INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 104-107

e-ISSN : 2583-1062

Impact Factor : 5.725

DESIGN AND DEVELOPMENT OF INTRUSION DETECTION SYSTEM ON APPLICATION LEVEL DDOS ATTACK

M.A.Ajai raju[1], Mrs.R.Golda selia[2], Dr.S.Geetha[3]

[1]Final Year M.Tech CFIS, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2]Professor, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[3]Head of Department, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

ABSTRACT

When you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a "cloud computing" service. If you are an organization, and you want to use, for example, an online invoicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a "cloud computing" service. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. Internet of Things (IoT) is increasingly becoming very popular in everyday life as it can connect the physical phenomena called as things with virtual world, i.e. the Internet. Not only new-age smart devices, wearables, cameras, smart lightings but also household appliances like washers, refrigerators, and house doors are being connected to the Internet, making a rich IoT ecosystem. Since the last decade, proliferation of sensor technologies has helped the rapid growth and mass adoption of the things. It is expected that by 2018, 11.8 billion things will be connected to the Internet. IoT has also opened up huge commercial and industrial opportunities in areas such as intelligent transportation, industrial automation. With this phenomenal growth of IoT, it is becoming critically important to protect these devices against cyber attacks. Otherwise, malicious users or attackers will take control of the devices and critical things will be at stake apart from privacy violation. Another problem is that these IoT devices have either no or little security features at device level. So, providing security at device level for a large number of heterogeneous IoT devices may not be feasible.

1. INTRODUCTION

The main goal of SDN is to separate the control plane from the data plane. Thus, data forwarding decisions are separately executed than the logical procedures of networking protocols. We can leverage on the features of SDN to bring in several benefits for IoT security. With the help of SDN, suspicious flows can be detected earlier with faster response at SDN-enabled switches. It becomes challenging due to different traffic profile of various IoT devices and different usage patterns over time.

When IoT devices are under attack, SDN can play a significant role in dynamic flow management and mitigation of the attack, by blocking or rate limiting the suspicious flows. The attack detection can be pushed to the edge of the IoT network. Such early detection enables early reaction to the attacks with mitigation and isolation of the attacked devices. Also, such early detection helps to reduce resource wastage due to attack traffic such as DoS or DDoS which consume a large amount of network bandwidth. Moreover, SDN can help improve the accuracy of detection mechanisms by running intelligent and sophisticated algorithms

2. LITERATURE SURVEY

Nikos Bizanis et.al, in this article, we survey the state-of-the-art on the application of SDN and NV to IoT. We review some general SDN-NV-enabled IoT architectures, along with real-life deployments and use-cases.

Olivier Flauzac et.al, we first present a new SDN based architecture for networking with or without infrastructure, that we call an SDN domain. Next, we propose a second architecture to include sensor networks in an SDN-based network and in a domain.

3. EXISTING SYSTEM

IP trace back provides a tracing mechanism to reconstruct the traffic routing path, and possibly identify the attack origin. IP trace back is useful for attack deterrence, attack mitigation and forensic investigation; it also find use in traffic path validation, bottleneck identification and fault diagnosis. Existing trace back solutions can, in general, be categorized into three types: marking-based, logging-based, and hybrid approaches. In marking-based solutions, routers embed trace back information in transiting traffic (flows or packets), consequently conveying the relevant information to end-hosts for path reconstruction.

3.1 Disadvantages

- Decrease Packet Delivery ratio.
- Increase time delay
- Increase routing overhead

4. PROPOSED SYSTEM

In this paper, we present the design and implementation of an automated resource management system that achieves a good balance between the two goals. Two goals are overload avoidance and green computing.

Overload avoidance: The capacity of a PM should be sufficient to satisfy the resource needs of all VMs running on it. Otherwise, the PM is overloaded and can lead to degraded performance of its VMs.

Green computing: The number of PMs used should be minimized as long as they can still satisfy the needs of all VMs. Idle PMs can be turned off to save energy.

4.1 Advantages of Proposed System

We make the following contributions: We develop a resource allocation system that can avoid overload in the system effectively while minimizing the number of servers used.

We introduce the concept of “skewness” to measure the uneven utilization of a server. By minimizing skewness, we can improve the overall utilization of servers in the face of multidimensional resource constraints.

4.2 Purpose of the Research

We address the problem of IoT security. With the help of SDN, we aim to prevent the attacks at network level instead of device level. Our objective is to protect the IoT devices from malicious attacks and reduce the damage upon an attack. The attack may be launched from the IoT device itself or the device is the target. This helps in fast identification of attacks on IoT devices and initiation of mitigation procedure as appropriate. We have used machine learning techniques to detect anomalies in the traffic.

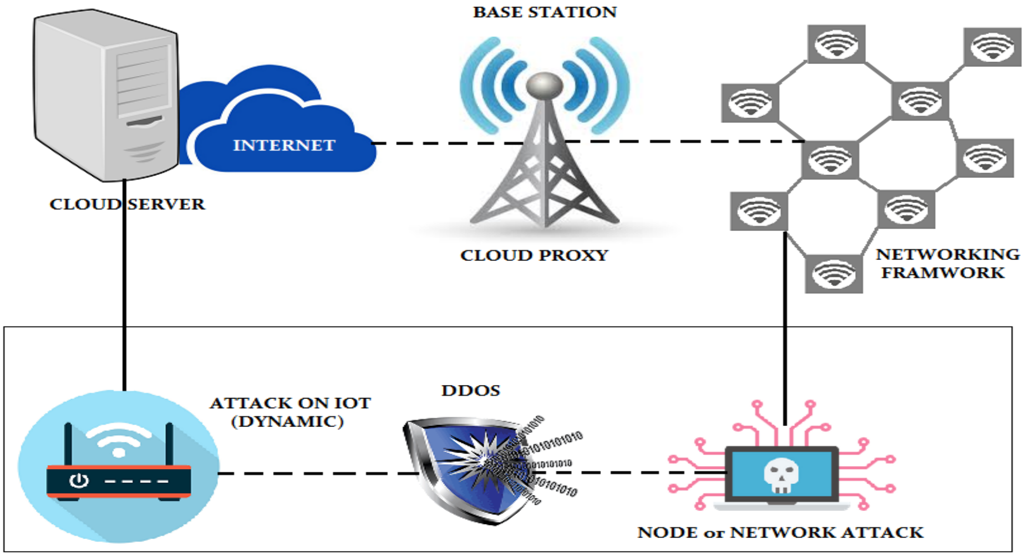

Figure 1. Architecture Diagram

4.3 List of Modules

- Network Topology Construction
- Path Selection
- Packet Sending
- Packet Marking And Logging
- Path Reconstruction
- Attacker
- Authentication

Network Topology Construction

A Network Topology may consist of the no. of routers that are connected with local area networks. Thus, a router can either receive data from the nearer router or from the local area network. A border router receives packets from its local network. A core router receives packets from other routers. The no. of routers connected to a single router is called as the degree of a router. This is calculated and stored in a table. The Upstream interfaces of each router also have to be found and stored in the interface table.

Path Selection

The path is said to be the way in which the selected packet or file has to be sent from the source to the destination**.** The Upstream interfaces of each router have to be found and it is stored in the interface table. With the help of that interface table, the desired path between the selected source and destination can be defined.

Packet Sending

One of the Packet or file is to be selected for the transformation process. The packet is sent along the defined path from the source LAN to destination LAN. The destination LAN receives the packet and checks whether that it has been sent along the defined path or not.

Packet Marking and Logging

Packet marking is the phase, where the efficient Packet Marking algorithm is applied at each router along the defined path. It calculates the Pmark value and stores in the hash table. If the P-mark is not overflow than the capacity of the router, then it is sent to the next router. Otherwise it refers the hash table and again applies the algorithm.

Path Reconstruction

Once the Packet has reached the destination after applying the Algorithm, there it checks whether it has sent from the correct upstream interfaces. If any of the attack is found, it request for the Path Reconstruction. Path Reconstruction is the Process of finding the new path for the same source and the destination in which no attack can be made.

Attacker

Routing attacks can abuse the route discovery and topology generation mechanisms of routing protocols. An attacker could, for example, advertise routes with hop counts higher or lower than real routes. This could be used to attract traffic to malicious nodes to the benefit of the attacker. Malicious activity may result in; the appropriation of data, sinking of packets and modification of packets. All such outcomes impair the networks ability to guarantee safe, private and reliable communication. Unsecured pro-active routing protocols exhibit vulnerability to packet replay and manipulation. Wormhole and Sybil attacks have been analyzed and addressed by protocols such as SAODV and SOLSR. The protection that these protocols offer is aimed at the protection of network routing services. These protocols do not protect data sent over the secured routes.

5. CONCLUSION AND FUTURE ENHANCEMENT

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

6. REFERENCES

[1] ITU report, “The Internet of Things,” 2005.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Elsevier FGCS, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] Gartner report, “Forecast: IoT Security, Worldwide,” 2016.

[4] IDC report, “Internet of Things: Security Practices,” 2016.

[5] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” 6th ACM SIGCOMM conference on Internet measurement, pp. 41–52, 2006.

[6] Dyn attack 2016, http://dyn.com/blog/dyn-analysis-summary-of-fridayoctober-21-attack/, [Online; accessed 18-07-2017].

[7] Mirai Malware 2016, http://blog.malwaremustdie.org/2016/08/mmd0056-2016-linuxmirai-just.html, [Online; accessed 18-07-2017].

[8] K. Palani, E. Holt, and S. Smith, “Invisible and forgotten: Zero-day blooms in the IoT,” IEEE PerCom Workshops, pp. 1–6, 2016.

[9] H. Zhang, A. C. Berg, M. Maire, and J. Malik, "SVM-KNN: Discriminative nearest neighbor classification for visual category recognition," IEEE CVPR Conference, pp. 2126–2136, 2006.

[10] K. Sood, S. Yu, and Y. Xiang, "Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review," IEEE Internet of Things Journal, vol. 3, no. 4, pp. 453–463, 2016.