ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Intelligent IoTs: Stave Off From DDoS Attack

Suparna .H .S
M.Tech Student
Department of Computer Science and Engineering
JNNCE Shimoga, Karnataka, India

Abstract:
We are living with interconnected devices in the era of Internet. These things are called “Internet of Things” which are connected through internet are making our life easier as well as complicated by compromising with the security issue and becoming “Insecure of Things” by greeting attacker to cause threat like DDoS (Distributed Denial of Service). This paper gives two novel approaches for improving IoTs, by preventing the system from getting enslaved and more importantly to detect and prevent DDoS attack by combined approach which includes behavior analysis model, conditional legitimate probability (CLP) ratio to serve legitimate traffic by fair share approach and C/R mechanism to distinguish between bots and real users..

Keywords: Intelligent IoTs, DDoS attack, includes behavior analysis model Challenge response (C/R), fair share mechanism.

I. INTRODUCTION

The term “Internet of Things” (IoT) was first coined by British technology pioneer Kevin Ashton [1] in the year 1999 who said “The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more” in RFID Journal. In internet of things, The ‘thing’ refers to an object with respect to user perspective which are having an IP address and is capable of collecting and transmitting the commands over the network without human intervention, it can be the sensors which SWITCH ON Air Conditioner 5 min before we reach our home, it can be door lock that locks itself when we exit from home or office or the device that maintains the vehicle health and intimates the user, like this IoT basically deals with connected things in our surrounding, as connected devices are growing day by day it is estimated that it may reach upto trillion by 2020 said the statistics. Recently, a series of massive DDoS (Distributed Denial-of-Service) attacks have occurred using botnets.

They were mainly propagated through compromised Internet of Things (IoT) devices like webcam, these massive attacks have highlighted the risks resulting from inadequate security mechanism in Internet of Things (IoTs) device, together with their worst effects on the Internet itself. Here, “Botnets” are networks made up of remote-controlled computers which are infected with malwares called "bots" and these bots contacts a remote server and gets in contact with other nearby bots and waits for instructions from whoever is controlling the botnet remotely through Command and Control infrastructure i.e. “Botmaster” who uses distributed computer over thousands of compromised systems to have DDOS attack on one target system.

Intention of attack is to attempt and make an online service unavailable by overwhelming it with traffic from multiple sources. Targets may be commercial websites, banks, news websites etc. This DDoS attack mimics the normal traffic and the incoming traffic floods into targeted servers by different sources and makes it impossible to stop the attack by blocking the IP addresses and even difficult to prevent it. There is a need to have improved IoT architecture and servicing algorithms at router level to detect and prevent DDoS attack.

II. RELATED WORK

A. IOT reference architecture

IoT reference architecture in [2] has four layers with the following capabilities.
1. Application layer which maintains IoT applications and authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus.
2. Service support layer and application support layer provides generic and specific support capabilities.
3. Networking layer provides relevant control functions of network connectivity, such as authentication, authorization and accounting and Transport capabilities which focus on transportation of IoT related control and management information and provide authorization, authentication, use data and signaling data confidentiality and signaling integrity protection.
4. Device layer provides two capabilities such as device capability which gathers and uploads data directly, indirectly or in ad hoc manner. It has gateway capability and provides authentication, authorization, device integrity validation, access control, data confidentiality and integrity protection. Management capabilities in this layer is similar to traditional communication networks, IoT management capabilities cover the traditional fault, configuration, accounting, performance and security.

B. Detecting DDoS attack through chaos theory

Chaos theory effectively detects DDoS attacks [3] by differentiating DDoS attacks from legitimate burst traffic. Predictability analysis on network traffic which shows that low-pass filtering and multiplexing can provide better predictability. However, due to the burst in network traffic, there is a possibility of large prediction error. Therefore these time series models should be relatively stable. Network traffic model is divided into two categories. Traditional traffic model and new traffic model. In this approach, after collecting network traffic packets and flow information, all network traffic is sampled and prediction of network traffic is obtained by suppressing the network traffic. This is done by pre-processing the traffic by cumulatively averaging the sequence xn with a time range to get prediction error which predicts whether traffic is normal or DDoS. No mechanism of preventing attack is incorporated in this approach.

C. Prevention of DDOS Attacks using New Cracking Algorithm

In this approach, it follows Packet filtering act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will discard the packet. It is observed that a web transaction typically consists of hundreds or even thousands of packets sent from a client to a server. During a DDoS attack, since the packets will be randomly dropped at high probability, each of these packets will go through a long delay [4] due to TCP timeouts and retransmissions even though it assures that only first packet is delayed, random packet dropping may result in the loss of legitimate packets too. Consequently, the total page download time in a transaction are delayed.

III. PROPOSED IOT ARCHITECTURE

Tradition architecture [5] of IOT consists of 4 layer and reference architecture of IoT contains 7 layers respectively. Here, proposed architecture of IoT is the integration of 5 layers as shown in the Figure 1.1 which concentrates on providing better security and data management in IoT environment.

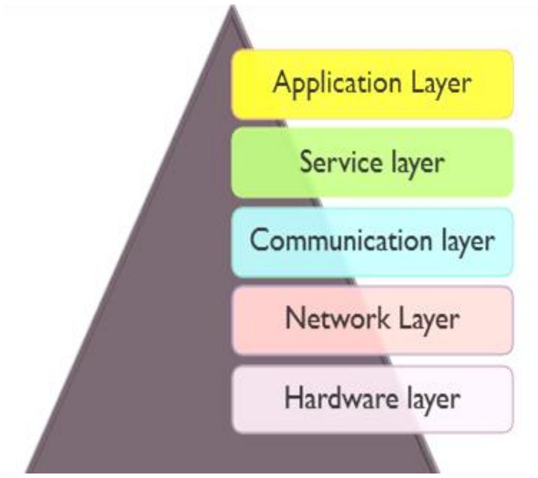

Figure.1. Proposed IoT architecture with five layer

Proposed IoT Architecture is the integration of 5 layers to perform various activities based on user perspective. Functionalities of five layers are

1. Application layer

Application layer is at the top in architecture framework which is responsible for providing applications to users in IoT environment and this layer should be equipped with the functionalities like authorization, authentication and Identity Management.

2. Service layer

Next layer is service layer which concentrates on service storage, composition and its organization. It also performs IoT monitoring and resource allocation and has database to check the credentials of authenticated user and provides requested services.

3. Communication layer

Communication layer is responsible for flow control mechanism and optimization function and all the decision making related to communication are made in this layer which also implements IoT web portal.

4. Network layer

Network layer is important in IoT stack which provides routing and addressing for the packets, it includes transportation capabilities and involves error detection and correction, capable of serving wide range of IoT applications with required speed. Many hybrid network models are built to support communication requirements for latency, bandwidth and security. This layer should be equipped with the feature of tracking the traffic that flows through it, where implementation of intelligent routers, gateways that process the legitimate traffic to its upper layer need to be monitored and given a fair share for packets to avoid DDoS kind of attack in IoT System.

5. Hardware layer

It includes embedded systems, sensors which process information based on real time and has integrated objects these elements provide identification and information storage (e.g. RFID tags), information collection (e.g. sensors), and information processing (e.g. embedded edge processors).This layer is made prominent to have proper identification for each IoT devices due to lack of physical hardware in IoT devices. Eg: webcams, modems etc. which are prone to attack as it shares network related information across the network so, attacker can get information through vulnerable insecure devices connected to Internet hence providing prominent on board security is required. Consider an attack-free scenario with respect to the proposed architecture explained through the Figure 1.2

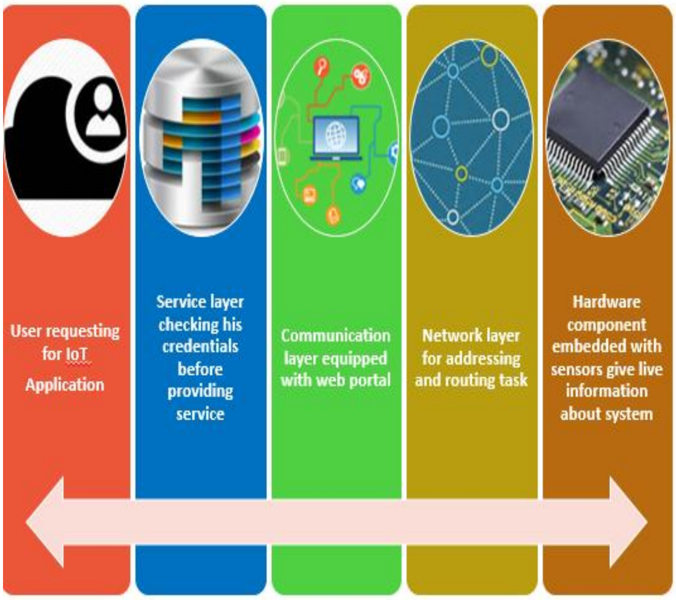
User requesting for IoT Application
Service layer checking his credentials before providing service
Communication layer equipped with web portal
Network layer for addressing and routing task
Hardware component embedded with sensors give live information about system

Figure.2. Attack-Free Scenario example supporting proposed architecture.

The first layer is the application layer where user should request for the services and in service layer requested user identity should be checked with his credentials registered in IoT database, then the hardware layer, includes the embedded components like sensors, RFID reader etc which places information about object on network layer, which includes the multiple networks with various technologies give information back to communication layer, where the IoT Web portal reside and performs cross platform communication using different protocols like HTTP, FTP and others. The communication layer transmit this live information to the services layer, where all decisions related to the monitoring, storage, organization, resources allocation (request based resource allocation is required in IoT to handle attacks) are made. Then, the received information is transmitted from the services layer to the application layer, where it goes to the authorized person to receive this information. And he can do additional request to retrieve the further information from the application if needed. These are done at basic level to avoid attackers gain access into our network by knowing device credentials and not letting to have control over system.

Basic IoT security challenges and measures to make IoT Intelligent and to prevent system from bots.

1. Need to have on board security
IoT devices are small, inexpensive devices which are little and having no physical security these computing platforms, constrained in memory and resources with limited security computing capabilities even encryption algorithms need higher processing power. Hence there is a need to design devices which includes on board security.

2. Laws, policies and certification
IoT devices that are existing in market are compromising with security and need to have certification on goods or things which are having authorized certification.

3. IP address usage
Products equipped with IP address and are not under use should kill the IP address, so that we can minimize systems getting enslaved by the attackers, It is mandatory to disconnect Internet enabled systems after use.

4. Management of ID and Password
Preset ID of IoT devices should be changed frequently, so that attacker cannot guess the password stored in the service provider server and can reduce the systems getting compromised with security. Eg: In IoT environment stealing content from unprotected webcams breaking into home control systems.

5. Antivirus and firewall
Antivirus software should be made up-to-date and install the latest security patches for computer, and usage of firewall to control programs that can gain access to the machine via the Internet.

6. Downloading free-wares
Downloading free-wares downloads Bots (malicious piece of code) into the system and user privacy is hampered and even systems get enslaved by bot master to launch DDoS attack. Once the system/device has been compromised, attacker run a small piece of program that communicates with all the compromised computers that they control and they can command those computers to start sending out requests across the internet to a specific server or website in a short period of time leads to paralyze the entire network and its impact results in DDoS attack.

IV. DDOS ATTACK ON IOT DEVICES

DDoS Attacks (Distributed Denial of Service Attacks) attempts to make online service unavailable by with its traffic from multiple sources where an attacker enslave multiple machines to carry out a DoS(Denial of Service) attack simultaneously, it utilizes resources and bandwidth. A botnet is powerful, and mimic the normal traffic. It is difficult to detect the attacker traffic from legitimate traffic. Hence there is a need to prevent not the attacks but the traffic that reaches the victim.

1. Combined Approach to Combat DDoS Attack

Novel approach to discard the attacker packets entering into the network and hitting the victim includes the following four major steps

Step 1: Analysis of the traffic baseline behavior
Step 2: Computing the Conditional Legitimate Probability
Step 3: Servicing using Fair share approach
Step 4: Challenge response mechanism

1.1 Analysis of the traffic baseline behavior

A nominal traffic consists of various packet attributes. Packet attributes of IP headers shown in Figure 1.3 which includes TTL (Time To Live), Packet Size, Protocol Used, Port Number etc. Based on the packets causing a traffic burst, data is gathered and compared to the baseline behavior attributes of normal traffic. If a suspicious behavior is detected, a deeper inspection process is triggered, which analyzes application-level parameters and resolves whether the suspicious behavior is a result of a legitimate burst of application traffic or a result of a malicious application .

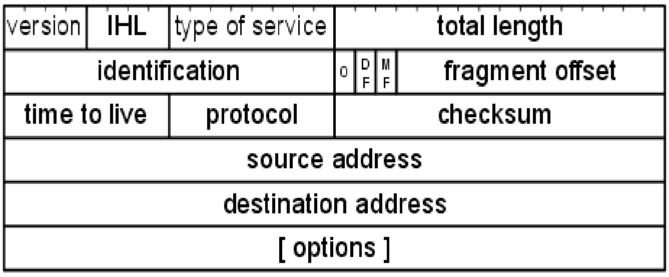

Figure. 1.3 IP header Format

1.2 Computing Conditional Legitimate Probability
The Conditional probability is produced by comparing traffic characteristics during the attack with legitimate traffic characteristics which gives the ratio of nominal packets by total packets involved in traffic. Consider a scenario where requesting packets from different sources causing a traffic and have anomaly in their behavior but cannot able to find whether it is caused by normal traffic or by attackers. So, in order to find the ratio of nomial traffic by total traffic we need to compute Conditional Legitimate Probability (CLP) [6]. Which includes few parameter to have calculation based on Bayes theorem and conditional probability. Consider Packet P arriving into the network which has few attribute values as seen in section 1.1 like TTL, Packet Size, involving the set of discrete value like attribute value Pv.

Eg: attribute of TTL= T{t1,t2,t3}, Packet Size S={s1,s2,s3} so on.

During an attack there are Pl legitimate packets and Pa attack packets arriving in T seconds totaling Pt (total packets). Selecting the probability of attribute values among the legitimate packets we have The Conditional Legitimate Probability (CLP) which is given by

$$CLP\ (Packet\ P) = P\ (Packet\ P\ is\ legitimate\ [Pl]\ \mid\ p\text{'s}\ attribute\ [Pv]\ , \ldots) \rightarrow \textbf{eq(1)}$$

According to Bayes' theorem, the conditional probability is given by

$$P\ (Pl \mid Pt) = P\ (Pl\ nPt) \mid P\ (Pl) \qquad \rightarrow \textbf{eq(2)}$$

Therefore,

$$CLP\ (P) = \frac{Pl * [Pl / Pv[a] + Pv[l] + \ldots]}{Pt\ * [Pt / Pm[a] + Pm[l] + \ldots]} \qquad \rightarrow \textbf{eq(3)}$$

Here we get the ratio of legitimate traffic over total traffic

i.e $Pv\ [A] / Pm[A] = partial\ score \rightarrow$ **eq(4)**

Computed by the equation 3.

Partial score obtained is stored in a score sheet for further comparison where stored value takes the log value computed by taking less time which is required to set the threshold to discard the attacker packets.

1.3 Servicing valid customer using Fair share approach

Fair share among the directly connected links is not good enough because in a structure of hierarchical routers upper router forwards all packets to the lower router. However, lower router only offers fair service to its inputs, it will discard packets which include both good and bad packets i.e in C/R mechanism we get valid customer packets there might be a chance of getting invalid packets generated by bots. The set of packets that are considered as good by checking partial score in score book is retained and fair service approach is done by rate limiting so that it limits the high rate packets arriving by fair service [7] provided over a large traffic from getting service after that victim limits the rate from the visible sources that send it packets at high rates. Each limit applies to packets with a particular visible source and a destination address in a particular range. However, limit the rate at which they are processed results in fair scheduling by visible source.

1.4 Challenge Response Mechanism

Fair scheduling by visible source is done which have chances of some unexpected invalid packets generated by bots still entering the system can be verified before providing service to it by Challenge response mechanism. It provides a secure mechanism to check Expected packets from valid customer over legitimate traffic v/s packets generated by bots. Based on the selection made challenges are sent and based on the response, source is determined whether it's a valid customer request or not.

For C/R mechanism CAPTCHA can be used which determines the source is a Bot or a real user[8], since a normal human can easily read the CAPTCHA, while the bot cannot process the image letters. To use the C/R mechanism, an attack mitigation system launches a series of queries to the source of a request in question, and according to the responses received, it decides whether to send an additional, more sophisticated challenge, or flag the source as a malicious user. C/R mechanisms use automated processes, and require no human intervention. Figure 1.4 shows the details structure of the combined approach involving the above mentioned steps to detect and prevent DDoS attack.

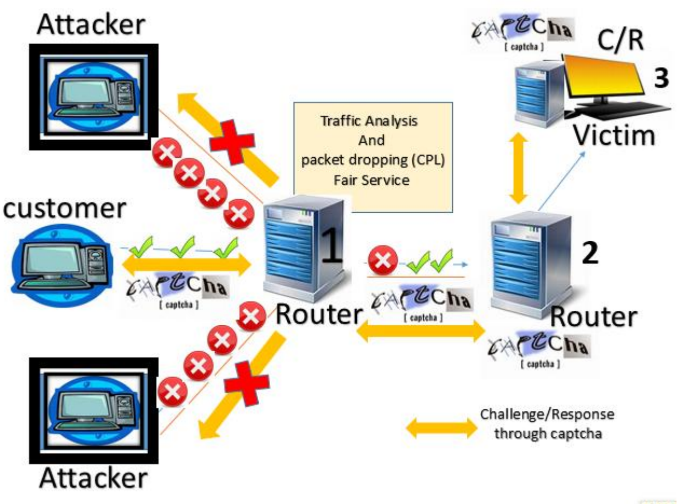
Attacker
CAPTCHA [captcha]
C/R
3
Victim
Traffic Analysis And packet dropping (CPL) Fair Service
customer
1
Router
2
Router
Challenge/Response through captcha
Attacker

Figure.4. Combined approach to detect and prevent DDoS attack

Implementation Consideration remarks,

- IoT devices used should not be compromised and have vulnerability
- During attack traffic should not hit victim server directly instead a virtual machine or intermediate router should be equipped with this mechanism to check the traffic.
- Challenge / Response should not be compromised
- By this approach Servicing will not be denied but processing requires bit longer time than expected.

V. CONCLUSION

Every device connected to the internet are made intelligent to protect themselves from an attacker so that we can prevent those devices from getting enslaved by the attacker to launch an attack. Here, proposed combined approach at router level helps in detection of legitimate traffic and prevent system from DDoS attack. .

VI. ACKNOWLEDGEMENT

I would like to thank Dr. Poornima K M Professor, Department of computer science and Engineering for extending her help in completion of the task. I would thank our guide Mr. Ravindra S for the guidance. I am also grateful to Dr. Nirmala Shivanand Prof. and Head of Computer Science and Engineering Department, JNNCE, Shivamogga for her indispensable support.

VII. REFERENCE

[1]. Chatzigiannakis et al., "true Self Confugaration of IoT", IEEE Latin America Transaction, pp 1667-1672,ISSN 1548-0992,volume 10,Issue 3,April 2012

[2]. Dina Gamal Darwish , "Improved Layered Architecture for Internet of Things" , International Journal of Computing Academic Research (IJCAR) ISSN 2305-9184 , Volume 4, pp.214-223,August 2015

[3]. Anjali. M, B .Padmavathi, "DDoS Attack Detection based on Chaos Theory and Artificial Neural Network",) International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Volume 5, pp.7276-7279, 2014

[4]. V.Priyadharshini , Dr.K.Kuppusamy,” Prevention of DDOS Attacks using New Cracking Algorithm”, International Journal of Engineering Research and Applications (IJERA) , ISSN: 2248-9622, Vol. 2, Issue 3, May-Jun 2012, pp.2263-226

[5]. Arpit Kumar,” Internet of Things and its enhanced data security”, International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-2, Issue-2, February 2015

[6]. M.Sivakumar, C.Senthilkumar,” Enhanced Detection and Prevention of DDoS Attacks using Packet Filtering Technique”, (IJCSIS) International Journal of Computer Science and Information Security National Conference on Research Issues in Image Analysis & Mining Intelligence ISSN: 1947-5500, 2015

[7].Donald Cohen K. Narayanaswamy, A Fair Service Approach to Defending Against Packet Flooding Attacks

[8]. https://security.radware.com/ddos-knowledge-center/ ddos pedia/ ddos-attack/

[9]. Ronen Kenig, Distinguish between legitimate users and attackers, The secret sauce of DDoS protection ,Radwareblog June 18, 2013