International Journal of Engineering & Technology, 7 (4.6) (2018) 388-390

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Defending Iot from Ddos Using Lightweight Authentication

G. A. Vani [1] & M. Metilda Florence[2]

[1 & 2] Department of Information Technology-SRM institute of Science and Technology, Chennai, India
**Corresponding author E-mail: vani_ga@srmuniv.edu.in*

Abstract

The emergence of Internet of things (IoT) is due to its ability to dutifully transfer the data through a network. Now the concern is that security is not considered as main priority while developing the product. IoT is prone to vulnerabilities where Botnet and DDoS kind of attacks are common and a major issue that has to be considered these days. Since IoT is in no way resistive to attacks, this paper is all about proposing a solution for the Distributed Denial of Services attack that happens on IoT platform. Light weight authentication is necessary for any IoT devices because to reduce the power consumption and increase the processing speed of the device [16]. The experimental setup is built on OS named Contiki with cooja simulator that suits to all the devices that are in the IoT environment.

Index Terms: *Internet of things, Distributed Denial of Services attack, network, algorithm, defense methodology.*

1. Introduction

IoT is the internet development platform-based technology which had gained its prominence in this internet world by connecting the physical devices to the internet. The reason behind IoT is automatic exchange of the data dutifully [2]. The speciality is that IoT does not require any human interaction to control. Which in the sense means that IoT is composition of both software and hardware. To be simple IoT is an object interfaced to internet to send and receive the data by controlling its network by self. The major difference between DoS and DDoS is that, DoS involves a single system and single internet connection whereas the DDoS involves multiple systems and connections to flood the systems.

A. Vulnerabilities in IoT
A. Loopholes In web interfaces:
IoT could allow its user to interact with but at the same time the security concern is that it also, the unauthorized user to access. The possibilities of attacks in this are:
(I) Account Enumeration
(II) Cross-site Scripting
(III) SQL-injection

B. Inadequate Authentication and Authorization:
This is due to its inability and improper built of the security design to authorize or to authenticate its legitimate user. The possibilities of attacks are are:
(I) Privilege Escalating
(II) Password guessing

C. Insufficient network services:
Improper network services to validate authorized user. The possibilities of attacks are:
(I) Denial of Services
(II) Buffer overflow
(III) Distributed denial of services

B. Distributed Denial of Services
DDoS is the subset of Denial of Services which collectively acts like botnet i.e., effects multiple devices connected to the open sources. Few attacks just try to breach into the machines without any intention to cause damage unlike them DoS kind of attacks are purely based on the connection termination or service termination to the legitimate users [5]. The assaults may loss even a month. On an application layer there is a chance of DoS or DDoS attack chances to take place by overloading the server machine with huge number of requests. On a network layer it can clog the network lines or the point where the connection can begin or end. The massive raise of IoT Botnets caused Domain Name System (DNS) server to fall down leading to Distributed denial of services attack. DNS is the server that converts domain name to IPs vice versa. Once it is attacked through DDoS it starts resolving its functions improperly [11]. Mirai Botnet is one good example of it. Mirai is a malicious code that affects the devices connected to IoTs. It can involve millions of IP addresses. Therefore, this gave an alarm for the organizations to ensure that all the security mechanisms are up to date and the devices inside them are well protected [6]. Finally, there is no more limitations to scale the future DDoS attacks driven by IoTs.

2. Related Works and Existing Method

By enhancing the features in the Intrusion Detection System (IDS), Kasinathan.P [6] proposed a solution for UDP flood attack in the Contiki operating system that was designed for IoT simulations.
Sudip Misra [7] proposed a solution for DDoS attack on IoT platform using Service Oriented Architecture (SOA) which detects and alerts the members by raising the alarms. And also positive result was seen in this.
Another model of solution was proposed for ICMP flood attack on IoT system which was not recommendable for mobile end users [8].

Sonar [9] proposed a solution for DDoS attack but this had a poor performance in terms of packet delivery ratio. But also, this earned 50% of result.

3. Proposed Methodology

The recent studies have shown that the DDoS attacks had been increased in 2018 compared to 2017 [10]. In addition to this Botnets has increased to threaten the users/cyberspace by exploiting into zero-day vulnerabilities. Computer Emergency Response Team (CERT) according to CERT, the major issues were security vulnerabilities in IoT devices. They stated that most of the IoTs are not getting integrated into the embedded security mechanisms. Finally, in order to defend IoT from the DDoS attack the organization should be protected, capable of detecting illegitimate traffic [15]. Not only the IoT environment and also due to its Resource constrained nature which is more prone to vulnerabilities is one main reason to give way to DDoS attack to take place. The current paper proposes a solution to flooding attack on the internet. The network here is of private network.

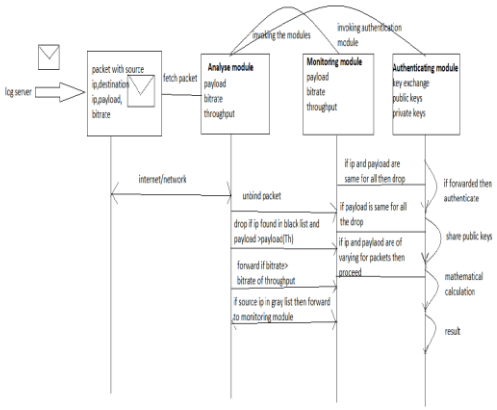

Fig1: A collaborative design of the system.

The above diagram illustrates about the invoking of phases in between and the functions inside each phase. The explanation is stated below.

The algorithm consists of three phases:

a. Analysis Phase
b. Detecting Phase
c. Authorising/Authenticating phase

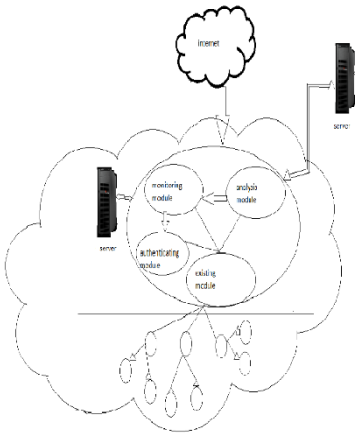

Figure2: Conceptual design

In the analyzing phase the traffic coming towards this network will be analyzed in such a way that the packet is malicious or not. Then the packet will be forwarded to Detection phase. Later comes the authenticating/authorizing phase, which gives privileges to packets after monitoring that the packet is non-malign and can travel through the network.

The proposed solution will work on 3 modes. First two levels will perform the checks on the packet by analyzing and detecting. Latter authentication. The analysis mode will collect each packet crossing its network. If the packet belongs to its network then the packet will be thoroughly performed checking to find whether the packet is having blacklisted IP on it. Next bit-rate, if the bit-rate of the packet is normal and it is having non-suspecting message content then the packet would be processed further.

The detection phase, this module will be invoked by the analysis module. If the packet is exceeding its threshold limit of its payload and the packet is from grey-list then this can be said that it is kind of attack named Denial of Service. Then the packet will be included in black-list. If the packet with similar features but of different IP addresses then it is DDoS attack.

Algorithm for Analysis Phase:

Analysis Phase:

1. Start
2. If IP belong to Black-list
3. Drop ()
4. else if Bitrate >=throughput
5. forward
6. else
7. payload>=throughput payload
8. drop ()
9. else if add IP to grey-list
10. forward as suspected packet
11. end

Algorithm for Detection Phase:

Detection Phase:

1. start
2. if payload is same
3. drop ()
4. alert: attack detected
5. else
6. proceed ()
7. end
8. if payload is malign
9. drop ()
10. else
11. proceed ()
12. stop

Algorithm for Authorizing phase:

Authorizing phase:

1. start
2. fetch packet
3. select keys
4. share the public keys
5. encrypt the packet
6. send to target
7. decrypt with private keys if necessary
8. stop

Why light-weight authentication?

Since IoTs are wearable and devices, the main aim would be on data collection and its richness [13]. Asymmetric algorithm or symmetric algorithm, whichever it might be its aim is to secure the communication between the devices [14]. The

mechanism/algorithm that has the tendency to authenticate by being simpler and faster on the platform is said to be authentication. Light-weight is nothing but simple and fast. As There are many algorithms that are efficient for security purposes, the point to be concern is all about its computations and mathematical calculations. As there are huge chances of performance deductions on processing heavy computation in the environment, light weight algorithms helps in overcoming the problem of performance deductions.

4. Conclusion

The proposed method is very simple in identifying the DoS and DDoS attacks. The design proposed system here is the general network with request handling servers with client systems Although the paper is about lightweight authentication, the paper involves mostly on analyzing and detecting of the attack and later authentication follows. The proposed solution is carried by using the tool Contiki Operating system using sky motes. As the mentioned solution is only for the DDoS attack, the future work of the paper is to carry analysis on different attacks. The currently proposed solution when compared to previous solutions is very simple. Therefore, by integrating this with authenticating schemes we can hopefully have a secure environment. The proposed method is very simple in identifying the DoS and DDoS attacks. The design in the proposed system here is the general network with request handling servers with client systems.

References

[1] https://ww.iotforall.com/5-worst-iot-hacking-vulnerabilities
[2] http://www.gkmit.co/articles/internet-of-things-iot-introduction-applications-and-future-scope
[3] https://www.cso.com.au/article/575407/internet-things-iot-threats-Countermeasures
[4] https://www.incapsula.com/ddos/denial-of-service.html
[5] https://www.corero.com/blog/870-the-rise-of-iot-botnet-threats-and-ddos-attacks.html
[6] Kasi Nathan P, et al. "DEMO: An IDS framework for internet of things empowered by 6LoWPAN." Proceedings of the 2013 ACMSIGSAC conference on Computer & communications security. ACM, 2013.
[7] Misra S, et al. "A learning automata-based solution for preventing distributed denial of service in Internet of things." Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing. IEEE, 2011.
[8] Hsiao-Chung LIN, and WANG Ping, "Implementation of an SDNbased Security Defense Mechanism Against DDoS Attacks."DEStech Transactions on Economics and Management, 2016.
[9] Sonar K. and Upadhyay H., "An Approach to Secure Internet of Things Against DDoS." Proceedings of International Conference on ICT for Sustainable Development. Springer Singapore, 2016.
[10] https://www.bleepingcomputer.com/news/security/dramatic-increase-of-ddos-attack-sizes-attributed-to-iot-devices
[11] https://dzone.com/articles/cert-analysis-on-iot-botnet-and-ddos-attacks
[12] https://www.networkcomputing.com/network-security/iot-based-ddos-threats-loom/1614938156
[13] https://ieeexplore.ieee.org/document/8039175
[14] https://ieeexplore.ieee.org/document/8073643
[15] https: www.networkcomputing.com/network-security/iot-based-ddos- Threats
[16] https: www.ncbi.nlm.nih.gov/pubmed