iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1015

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

A Survey: Mitigation of DDoS attack on IoT Environment

Kishan Patel[1], Hardik Upadhyay[2]
[1]*GTU PG School, Research Scholar, Ahmedabad, India*
[2]*GPERI, Assistant Professor, Mehsana, India*

Abstract: ***Nowadays, there are lots of IoT devices are used in Industry, Home appliances, Automobile industry and many more places. Issues regarding security of the Internet of Things (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, Denial of Service (DoS) attack block the usage of authentic user and consume bandwidth, make network resource unavailable; if this attack is performed from different sources its call Distributed Denial of Service attack (DDoS). DDos attack is the most common attack which is used to bring down the whole network without having any loophole in the network security. Here in this paper we put concentration on DDoS. To mitigate such attack it need some techniques that can detect and prevent it from attack. In this paper we discuss different techniques of mitigating DDoS attacks on IoT.***

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

I. INDRODUCTION

A. 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.

B. 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 preprogrammed to request a particular service at same time.

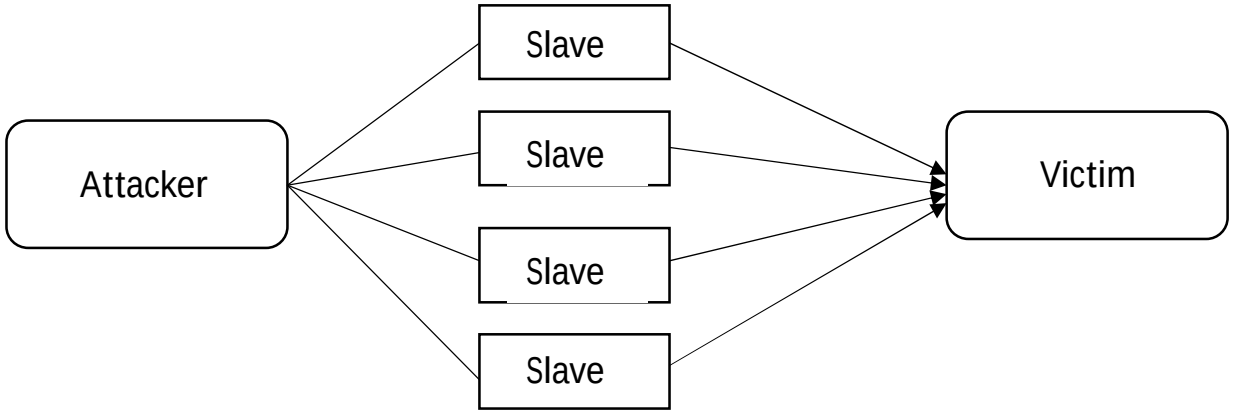


Fig.1: DDos Attack flow

©IJRASET (UGC Approved Journal): All Rights are Reserved

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.

C. Classification Of Ddos Attack

1) *UDP flood:* This attack is performed using User Datagram Protocol, a session less/connectionless network protocol. In this attack large number of UDP packets are sends to random port on remote host machine this causing victim system to check for listening port repeatedly and reply with ICMP packets. This attack makes target host inaccessible.
2) *ICMP/PING flood:* This attack perform same as UDP flood attack, an ICMP request overwhelms the target machine resources with ICMP Echo Request packets. Ping request packets are sending by attacker as fast as possible without waiting for replies. By this attack, the goal of attacker is to consume the incoming and outgoing bandwidth causing system slowdown.
3) *SYN flood:* Attack in which attacker try to exploit weakness of the TCP connection sequence(the "three-way-handshake"), wherein a SYN request is used to initiate the connection then host reply with SYN-ACK responses, and then confirmed by an ACK response by the requester. In a SYN flood attack scenario, the attacker sends multiple SYN requests, but either does not respond to target machine SYN-ACK response, or sends the SYN packet from spoofed IP address. Also in some case the target system continues to wait for ACK for every request. This attack binds resources until new connection can be made resulting in denial of service.
4) *Ping of Death:* A ping of Death ("POD") attack on any computer system involves the sending large number of malformed or malicious ping to a computer. The maximum IP packet length (including header) is 65,535 bytes. In any case, the Data Link Layer as a rule postures points of confinement to the greatest frame size - for instance 1500 bytes over an Ethernet network. For this situation, a huge IP packet is part over different IP packet (known as fragments), and the beneficiary host reassembles the IP packets into the entire packet. In POD scenario, the fragment is manipulated with malicious content, the recipient host ends up with an IP packet larger than 65,535 bytes when reassembled. This can be resulted in overflow memory buffers allocated for the packet causing denial of service for legitimate request packets.
5) *DNS amplification:* DNS amplification is a Network time protocol (NTP) DDoS attacks and SYN packet flood are the examples of Network layer attack. All above attacks takes advantages of vulnerabilities of protocols and some services of servers, etc. For example In DNS amplification attack, attacker use fake DNS queries to DNS server which replies to the victim and thus overwhelms their systems due to the too many responses.

II. RECENT DDOS MITIGATION TECHNIQUES

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

©IJRASET (UGC Approved Journal): All Rights are Reserved

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.

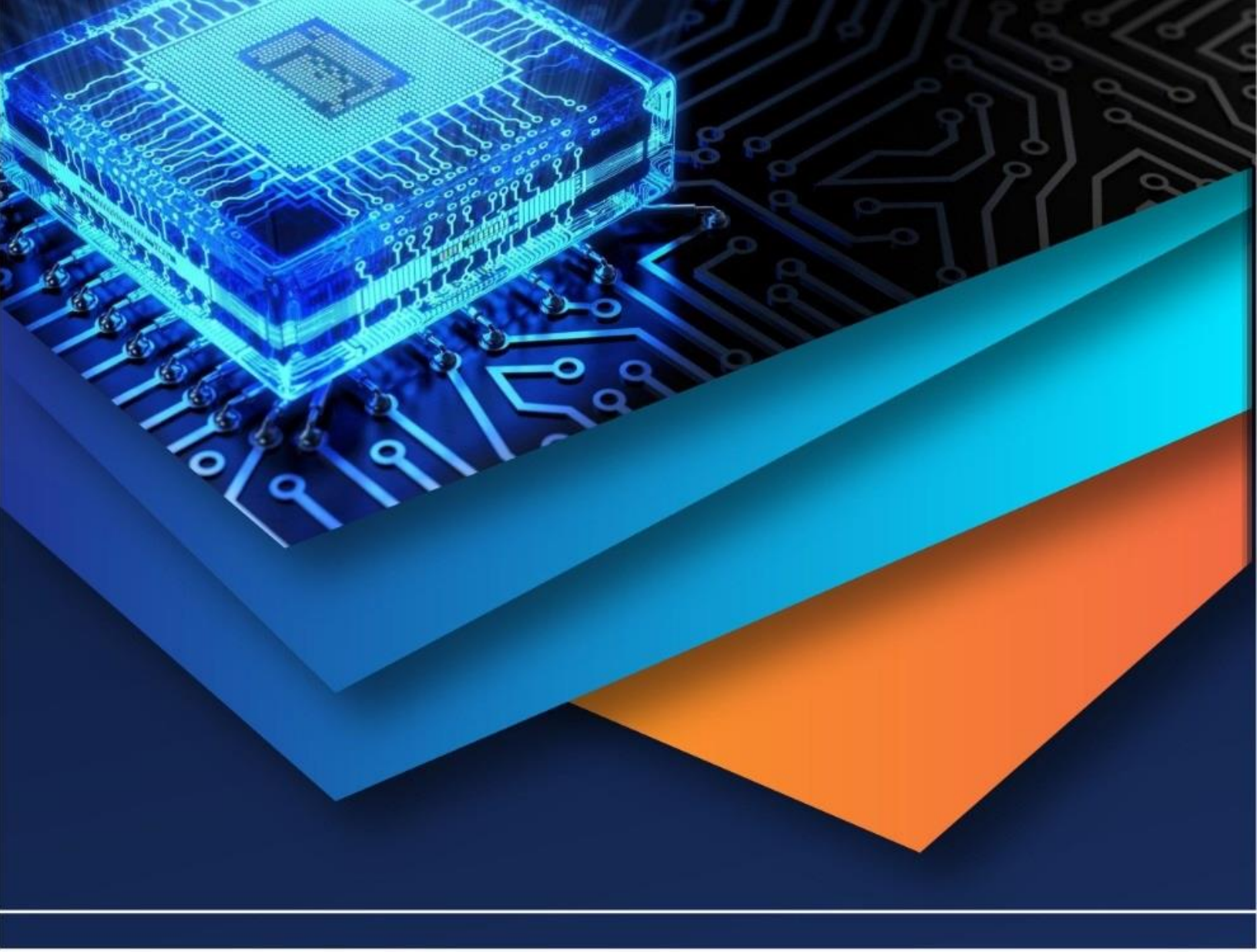
III. CONCLUSION

Internet of Things is quickly growing and turned out to be important and helpful update in coming future. With this notoriety of IoT security worried about it is assume imperative part. Keep IoT from DoS/DDoS attack isn't simple task, it faces such a significant number of difficulties because of low power, low preparing and low memory. In this paper we present some techniques for mitigating DDoS attacks which can be destroy IoT network.

REFERENCES

[1] En.wikipedia.org. (2017). Internet of things. [online] Available at: https://en.wikipedia.org/wiki/Internet_of_things [Accessed 1 Dec. 2017].
[2] Masudur Rahman and Wah Man Cheung, “A Novel Cloud Computing Security Model to Detect and Prevent DOS and DDOS Attack,” Int. J. Advanced Comput. Sci. and Applicat. (IJACSA), vol.5, no.6, pp.119-122, 2014.
[3] NidhiSrivastav and Rama Krishna Challa, “Novel Intrusion Detection System integrating Layered Framework with Neural Network,” 3rd IEEE Int. Advance Computing Conf., pp.682-689, Feb.2013.
[4] Ahmed, M.E. and Kim, H., DDoS Attack Mitigation in Internet of Things Using Software Defined Networking.
[5] Singh, K.J. and De, T., 2015, January. DDOS Attack Detection and Mitigation Technique Based On Http Count and Verification Using CAPTCHA. In Computational Intelligence and Networks (CINE), 2015 International Conference on (pp. 196-197). IEEE.
[6] Ramadhan, G., Kurniawan, Y. and Kim, C.S., 2016, October. Design of TCP SYN Flood DDoS attack detection using artificial immune systems. In System Engineering and Technology (ICSET), 2016 6th International Conference on (pp. 72-76). IEEE.
[7] Kawamura, T., Fukushi, M., Hirano, Y., Fujita, Y. and Hamamoto, Y., 2017, June. An NTP-based detection module for DDoS attacks on IoT. In Consumer Electronics-Taiwan (ICCE-TW), 2017 IEEE International Conference on (pp. 15-16). IEEE.
[8] Dowling, S., Schukat, M. and Melvin, H., 2017, June. A ZigBee honeypot to assess IoT Cyberattack behaviour. In Signals and Systems Conference (ISSC), 2017 28th Irish (pp. 1-6). IEEE.
[9] Misra, S., Krishna, P.V., Agarwal, H., Saxena, A. and Obaidat, M.S., 2011, October. A learning automata based solution for preventing distributed denial of service in Internet of things. In Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing (pp. 114-122). IEEE.
[10] Sherif M. Khattab, ChatreeSangpachatanaruk, Daniel Moss´e, Rami Melhem and TaiebZnati “Roaming Honeypots for Mitigating Service level Denial-of-Service Attacks” in 24th International Conference on Distributed Computing Systems, Mar. 2004, pp. 328–337.
[11] Theodor Richardson “Preventing Attacks on Back-End Servers using Masquerading/Honeypots” in Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Jun. 2006, pp. 381–388.
[12] Techopedia.com. (2017). What is Honeypot? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/10278/honeypot [Accessed 05 Dec. 2017].
[13] Jelic, F. (2017). Analysis: Record DDoS Attacks by Mirai – IoT Botnet. [online] Deep Dot Web. Available at: https://www.deepdotweb.com/2016/11/06/analysis-record-DDoS-attacks-mirai-iot-botnet/ [Accessed 10 Nov. 2017].
[14] KeyCDN Support. (2017). DDoS Attack – KeyCDN Support. [online] Available at: https://www.keycdn.com/support/DDoS-attack/ [Accessed 20 Oct. 2017].
[15] Enisa.europa.eu. (2017). Major DDoS Attacks Involving IoT Devices — ENISA. [online] Available at: https://www.enisa.europa.eu/publications/info-notes/major-DDoS-attacks-involving-iot-devices [Accessed 25 Nov. 2017].
[16] Tripwire, I. (2017). The 5 Most Significant DDoS Attacks of 2016. [online] The State of Security. Available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-DDoS-attacks-2016/ [Accessed 15 Dec. 2017].
[17]

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)