A Rule based Approach to Mitigate DDoS attack in IoT Environment

Kishan Patel[1], Hardik Upadhyay[2]

[1] *Research Scholar, GTU PG School, Gujarat, India*
[2] *Assistant Professor, GPERI, Gujarat, India*

ABSTRACT

Nowadays, there are lots of Internet of Things (IoT) devices are used in Industry, Home appliances, Automobile industry and many more places. Issues regarding security of the IoT are the primary reason why it fails to attract more people. Each day, beside the new technology comes a millions of vulnerabilities waiting to be exploited. IoT is that the latest trend and like all technology, it's open for exploitation. In IoT environment, Distributed Denial of service attack (DDoS) could be a major issue, because of the limited computing and power resources of standard IoT devices are prioritized in implementing functionality instead of security features. DDoS attack is the most common attack which is used to bring down the whole network without having any loophole in the network security. The main purpose of this work is to mitigate DDoS attacks against the IoT using honeypot model in Raspberry Pi. Honeypots are the network setup with intentional loopholes. The purpose of honeypot is to invite attackers, so the activities and methods used to attack can be studied and it can also help to increase network security. Conclusion came out after reviewing some research papers that there are lots of DDoS attack mitigation techniques are proposed by many researchers, but very few are proposed for IoT environment. Primary focus of this dissertation work is to proposed mitigation techniques of DDoS attack on IoT device using honeypot and IDS with low cost and high performance resources.

Keyword: *Internet of Things, Denial of Service Attack, Distributed Denial of Service Attack, IoT security, Security Breach*

1. INDRODUCTION

1.1 Internet of things

Internet of Things is not another word now-a-days for anybody in light of the fact that everything now going to be accessed by means of Internet. The word *IoT* defined by Wikipedia as, "*The Internet of things (IoT) is the network of physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data."*[1] The "thing" in the internet of thing can be a person with a smart watch, a farm with some sensors, car that has built-in sensors to notify the driver when any object near the car or any other devices that has IP address for connecting to the network for the transfer of the data. Internet of Things (IoT) speaks to a general idea for the adaptability of system gadgets to detect and gather data from the globe around us, at that point share that information over the web where it will be handled and used for various interesting purposes. These days some utilization the term Industrial Internet conversely with IoT (IIoT). This alludes basically to business uses of IoT innovation in the realm of manufacturing.

1.2 Dos/DDos Attack

A denial of service (DoS) attack take effect once a service that might usually work is inaccessible. There may be many reasons for inaccessibility, however it always refers to infrastructure that can't cope because of capability overload. During a Distributed Denial of Service (DDoS) attack, an oversized range of systems maliciously attack on one target system or network. This attack can be often perform through a botnet, where there are lots of devices are preprogramed to request a particular service at same time.

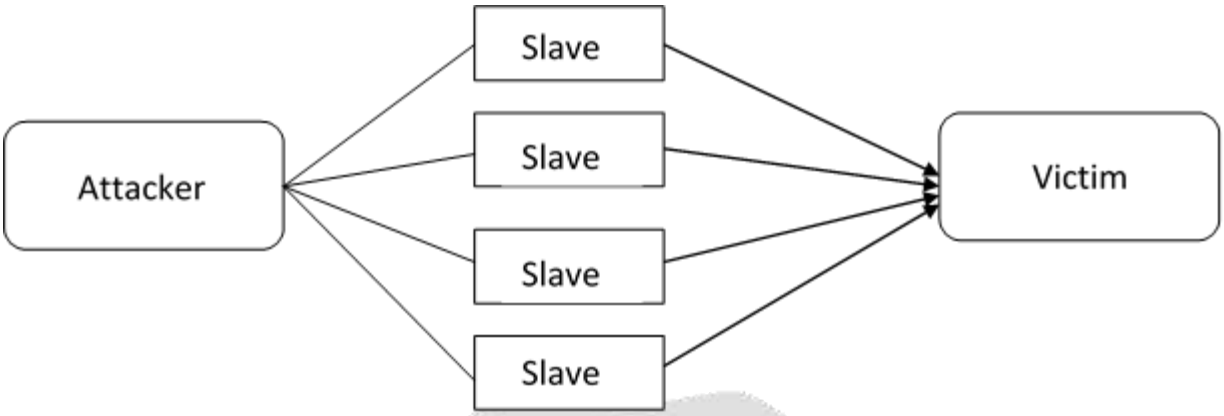

Fig.1: DDos Attack flow

In fig.1 general DDos attack flow is shown where attacker use slave systems as botnet to perform attacks like send flood packets into victim system to consume resources and network bandwidth. Nowadays people are getting used to IoT devices i.e. smart watches, smart phone, smart refrigerator, etc. As increasing usage of IoT in their daily life number of devices are increased day by day, so attacks related to IoT became major concern. Above described attacks are common attacks happened in IoT environments. Among them DDoS attack would be a very danger attack because of its characteristic take benefits of limited computing power of IoT device. DDoS attack made device unavailable or irresponsible. On the cusp of 2017, one thing's clear: distributed denial-of-service (DDoS) attacks created their mark in 2016. Arbor Networks half-track 124,000 DDoS attacks every week between Jan 2015 and June 2016. Moreover, 274 of the attacks determined within the first half of 2016 reached over 100 Gbps (as compared to 223 in all of 2015), whereas 46 attacks registered higher than 200 Gbps (as compared to 16 in 2015). Together, those campaigns' peak attack size inflated by 73 % to 579 Gbps.

1.3 CLASSIFICATION OF DDOS ATTACK

1) ***UDP flood***
2) ICMP/PING flood
3) SYN flood
4) Ping of Death
5) DNS amplification

2. RELATED WORK

Authors in paper [2] gave an equipment based watermarking checking framework technology to shield organizations from these attacks. This techniques utilizes trust investigation of the incoming packets using trace-back methods. In this procedure just the trusted packets are permitted inside the network. Authors in paper [3] introduced an intrusion detection system that uses a layered model integrated with neural network. They proposed two models in particular A and B where model A considers all features of the practice dataset and B considers features adding to the order procedure. This proposed framework detects four regular types of attacks like DOS, Remote to local (R2L), User to root (U2R) and ordinary records. This framework used the KDD 1999 database with a specific end goal to accomplish accurate results. Further, this approach other than detecting wide variety of attacks additionally has less false alarm rate. Paper [4] gives solution for DDoS mitigation using software defined network. This paper gives solution free from the limitation of proprietary software of routers. Here author presents approach for anomaly detection using SDN infrastructure in which collection of traffic data flow information which is maintained on all the SDN enabled switches placed on network. This method successfully achieve high detection accuracy. This mitigation technique need some future work of sharing in-line sampling based ADSs in an efficient way to overcome burden of growing IP traffic and limited computational resources. Author in [5] presents detection and mitigation of DDoS attack methods which are distinguish by various stages. All the stages are capable to filter malicious users of DDoS attack. Stages are named as restriction of user access, limitation of traffic rate and

CAPTCHA verification technique. In Restriction of access, Blacklisting of IP address is used as concept. In Limitation of rate and Captcha verification stage, reducing the rate of http connection bound the same IPs accessing with the same object in the server. In paper [6] author proposed system in which the Dendric Cell Algorithm (DCA) continuous check the traffic and compare the SYN packet and SYN-ACK packet ratio. If the ratio is higher than median value, it means there is lot of SYN packets are incoming and very little SYN_ACK packet. Like that TCP SYN flood attack is detected. This proposed system is could be used with IDS system and it is implemented in python language. Authors in [7] proposes an event detection system which can be embedded into IoT devices. The proposed module able to focuses on the system behavior under DDoS attacks and detects it by information obtained from NTP (Network Time Protocol) used in time synchronization service. The advantage of this solution is that, it is different from the existing ones, it does not require any expensive equipment or tools (e.g. monitoring server) nor periodic maintenance involving technical knowledge.

3. PROPOSED SYSTEM

Based on conducted survey about mitigation techniques of DDoS attack on IoT devices as it has low computing power, providing security in every device is not possible. However at the present juncture this research remains theoretic with only theoretic models being proposed. The practical implementation of Rule based detection and mitigation in IoT systems for the purpose of DDoS attack prevention is an area that remains unexplored. With keeping this in mind, we would plan to deploy a rule based security system for an IoT environment in this research work. Use of rule based detection system would be helpful to mitigate DDoS attack as well as collect information of the attacker so that information could be used for future attacks prevention. Use of rule based security system in Raspberry Pi is might be cost effective solution. After reviewed some research paper about DDoS detection techniques, using rule based intrusion detection system is still unexplored area for IoT environment. To mitigate Dos attack in IoT environment by using rule based security system which is protect like pillared with a verification system to maintain the efficiency (data received/data transmitted).

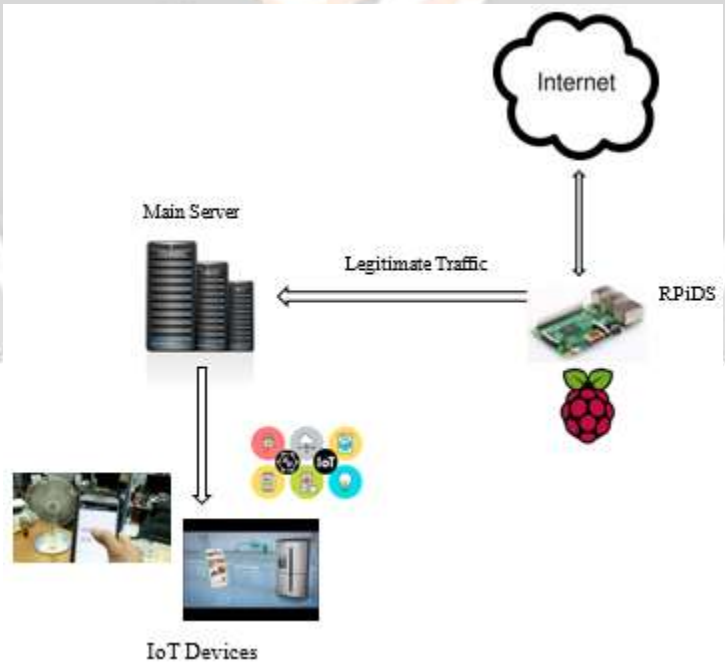

Fig.2: Proposed system architecture

3.1 Proposed system (Flow Diagram)

Overall flow diagram of the proposed work as shown below. Proposed work divided into two part as detection of the malicious traffic and mitigation of the DDoS attack.

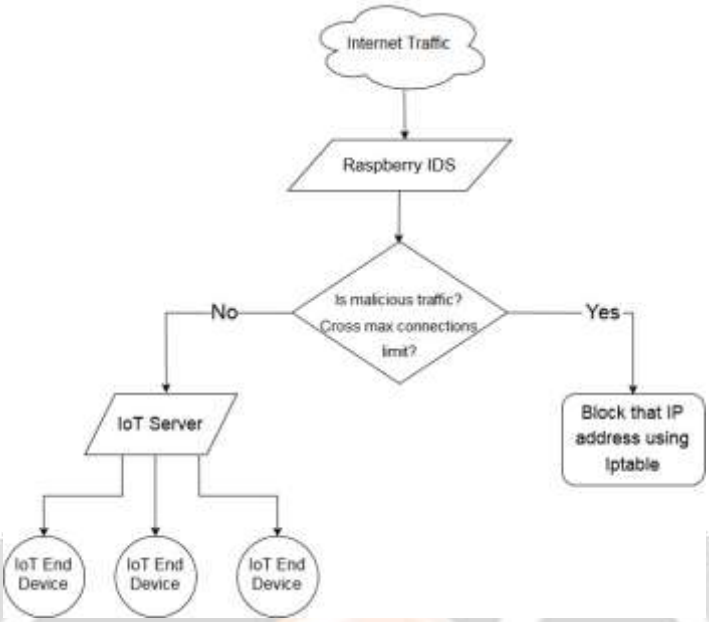

Fig.3: Flow diagram

Overall process of the detection and mitigation of DDoS attack following below flow diagram.

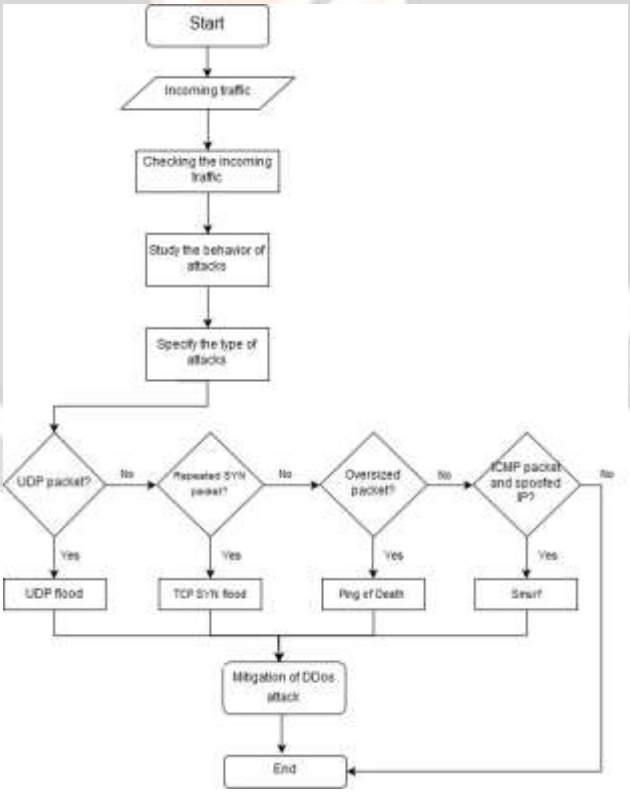

Fig.4: DDoS detection Flow diagram

Proposed system is work according to above flow diagram. Whenever client request coming from internet for any IoT device, first of all, the request is inspect by RPiDS for any illegitimate request. If IDS system detect any malicious traffic or check for max connection limit crossed then that IP address blocked by Iptables rules. Iptables

then inspect the packet associated with the request. If it can find ICMP flood, UDP flood, SYN flood, TCP flood and HTTP flood attack then block that IP address. RPiDS device is raspberry device with Raspbian OS, having capability of detect intrusion based on rules and mitigation based on Iptables.

4. IMPLEMENTATION

Flow of the implementation would be described here. Implantation work divided into three parts as following:

Installation: Raspbian OS on Raspberry Pi device, Snort IDS in raspberry PI, DDoS Attack tools in windows OS, Kali Linux for more attacking tools, Putty and Windows and Linux OS on 5-6 machine for DDoS attack.

Configuration: Raspberry Pi access using SSH via Putty, Snort configuration for Raspberry Pi network interface, Create and Set Rules for Detection of DoS and DDoS attack and Create and Set Rules for Iptables in raspberry pi, Setup attack tool on Kali and Windows OS, Network interface, Backup Raspberry Pi, Prepare testing bed, Search for various tool for DDoS attack, Install them on 5-6 machine, Set bandwidth according to test case and Connect all the machine with raspberry pi network.

Testing: Perform DDoS attack, Check Resource (i.e. Memory, cache) Monitor of Raspberry Pi and Check Network bandwidth of Raspberry Pi and Prepare test report.

Following are some screenshots of the implementation of proposed work.

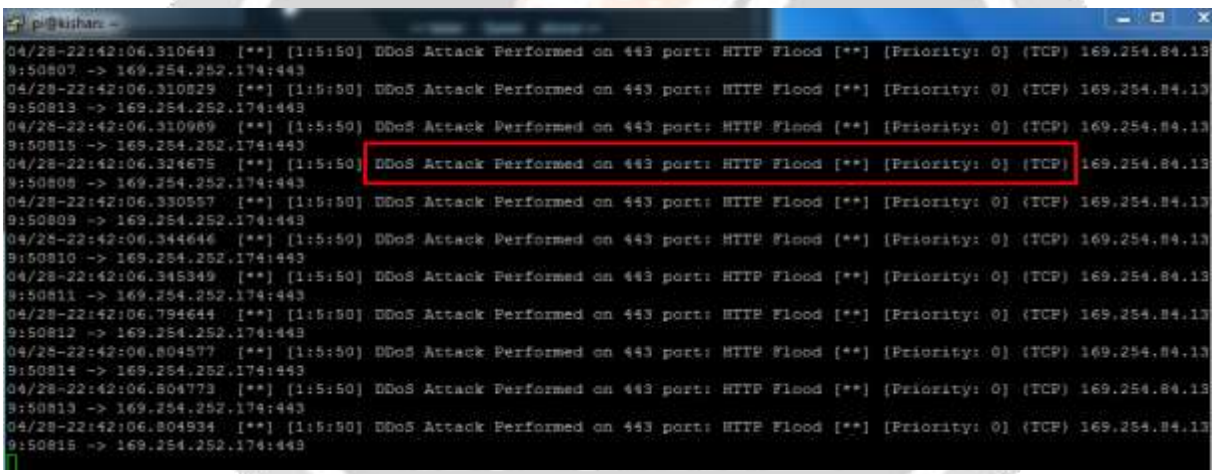

Fig.6: Http flood attack detected

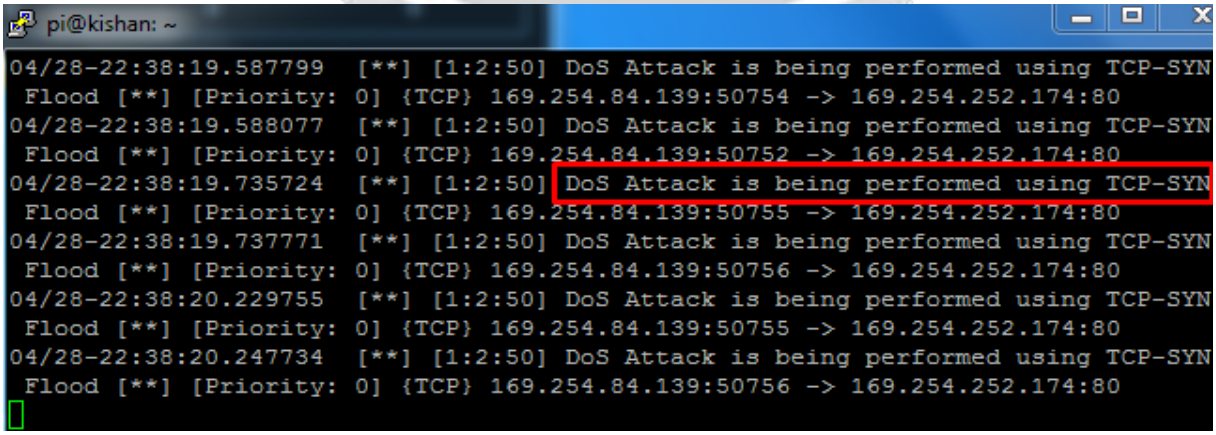

Fig.7: TCP-SYN attack detected

Fig.8: Mitigation of DDoS attack

5. RESULT AND ANALYSIS

The series of attack on the IoT server is performed here. The different types of DDoS attack are successfully detected as well as mitigated by the proposed system solution. All the testing results are enlisted below. Testing of the proposed system based on manually test. All the attacks are performed 20 times. As shown in below graph, Detection and Mitigation of SYN flood attack is 100%, TCP flood attack 85%, UDP flood attack 100%, HTTP flood attack 95% and ICMP flood attack 100%. After analysis of testing results, overall efficiency of the proposed work is 96%.

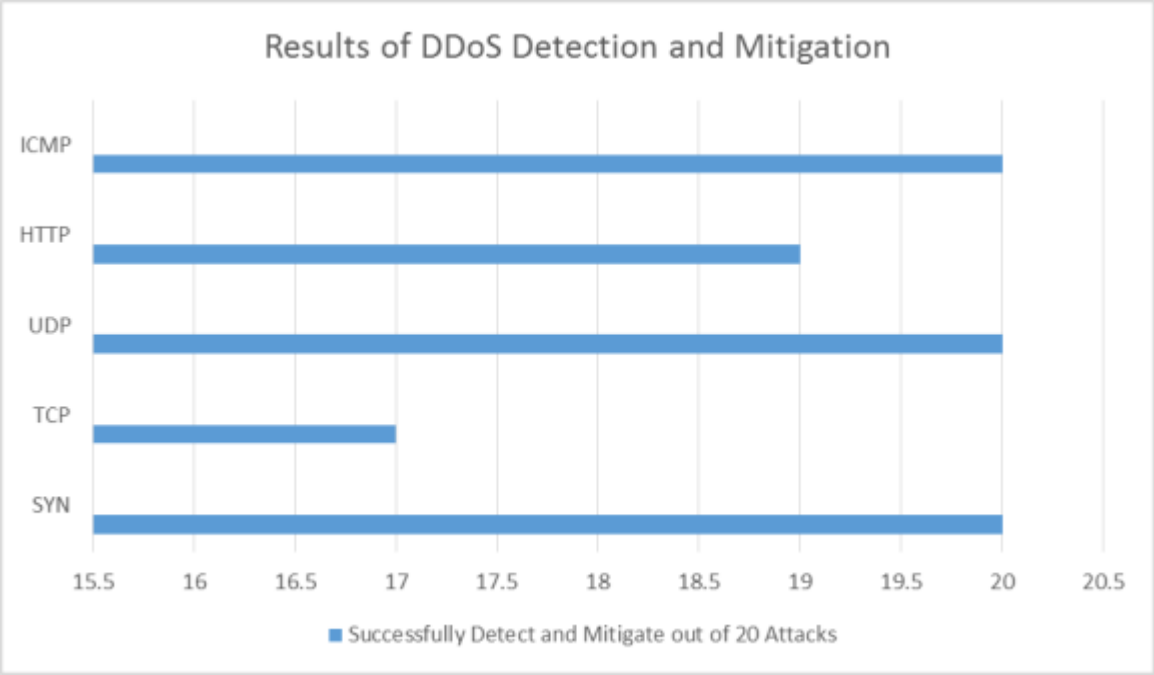

Chart.1: Result and Analysis

6. CONCLUSIONS

With emergence of IoT technology there is a requirement to secure the IoT environment from the DDoS attack. Finding out the DDoS attack and mitigate those attacks are the most challenging task. The proposed system detects and mitigate the DDoS attack using rule based approach and implemented in Raspberry Pi. The proposed system precisely detects and mitigates the DDoS attack in IoT environment. This thesis gives the detailed idea about IoT Environment, DDoS attack, Detection and Mitigation techniques of the DDoS attack.

7. REFERENCES

[1] M. Ahmed and H. Kim, "DDoS Attack Mitigation in Internet of Things Using Software Defined Networking", *2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService)*, 2017.

[2] K. Singh and T. De, "DDOS Attack Detection and Mitigation Technique Based on Http Count and Verification Using CAPTCHA", *2015 International Conference on Computational Intelligence and Networks*, 2015.

[3] G. Ramadhan, Y. Kurniawan and Chang-Soo Kim, "Design of TCP SYN Flood DDoS attack detection using artificial immune systems", *2016 6th International Conference on System Engineering and Technology (ICSET)*, 2016.

[4] T. Kawamura, M. Fukushi, Y. Hirano, Y. Fujita and Y. Hamamoto, "An NTP-based detection module for DDoS attacks on IoT", *2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, 2017.

[5] S. Dowling, M. Schukat and H. Melvin, "A ZigBee honeypot to assess IoT cyberattack behaviour", *2017 28th Irish Signals and Systems Conference (ISSC)*, 2017.

[6] S. Misra, P. Krishna, H. Agarwal, A. Saxena and M. Obaidat, "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things", *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011.

[7] S. Khattab, C. Sangpachatanaruk, D. Mosse, R. Melhem and T. Znati, "Roaming honeypots for mitigating service-level denial-of-service attacks", *24th International Conference on Distributed Computing Systems, 2004. Proceedings*, 2004.

BIOGRAPHIES

Patel Kishan Vitthalbhai
Research Scholar at GTU PG School, Ahmedabad