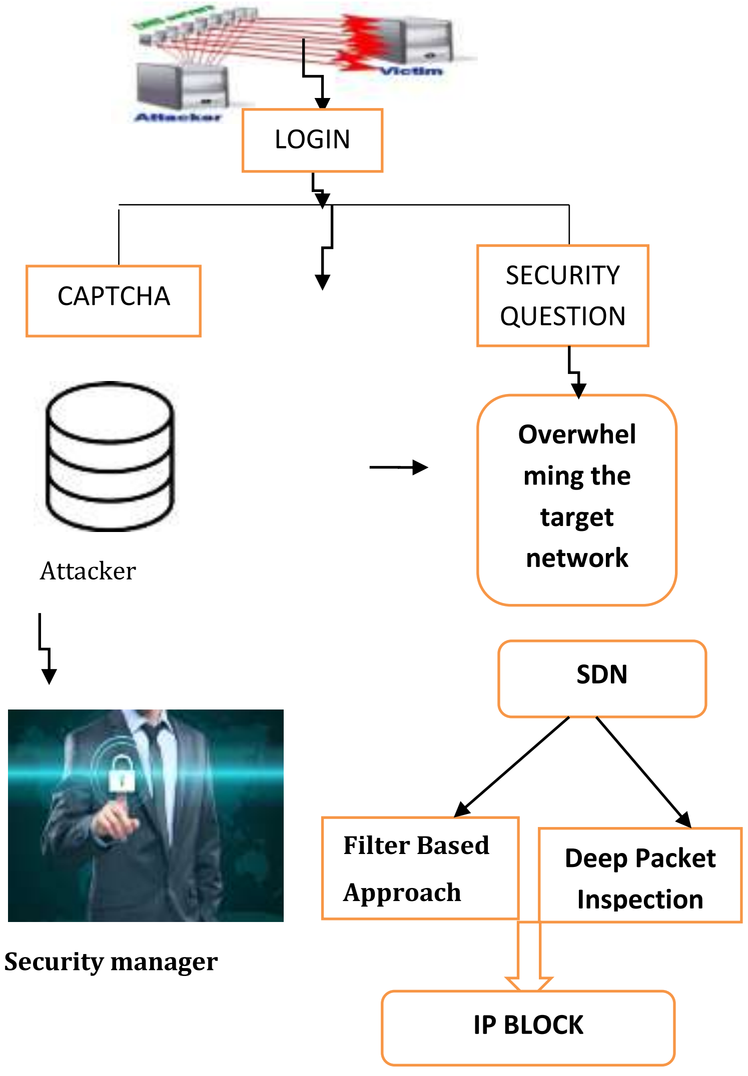

Fig -1: SDN Based method for IP Block

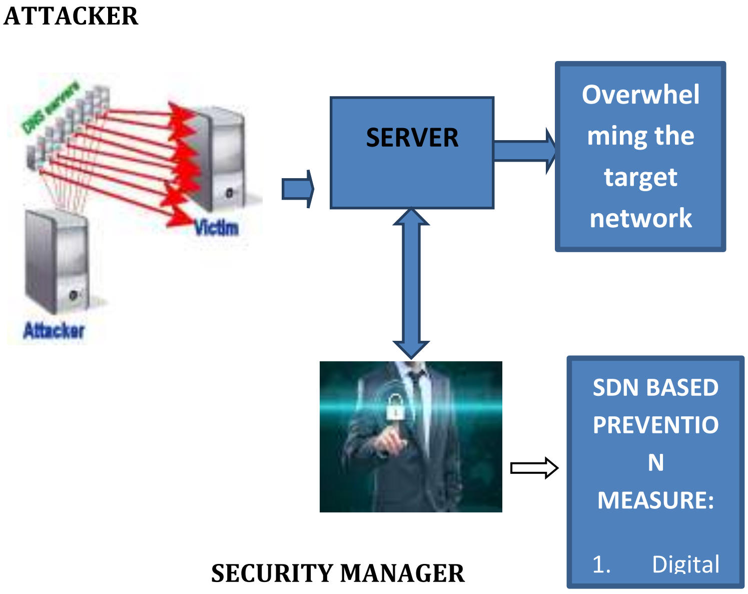

Fig -2: Server side

5. CONCLUSION

Cloud is the important part of the fast growing network based on the internet and the availability of the cloud is the most important. To keep the cloud all the time available to the users, it is necessary to have the detection and prevention for the threats which affect on the availability of the cloud. This paper provides the techniques available for detection and prevention for the DNS based DDoS attack using SDN policies are effective. The future work is to find a solution which can successfully detect and prevent DDoS attack in cloud

REFERENCES

[1] E. Bertino and N. Islam, "Botnets and Internet of Things security," Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[2] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the Source," in Proc. IEEE Int. Conf. Netw. Protocols. IEEE Comput. Soc., Nov. 2002, pp. 312–321.

[3] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the age of machine learning and software-defined networking," IEEE Internet Things J., vol. 5, no. 6, pp. 4829–4842, Dec. 2018.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.

[5] G. Wangen, A. Shalaginov, and C. Hallstensen, "Cyber security risk assessment of a DDoS attack," in Proc. Int. Conf. Secur. Cham, Switzerland: Springer, Aug. 2016, pp. 183–202.

[6] K. Malialis and D. Kudenko, ‘‘Multiagent router throttling: Decentralized coordinated response against DDoS attacks,’’ in Proc. 25th IAAI Conf.. Jun. 2013, pp. 1551–1556.

[7] K. Malialis and D. Kudenko, ‘‘Distributed response to network intrusions using multi agent reinforcement learning,’’Eng.Appl.Artif.Intell.,vol.41, pp. 270–284, May