Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

A SURVEY OF MITIGATION TECHNIQUES OF DENIAL-OF-SERVICE ATTACK ON INTERNET OF THINGS

Ruchi Chauhan, Electronics and Telecommunication, Atharva College of Engineering, Mumbai, India ruchichauhan@atharvacoe.ac.in
Shikha Malik, Electronics and Telecommunication, Atharva College of Engineering, Mumbai, India shikhamalik@atharvacoe.ac.in

***Abstract*—** IoT is a new technology which is finding its presence in many domains which includes industry, home appliances, and automobile sector etc. One of the foremost aims of IoT devices is to capture data and exchange the same seamlessly into information network. Vulnerability of IoT network to many attacks leads to major concern of security in IoT devices. One such attack is Denial of service attack which blocks the authentic user from accessing network and makes network resources unavailable for an uncertain period of time. To extenuate Dos, attack some technique is required which can sense the attack and prevent it from damaging the network. This paper aims to review different methods and techniques and suggest the use of AI, ML and trust- based mechanism to attenuate DoS attack on IoT.

Keywords— Internet of Things, Security, DoS attack, Mitigation

I. INTRODUCTION

Internet of Things (IoT) also known as Internet of Everything as it is a system of sensors embed with hardware and software enabling items to trade information with the administrator, maker, specialist co-op, as well as other associated gadgets [1]. In general IoT can be defined as the network of sensors integrated with other electronic devices which have capabilities to sense, process and communicate data with the computer to take decisions artificially with minimum human interventions. More than 100 billion devices are estimated to be connected by IoT by the year 2025 and it will be 11 trillion dollar industry. Concurrent to this rise, IoT industry is also facing many obstacles in terms of hacking of IoT devices, infiltration issues along with intrusion in privacy [2].

DOS attack causes damage to the network availability and is among one of the most severe attacks on IoT network [3]. DOS attack aims at making services or resources unavailable by flooding it with traffic from a number of systems or BOT in short span. DOS attack affects every layer in IoT stack and has critical impact on confidentiality, integrity and availability of a data as well as resources [4].

II. IOT ARCHITECTURE AND SECURITY ISSUES

A. IoT Architecture

IoT communications structure [5] as shown in below figure has four different stages consisting of sensors and smart items, clever devices and gateways, and back-end data centers and services.

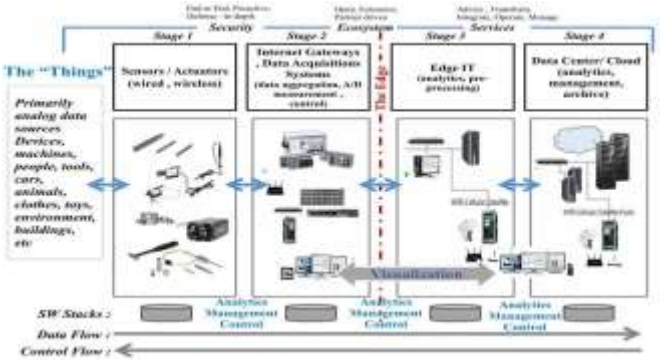

Fig 1. IoT Architecture [5]

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

Stage 1. Sensors / Actuators: Sensing devices gathers data from the environment or things under measurement and convert it into some measurable data [5]. Actuators can also arbitrate to change the physical conditions that produce the data. An actuator can shut off a power supply, adjust valve of air flow, or move a robotic arm in an aggregation process.

Stage 2. The Internet Gateway: The sensors and actuators gather data is in the analog form. Further processing of the data requires it to be converted into digital streams [5]. The Internet gateway which can be border router (BR) routes these digitized data over Wi-Fi, wired LANs, or the Internet to next stage for further processing.

Stage 3. Edge IT: Digitized and aggregated data require further processing which is done by edge IT [5] systems before sending it to next stage.
Stage 4. Cloud and data center: At this stage a more in-depth processing of IoT data is carried out using robust systemswhich examine, control and firmly store the data.

A. *IoT Protocol Stack*

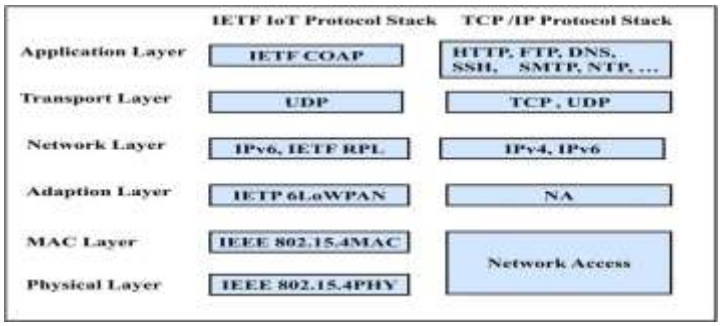

Fig.2 Protocol Stack of TCP/IP network Vs IoT Network [7]

The traditional TCP/IP network stack is heavy (requires large memory and computational power). In case of IoT devices there are various protocols available at application layer like CoAP, MQTT etc. The transport layer is occupied with Datagram Transport Layer Security which is a alternate variation of TLS made for IoT devices [7]. As IoT devices uses IPv6 addressing scheme the protocol used at the network layer is RPL Protocol based on IPv6.

B. *IoT Security Issues*

IoT devices form a network of billions of devices continuously exchanging information. The security of the network is impacted by poorly connected devices which pose a challenge to the entire Internet. This challenge is further augmented by lack of common standard and architecture for the IoT security [6]. Following are some of the main challenges in IoT

1. *Privacy Issues:* A lot of IoT nodes collect very critical and private information like name, mobile number, account number etc. This hypersensitive information is transmitted across over the net without any significant guard which is a big threat as intruder may get access to it.

2. *Inadequate authentication/authorization:* Huge number of IoT devices (web cameras, Television, door locks etc) present in the market are found not to have secure passcodes. Usually, a lot of devices uses identical passcodes which leads to an intruder getting access to all easily.

3. *Absence of transport encryption/standard:* IoT framework lacks a proper structure and there is no encryption of data in network transmission of IoT devices. Standard transport encryption systems are requirement of present time to preserve privacy of information.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

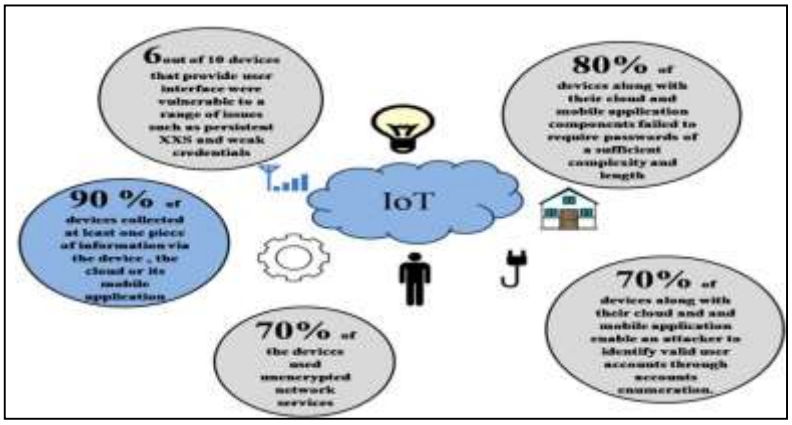

Fig. 3. Security Issues in IoT devices [6]

4. *Web interface vulnerability:* Attackers use this security gap to capture access in various network applications. Periodic cross-site design, endangered fragile sessions and substandard administration are big security problems .

5. *Software and firmware vulnerability:* Due to lack of encryption structure, 60% or more IoT devices have vulnerable software and hardware. Remote access to these devices by malicious software and firmware can happen through system updates.
Another key issue in IoT is privacy conservation of IoT devices and users which results in non-optimum utilization ofmultiple devices in IoT network.

III. DENIAL OF SERVICE (DOS) ATTACK

DOS attack prevents the legitimate user to access the information, services or resources they expect to use. This attack is done by the third-party invader aiming to make system or network unavailable to the actual user [8]. The attack is carried out by flooding the victim machine with traffic or by dispatching some information which leads to crash. DOS attack impacts all layers of IoT network. The below explained are two types of DOS attacks.

A. *Flooding attack*
B. *Crash Attack*

A. Types of Flooding Attack

1. *UDP Flood Attack*: A connectionless protocol User Datagram Protocol (UDP) is used to launch the attack. The host machine random port receives huge number of UDP packets causing the legitimate user system to continuously check forlistening port and revert with ICMP packets making target host unavailable

2. *ICMP Flood Attack:* In Internet Control Message Protocol (ICMP) flood DOS attack, the attacker delivers spoofed packets to all the targeted system in the network to take benefit of any flawed system device.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

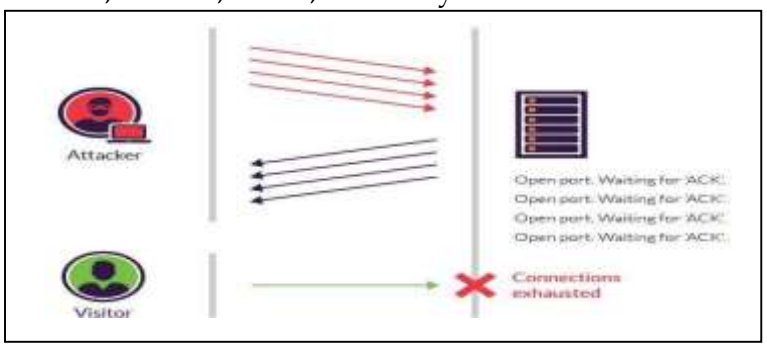

Fig 4. SYN Flood Attack [19]

3. *SYN Flood Attack:* It uses exposed and liable Transmission Control Protocol (TCP) connection three-way handshake. In this attack the intruder sends repeatedly SYN packets using Spoofed IP address to the victim machine which responds to it by sending SYN ACK to the attacker machine [19]. The intruder does not revert with SYN ACK packet and if spoofed IP address is used it never receives any acknowledge packet. But till the connection time out occur the victim machine has to keep the port open to listen and before the time out attacker send another packet as a result the service becomes unavailable.

B. Crash Attack are classified as:

1. *Smurf Attack:* System can be completely shut down in this type of attack. Intruder generates large number of ICMPpackets with victims IP address and by using an IP Broadcast Address such packets can be broadcast in the network [21].On receiving ICMP packets the network machines responds by sending response to target machine. If the devices in the network are huge and each machine is responding to target machine than the victim's system is crashed and it becomes almost impossible to work.
2. *Ping of death (POD) attack*: In this type of attack scenario a packet bigger than the maximum IP packet length is send to the victim system [20]. 65,535 bytes is the utmost length of IP packet. In usual case a large packet is broken downinto fragments and is reassembled to make the entire IP packet. But in case of POD the fragments are injected with malicious content as a result the host reassembles a packet larger than the maximum length which causes buffer overflow leading to Denial-of Service attack for authentic packet request.

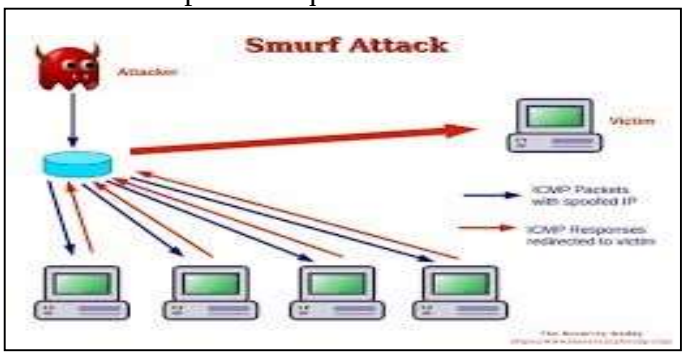

Fig. 5 Smurf Attack [21]

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

Fig. 6 Ping of Death Attack [20]

IV. A REVIEW OF MITIGATION TECHNIQUES FOR DOS ATTACK

In this section, we address different mitigation technique used for DOS attack in IoT network.

The authors of [9] studied the consequences of DOS attack on Wireless and Wired LAN interface. Using Raspberry Pi Open WRT and Open v Switch authors evaluated that with the rise in DOS attack from Wired to Wired interface ping time also rises and 70% packet loss was observed with DOS on wireless interface to wired interface and conclude that severity of DOS on wired to wireless interface is most on IoT gateway.

Authors of [12] have created three test bed using data logging hardware to analyze the aftermath of DOS attack on IoT sensor node and found that DOS attack impact the availability of data of sensor node considerably and suggested the use of some IDS for prevention of DOS attack.

Santosh kumar et .al [10] proposed Topology Management Method (TMM) to mitigate DOS attack constructed on nodes behavioral examination. They also implemented Fine grained Detection Algorithm to find the deviation of node behavior from normal behavior and emphasis that deauthentication attack has low false positive rate of detection and detection of DOS attack is better than Wired IDS

The authors of [11] proposed an IDS forth with IPS based on machine learning for detecting DOS attacks which not only detects but also prevents victim from DOS attack. More than 96% accuracy and detection rate was achieved using above method.

Authors of [13] analyzed the DOS effect for UDP based DTLS and mitigated DOS attack by using HMAC –MD5 encryption and cookie interchange in DTLS handshake procedure and observed that 9% energy saving were achieved using enhanced DTLS.

Gronza et.al [14] proposed a formal method of automatic detecting DOS attack. Proposed method was able to mitigate resource exhaustion attack and allowed in depth valid protocol.

The authors of [15] propose mitigation of DOS attack in MQTT publish and subscribe architecture by CoP (control (lane) in which trusted nodes implies security policies to the gateway which in turn collects feedback from nodes and selects messages as per security policy.

Rahman et al [16] uses watermarking-based technology which used traced back method for examining the trust of incoming packets and permit only trusted nodes to communicate in the network.

Authors of [17] uses Advanced Encryption System (AES)to mitigate the security issues like CIA for IoT. Authors made alteration in the standard AES by doubling the encryption of AES and addition of white box. This white Box was used in place of S box (Substitute-Byte) in the traditional AES. The advantage of using white box is to decompose AES cipher into round functions. By doubling the AES process, it becomes difficult for the attacker to interrupt the network and is able to mitigate DOS attack.

In paper [18] authors used J48 machine learning technique to create an IDS which can detect Dos attack. 100% accuracy was achieved in detecting DOS attack with system ability to capture 75% of packets.

The authors of [19] modified and put into use three network-based mitigation strategies for TCP SYN authentication as a possible countermeasure, their modifications make it possible to deflect even more sophisticated SYN floods that are capable of evading the majority of conventional methods. This results in a delayed initial connection attempt, but there is no significant additional latency in any subsequent SYN segments (<; 0.2ms).
Based on an analysis of energy consumption, the paper [20] proposes a novel strategy for detecting cyberattacks in the Internet of Things infrastructure. The method also makes use of an analysis of the IoT software's actions in order to increase the accuracy with which cyberattacks can be detected. With a detection rate of up to 99.95 percent, the proposed method makes it possible to detect attacks like DoS/DDoS with high efficiency

TABLE I. MITIGATION TECHNIQUES FOR DOS ATTACK

Author and **Year**	**Attacks**	**Technique**	**Conclusion**
Maslina Daud et.al 2018 [9]	SYN flood attack using hping3 program	Testbed created using OpenWRT and OVS	Ping time rises with rise in DOS attack and up to 70% packet loss rate
Yungee Lee, Wangkwang Lee and Kyungback Kim, 2017 [12]	Application layer DOS	Testbed setup for IoT sensor node and attacker	Lifespan of IoT nodes reduces with DOS attack
S. Santhosh Kumar ; K. Kulothungan , 2017 [10]	Flooding attack	Topology management method and fine-grained detection algorithm	Detection Accuracy of 80% and 84% precision
Y Maleh, A Ezzati, M Belaissaoui , 2016 [13]	IP spoofing attack DOS Attack	Encryption by HMAC-MDS	Enhanced DTLS with 9% energy saving
Masudur Rahman and Wah Man, 2014 [16]	SYN Flood Attack	Hardware based watermarking and filtering method	Consume less resource and provides an additional defense layer against DOS
Bogdan-Cosmin Chifor, Ion Bica, Victor-Valeriu Patrici, 2017 [15]	DOS attack on MQTT protocol	MQTT based CoP	Address DOS attack and suggested use of distributed architecture
Yasir Javed, Adnan Shahid Khan, Abdul Qahar, Johari Abdullah, 2019	Application layer DOS	Modified Advanced Encryption System	Addresses DOS attack but proposed method needs to be evaluated in real time

[17]			
Mayank Agarwal ; Santosh Biswas ; Sukumar Nandi, 2015 [11]	De- authentication DOS	Machine learning based IDS	Accuracy and detection exceed 96%
Bakhtiar, F. A., Pramukantoro, E. S., & Nihri, H. (2019) [18]	SYN Flood and UDP Flood	J48 machine learning based IDS	100% detection accuracy and 75% packet capture
Patrik Goldschmidt; Jan Kučera (2021) [19]	SYN Flood Attack	Modified versions of three network-based mitigation techniques for TCP SYN authentication	Delayed initial connection attempt, but no further latency in any subsequent SYN segments
Kira Bobrovnikova; Oleg Savenko; Sergii Lysenko; Ivan Hurman (2022) [20]	DOS /DDoS Attack	Energy Consumption Analysis	High Efficiency with 99.95 % detection

v. CONCLUSION

Denial of Service attack on IoT devices has a severe impact on availability of services and resources leading to compromise of confidentiality, integrity and availability. DOS attack is broadly classified into two categories flooding attack and crash attack. This paper emphasizes on various mitigation techniques used to address Dos attack in IoT. However, many methods are still at proof-of-concept level. The focus of research community should be on Artificial intelligence, machine learning and trust-based mechanism which should be able to quarantine IoT network from all types of DOS attack.

REFERENCES

[1] Rwan Mahmood, Tasneem Yousuf, Fadi Aloul,Imran Zualkernan, “Internet of Things(IoT) Security: Current status, Challenges and Prospective Measures”, The 10th International conference for Technology and Secured Transactions(ICITST-2015).

[2] Q.Jing, A.V.Vasilakos ,J. Wan , J. Lu and D. Qiu,”Security of the Internet of things: Prespectives and Challenges”, Wireless networks, vol. 20, no. 8 ,pp. 2481-2501,2014

[3] Qifeng Chen , Haoming Chen , Yanpu Cai , Yanqi Zhang , Xin Huang ,”Denial of Service Attack on IoT System”,2018 9th International Conference on Information Technology in Medicine and Education (ITME), 27 December 2018

[4] A. Rghiout, A. Khannous, and M. Bouhorma, “Denial-of-service attacks on 6lowpan-RPL networks: Issues and practical solutions,” Journal of Advanced Computer Science & Technology, vol. 3, no. 2, pp. 143–153, 2014..

[5] Mohammed Ali Jabraeil, Jamali,Bahareh Bahrami, Aash Heidari, Parisa Allahverdizadeh, Farhad Norouzi,” IoT Architecture”, eai/springer Innovations in communication and computing book series, June 2019

[6] S. Raza, L. Wallgren, and T. Voigt, “Real time intrusion detection in the internet of things,” Ad-Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013

[7] Pallavi Sethi and Smruti R. Sarangi ,”Internet of Things: Architectures, Protocols, and Applications”,,Journal of Electrical and Computer Engineering , 2017,Article ID 9324035

[8] K. Munivara Prasad, A. Rama Mohan Reddy & K.Venugopal Rao,”DoS and DDoS Attacks:

Defense, Detection and Traceback Mechanisms -A Survey ,Global Journal of Computer Science and Technology: E Network, Web & Security ,Volume 14 ,Issue 7 Version 1.0 2014 (USA) ISSN: 0975-4172 & Print ISSN: 0975-4350

[9] Maslina Daud ; Rajah Rasiah ; Mary George ; David Asirvatham ; Abdul Fuad Abdul Rahman ; Azni Ab Halim,"Denial of Service (DOS): Impact on Sensors", 2018 4th International Conference on Information Management (ICIM) Oxford, UK

[10] S. Santhosh Kumar ; K. Kulothungan,"An Anomaly Behavior based Detection and Prevention of DoS Attack in IoT Environment",2017 Ninth International Conference on Advanced Computing (ICoAC)

[11] Mayank Agarwal ; Santosh Biswas ; Sukumar Nandi," Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach",2015 IEEE International Conference on Systems, Man, and Cybernetics

[12] Yungee Lee, Wangkwang Lee and Kyungback Kim," Assessing the Impact of DoS Attacks on Iot Gateway", Advanced Multimedia and Ubiquitiousb Enginering, Springer 2017

[13] Y Maleh, A Ezzati, M Belaissaoui ," DoS Attacks Analysis and Improvement in DTLS Protocol for Internet of Things", ACM International Conference on Big Data and Advanced Wireless Technologies, At Blagoevgrad, Bulgaria November, 2016

[14] Bogdan Groza Politehnica, Marius Minea," Formal Modelling and Automatic Detection of Resource Exhaustion Attacks" ASIACCS 11, March 22–24, 2011, Hong Kong, Chin

[15] Bogdan-Cosmin Chifor, Ion Bica, Victor-Valeriu Patrici," Mitigating DoS attacks in publish-subscribe IoT networks" International Conference – 9th Edition Electronics, Computers and Artificial Intelligence 29 June -01 July, 2017, Targoviste, Romania

[16] Masudur Rahman and Wah Man, "A Novel Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 6, 2014

[17] Yasir Javed, Adnan Shahid Khan, Abdul Qahar, Johari Abdullah," Preventing DoS Attacks in IoT Using AES",Journal of Telecommunication,
Electronic and Computer Engineering, e-ISSN: 2289-8131 Vol. 9 No. 3-11

[18] Bakhtiar, F. A., Pramukantoro, E. S., & Nihri, H., "A Lightweight IDS Based on J48 Algorithm for Detecting DoS Attacks on IoT Middleware", 2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech). doi:10.1109/lifetech.2019.8884057

[19] Patrik Goldschmidt; Jan Kučera , " A Defense against SYN Flood DoS attack using Network Based Mitigation Techniques", 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), 17-21 May 2021. France

[20] Kira Bobrovnikova; Oleg Savenko; Sergii Lysenko; Ivan Hurman, "IoT Cyberattack Detection Approach Based on Energy Consumption Analysis",2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), 09-11 December 2022, Greece

[21] imperva.com.'TCP SYN Flood',[Online].Available https://www.imperva.com/learn/application-security/synflood/.[Accessed: 2- March -2020]

[22] pluralsight.com,'ping of death and other DoS network attacks',2009. [Online].Available:https://www.pluralsight.com/.[Accessed:2- March -2020]

[23] thesecuritybuddy.com,'what-is-smurf-attack',2017. [Online]. Available: https://www.thesecuritybuddy.com/dos-ddosprevention/what-is-smurf- attack/. [Accessed: 2-March-2020]