As per UGC guidelines *an electronic bar code is provided to seure your paper*

International Journal for Modern Trends in Science and Technology, 9(SI01):118-125, 2023
Copyright © 2023International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST09SI0123
Available online at: http://www.ijmtst.com/vol9si01.html

An In-Depth Analysis of Distributed Denial-of-Service Attacks, Their Varieties, and the Countermeasures Employed in the IoT Network

S.Ramya[1], G. Jyostna[1], A. Saipujitha[1], Y.V.K. Durga Bhavani[1,2]

[1]Department of Information Technology, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada.
[2]Research Scholar, Department of Computer Science and Engineering, Basaveshwar Engineering College(A), Bagalkot, Karnataka.

To Cite this Article
S.Ramya, G. Jyostna, A. Saipujitha and Y.V.K. Durga Bhavani. An In-Depth Analysis of Distributed Denial-of-Service Attacks, Their Varieties, and the Countermeasures Employed in the IoT Network. International Journal for Modern Trends in Science and Technology 2023, 9(SI01), pp.118-125. https://doi.org/10.46501/IJMTST09SI0123

Article Info
Received: 26 January 2023; Accepted: 22 February 2023; Published: 26 February 2023

ABSTRACT

In today's internet world, the Internet of Things (IoT) has its own importance. Along with some advantages, it also has some drawbacks. Through this review paper, we will talk about Distributed Denial of Service Attack (DDoS) in major flows of IoT like how it works, different types and mitigation methods.

KEYWORDS: DDoS, IoT, RFID, WSN, SYN

1.INTRODUCTION

The term "Internet of Things" (IoT) was introduced by Ashton in 1999. The primary function of IoT is to interconnect the daily usable devices to easily do the computational task in an accurate and managed way. IoT works with sensing devices, the internet, electronics devices, etc., to make the devices smart, just like Artificial Intelligence (AI). IoT makes devices smart because it connects devices to communicate, process, and analyze the data from algorithm/computer language, then send it and show the output. The interaction between IoT objects can be human to human, machine to machine and human to machine.

IoT is presently finding its application in many fields; some of them are described as follows:

- *Agriculture Sector:* The IoT in the agriculture sector is used to check the fertility of the soil, to give information about the climate and suitable seasons for crops, use of insecticides and fertilizers, and irrigation purposes to help the farmer so a farmer can earn more profit.
- *Health Sector:* IoT makes decisions using patient data in the health sector, i.e. taking medicine and checking the body's health through smart devices. IoT control city traffic, distributes water, manages sewage and other wastes, calculates pollution level, manages light on roads and streets, parking, etc.
- *Transport Sector:* In transport, IoT uses vehicle tracking, truck/trailer weight measurement, vehicle maintenance/services, insurance etc.

- *Home Sector:* In homes, IoT sensors are embedded in the smoke detectors, home appliances, light bulbs, windows, doors, locks etc.

A layer diagram of IoT architecture with supporting technologies is as shown in figure 1 below. IoT architecture consists of 5 layers: perception, network, processing, application, and business.

Perception Layer: The first layer works like the human eye, nose, and ears. It is also called the sensor layer because it senses surrounding environments through its sensors and sends the data to electronic devices. It works between the physical world and digital signaling, i.e. it converts the data from digital to physical and vice-versa.

Network layer:It operates between the perception layer and processing layer. It collects the data from the perception layer. It transfers data to the processing layer through 3G, 4G, Universal Mobile Telecommunication System (UTMS), Near Field Communication (NFC), Radio Frequency Identification (RFID), Wireless Fidelity (Wi-Fi) etc. Its main work is to provide communication between these two layers. These layers use protocols like Data Distribution Service (DDS), Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), Message Queuing telemetry Transport (MQTT) etc., to share data across devices.

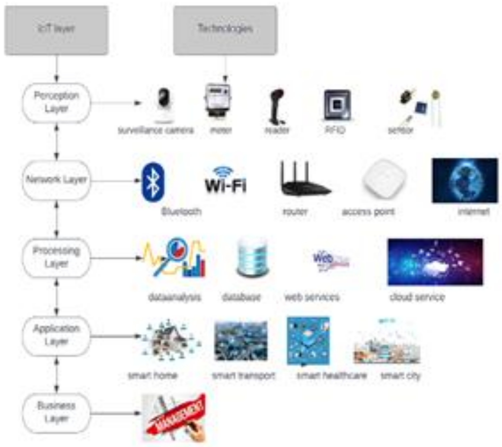

Fig.1: IoT layers and their technologies

Processing layer:It interacts between the network layer and the application layer. It has additional features like memory (storage), computation, processing, analysis, action-taking ability, etc. it is the main working layer of IoT architecture.

Application layer:It interfaces between devices and networks. The main protocols used on this layer are Hypertext Transfer Protocol (HTTP), MQTT, DDS, Extensible Messaging and Presence Protocol (XMPP) etc.

Business layer: This layered work is problem-solving, created in the network or application layer. It is concerned with the processing, transformation, rules and regulation, policies and data management and validity etc.

Distributed Denial of Service attack is a cybercrime in which attackers steal information from the server with the help of internet traffic. Due to this, the server slows down, and the victim cannot access information via the internet. Different attacks target IoT layers, such as volume-based, protocol, and application-layer attacks. In volume-based attack aims to control bandwidth e.g., Domain Name System (DNS). In protocol, attack consumes the web server capacity such as firewalls e.g., SYN attack. Protocol attack occurs mostly in layer 3 and 4 of OSI model. Application layer attack occur in layer 7 of OSI model, targets the layer where web pages are generated in response to Hyper Text Transfer Protocol (HTTP) request.

2. LITERATURE REVIEW

In [1] and [2], authors have explained generic IoT architecture and challenges regarding different layers such as application, network, business, perception and processing layer, IoT vulnerability and its security. In [4], authors have explained IoT models like the agent handler or IRC-based models. It discussed how Wireless Sensor Network (WSN) and Radio Frequency Identification (RFID) are attacked and their countermeasure. In [5] and [9], authors have analyzed IoT' 's security challenges. They have also explained about the security design strategy to use IoT efficiently and increase the interaction between humans and IoT.

Author [7] [11] discussed the different defense techniques using offensive load equalization and throttling methods. Their proposed solution used the assumption that the communication nodes are present in a specific geographical location and proposed an algorithm for checking the DDoS attack by comparing a server's packet buffer utilization rate.

Author [8] talks about the mitigation methods or the solution of attacks in IoT, such as prevention using filtration. The filtration technique includes ingress filtering, router-based packet filtering etc. other techniques are the secure overlay technique, honeypots; the load balancing technique helps to prevent the attack.

Author [14] discusses the future aspects of DDoS attacks in IoT. The growth of IoT devices and the rapid deployment of 5G capabilities worldwide will be a lethal mix. Furthermore, the increasing digitalization of enterprises has taken a significant jump due to the COVID-19 epidemic. Hackers employing cloud technology are already being carried out very efficiently DDoS attacks. Author [15] talks about the detection method of DDoS attacks using techniques such as signature detection, multi tops, ICMP traceback Message, capability-based response and anomaly detection. These are the methods of detecting attacks and are also used to mitigate the attack.

The paper organization is done as follows: Section I gives a study about the IoT with layer architecture of the IoT. Section II describes literature survey of DDoS attacks, and detection techniques. Section III gives information about DDoS attack and its architecture And Section IV gives information about types of DDoS attacks. Section Vdescribes the detection and prevention schemes of DDoS attacks. Section VI describes about future of DDoS attack. And Finally, section VII concludes the paper.

3. DDOS ATTACK

"Distributed Denial of Service" (DDoS) attacks occur at the network layer, due to which it slows down the system with fake traffic. First of all, DDoS attacks will check the limits of the network by sending spikes of counterfeit packets. It uses bot-net; bot-net consists of connected IoT devices, websites and systems. To mitigate a DDoS attack, define the "traffic pattern". It separates the human traffic from the incoming traffic by using the signature technique, IP address, etc. The following process is filtering, such as firewall and anti-virus.

DDoS attacks are a type of "Denial of Service" (DoS) assault that is less complex and occasionally extra attractive. The main goal of these assaults is to render a victim facility inoperable, resulting in a denial of service for common handlers. One explanation is the overflow of information measures on the directed server, which provides certain facilities or sources.

Most attacks are directed at internet services or services provided by various groups and businesses, such as news services, banking, government administrative offices, and businesses. The key difference between DoS and DDoS assaults is the assault link. A single network (i.e. a PC or a server) is used in a DoS attack. The attacker is straight testing the setup node.

The DDoS assault, on the other hand, employs several setup nodes and multiple setup properties. These infected net nodes are known as zombies or bot-nets, and the perpetrator manages them roundabout. It results in the assault being made up of many requests (typically hundreds or thousands) coming from all over the globe. With the victimization of Trojan horses or other malware operating on compromised network nodes of targets, the perpetrator often establishes the essential infrastructure of bot-nets.

The message behavior of a DDoS assault might resemble conventional traffic at times. As a result, detecting and defending against this type of assault is more complicated than detecting and defending against a simpler DoS attack. DDoS assaults concentrate on a single target node in a brief period and with a certain level of assaults strength. In comparison to DoS assaults, the strength is substantially higher.

Bot-net arrangement is now being developed to launch an assault at a later date. That is why it is critical to guarantee the highest level of safety and security for any net arrangement. The DDoS assault has the potential to reason not only financial losses due to the denial of online services to users and reduces the trustworthiness of businesses and their services.

A. DOS ATTACK

Denial of Service (DOS) attacks occur when attackers create traffic on the victim's website due to traffic websites going slow or shut down for some time. It harms the victim's time and money. Any other website user who wants to use it could not access it due to traffic created by an attacker. Attackers send a considerable number of packets simultaneously, due to which the system/website cannot handle the huge address. This attack does not harm or lose the data/information and other victims' assets. It makes the service inaccessible.

Bandwidth consumption fault occurs due to the DoS attack, which fills the site limit so no other request can go through. It affects as long as DoS is maintained. Resource starvation faults have little impact on other sources, and it does not affect as long as bandwidth consumption fault. "Domain name service" (DNS) fault impacts on multi websites.

DoS attack has two methods: flooding and crashing attacks. Under flooding attacks, there are some sub-attacks like buffer overflow attacks, "Internet Control Message Protocol" (ICMP) attacks, and Synchronization (SYN) attacks. Buffer overflow attacks send huge packets to network addresses that the programmers have built the system to handle. ICMP attack amplifies the traffic. SYN attacks connect the server used by the victim.

There are many reasons for DoS attacks. Financial: in which attackers want money. Political reason: The attacker should be a part of a demonstration against the government and want to shut down the government site at government action. Personal reason: the attacker has a grievance against the company and wants revenge.

B. DDoS attack architecture

DDoS architecture is based on the Agent-handler and Internet Relay Chat (IRC) models.

1) *Agent-handler model*: first of all attacker makes a handler to control the system. This handler works independently or remotely. After that attacker sends all necessary information like algorithms and commands to the handler to be ready for attack. Then attacker controls the handler and sends a massive amount of packets to the victim system. In this attack, the attacker generally used spoofed "Internet Protocol" (IP) addresses to hide his own identity or location. The attacked system may not even know that its system has been hacked and are involved in DDoS attacks. Agents are frequently told to speak with one or more handlers, depending on how the attacker configures the DDoS assault network. Typically, attackers will aim to install the consumer computer code on a hacked router or network server that processes large amounts of traffic. This makes it more difficult to distinguish between communications between the consumer and the handler and between the handler and the agents. The phrases "handler" and "agents" are frequently substituted with "master" and "daemons" in descriptions of DDoS tools. An agent handler model architecture describes below in figure 2:

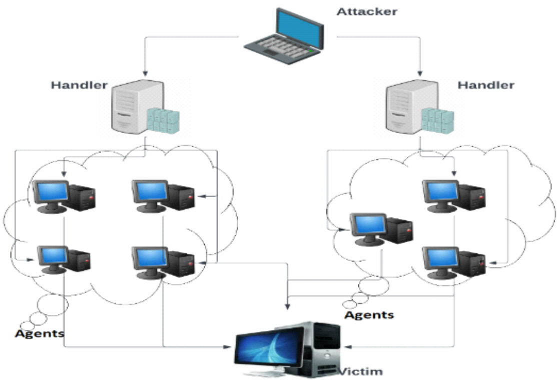

Fig. 2: IoT Architecture

2) *IRC based model:*

The IRC-based DDoS assault is similar to the Agent-Handler approach. Instead of a consumer application installed on a network server, the consumer is connected to the agents over an IRC line. The use of "legal" IRC ports for transmitting orders to the agents is an additional benefit of the associate IRC channel to the aggressor. Furthermore, IRC systems hide their precision and make it simple. Another benefit is that the aggressor does not need to keep track of the agents because he can browse to the IRC server and view a list of all accessible agents. Once the agent is up and running, the agent software system installed within the IRC network typically talks with the IRC channel and alerts the aggressor.

C. Phases of DDOS Attacks

The DDoS attack mainly includes three phases, i.e. Phase 1: Recruiting, Phase 2: Propagation and Phase 3: Attack.

1) *Recruiting:* In this phase, the attacker creates a handler. The attacker used a self-propagated algorithm to control the handler. There are many scanning used in recruiting attacks to describe below:

a) *Random scanning:* It uses infected IP addresses and creates huge traffic and many fraud probes.

b) *Hit-list scanning:* It helps to decrease the infected system. In this scanning, the attacker makes a list of the vulnerable system and scans

c) *Permutation scanning*: It helps to stop multi-probe at the same IP address. In this case, an already infected system via hit-list scanning, the new infection starts at the permutation scanning. If an already infected system is found during the scanning, it does not infect this system again.

d) *Topological scanning*: It is an alternative to hit-list scanning. It does not need the attacker list because it can produce its list in peers.

2) *Propagation:* It propagates the attack code containing information of the victim system, time, and duration of the attack. There are some phases under propagation described below:

a) *Central source propagation*: in this case, the attack code propagates from the central server.

b) *Back chaining propagation:* attacker interact between the attack and victim machine.

c) *Autonomous propagation*: as the name suggests, it automatically sends the attack to the victim system without the attacker.

Last phase attacks. A huge technique was used to execute the attack

4. TYPES OF DDOS ATTACK

To better understand DDoS, it is important to understand its classification. Attackers exploit different layers such as network, transport, and application layer. Different types of DDoS attacks i.e., flooding, and logical attacks describe below in figure 3:

1) *Flooding attack:* This sor-snippt of DDoS assault is designed to excess server sources such as information measurement, memory, or computer hardware by utilizing huge amounts of packets. This approach leads genuine users to experience a DoS. Flooding packets are often achieved by exploiting communication protocol flaws (TCP, UDP, ICMP, FTP, SIP or HTTP). The most significant flooding assaults are listed here.

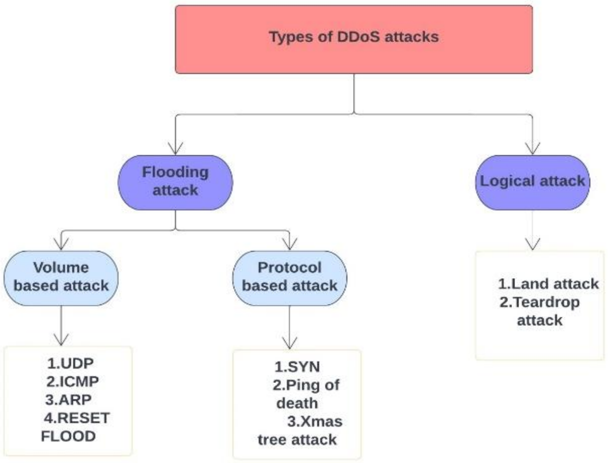

Fig 3: Different Types of DDoS attack

a) *UDP flood attack*: in this attack attacker send a considerable amount of packets from the handler. The attacker also spoofed IP addresses and sent huge packets until every bandwidth consumed by the system and system stopped its normal function.

b) *ICMP flood attack:* The ICMP flood assault is also known as the Smurf or Ping flood attack. This exploit drives a massive sum of ICMP ECHO applications to some susceptible network's multicast scientific discipline address. The request's supply scientific discipline address is the same as the victim's scientific discipline address. All nodes respond to the victim with an ICMP ECHO reply address during this victim network. The deluge of ICMP ECHO answers causes the target system to burden. The assault has been accomplished on the TCP/IP network layer.

c) *The "Address Resolution Protocol" (ARP) flood attack:*The ARP flood attack uses faked ARP queries to overwhelm the intended victim. It results in the victim's compute and memory sources being depleted. These attack types are acceptable for usage in a native network. There will be periodic causation of faked ARP answers (e.g. from a network gateway) carrying the aggressor's science address in a different method. This is known as the ARP Spoofing Assault, and it achieves the renowned MITM (Man in the Middle) attack after all circulation is directed across the aggressor.

d) *The Reset (RST) flood attack*: The Reorganize flood assault employs TCP packets with an RST flag and faked supply scientific discipline addresses. If a huge sum of these packets is transmitted to the target's ports, it is likely that more or less recent communication will be rearranged.

e) *HTTP flood attack:* attackers exploit HTTP by using HTTP GET and HTTP POST techniques. It is similar to an SYN attack that makes a TCP connection with the botnet IP address.

f) *SYN attack:* attacker makes a connection through TCP between the two parties. The attacker creates three-way handshaking. First, the packet sends from client to server, and the server acknowledges the client by sending an SYN+ACK (acknowledgement) packet. After this client again sent the ACK packet to the server to finalize the handshake. The attacker exploits the flood server memory and creates many incomplete connections. The attacker uses a spoof IP address; the server sends the SYN+ACP to the attacker, but the IP address does not exist, so it does not receive the ACP packets.

g) *The "Christmas" (Xmas) tree attack:*In the Xmas tree attack, a wrongdoer produces Christmas tree packets, which have fixed flags like FIN, URG, and PSH inside the communications protocol header. It is tough to process these flags. In the event of many incoming packets, this fact produces associate overload on the directed node.

h) *Ping of death attack*: The attacker makes the maximum data packet size due to which the victim system crashes. The system on the victim node attempts to tack together the packet. This might result in a buffer run-off fault and a system crash.

i) *The unapproachable host flood:*The Reset flood is similar to the unapproachable host flood attack. With a faked source information processing address, the offender sends an ICMP report stating "Host inaccessible" to arbitrary ports on the victim's computer. There's a potential that the current session may be cancelled.

2) *Logical attacks*:

Logical assaults exploit flaws in programs or software on a victim's device. In contrast to flooding assaults, these attacks employ tiny volumes of messages. The goal is to render the victim gadget non-functional. The most well-known varieties are listed below.

a) *Land attack:* attacker attach the IP address with packets, and when the victim receives packets, it automatically responds to the IP address and makes an infinite loop between these two parties.

b) *Teardrop attack*: The Teardrop attack occurs when a miscreant transmits a transfer packet with improper balance settings. The main aim is to make the system resources unavailable.

5. DETECTION AND PREVENTION OF DDOS ATTACK

A. Detection Of DDOS Attack

We can detect these devices before attackers attack them. This detection informs the admin and the victim, reducing its impact. This ensures the network safety of the victim.

- *Signature detection:*

It detects the normal traffic and the attacker signature separated. This differentiates the already existing attack and unnoticed attack. The detection methods based on signatures provided good data of DDoS assaults. The characteristic of this detection was monitored by a team and used in safety and security on systems like firewalls and routers and noticed the DDoS assault. As a result, current detection systems do not recognize recent and undiscovered assaults.

- *MULTOPS:*

Multi-level tree for online packet statistics. Its main work is to find out the bandwidth flood attack. It checks the packets' rate and whether incoming and outgoing packets/traffic are similar or not.

- *ICMP trace-back Message:*

It occurs in a router, and this help to find out what was the source. But this technique generates extra traffic. This method needs additional processing within the router and extra space.

- *Capability based response*:

The attacker does not mind about the misbehavior or packets and sends them. The capability technique solves such misbehaving packets.

- *Anomaly detection:*

It can handle the new kind of signature detection assault. Flood assaults, for example, will be noticed if the number of TCP-SYN, UDP, or ICMP packets increases. These detection algorithms attempt to detect anomalies in typical network circulation.

- *Other methods:*

There is a huge technique to find the attack. In the application layer, the browser's behavior can check the attack, but if the attacker uses the proxy, he cannot find it. Attack source identification, DWARD method, probabilistic packet marking, deterministic packet marking etc., are used to detect the DDoS attack.

B. Prevention against DDoS attacks

A DDoS defense instrument, in general, consists of four fundamental components. Initially, it appears to be a DDoS bar. First of all, it detects the source of the attack and breaks those attack packets into different parts. After that, it stops the attacks. This also ensures that there is as little damage as possible, for which it acts as the backup line. This work makes its structure very complex. It needs a secure network such as firewalls, network infrastructure (router), sensors, etc.

Management and elastic management are generally required together. It is also vital to plan for emergency conditions in a DDoS assault. The following sections in fig 4 outline the fundamental methods and approaches that can help to mitigate DDoS threats.

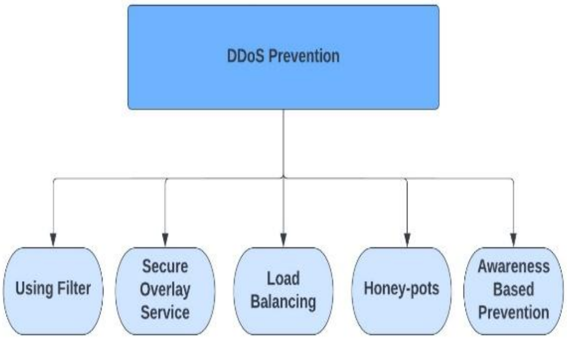

Fig 4: Different Methods to Prevent DDoS Attack

1) Prevention using filter

This filtering is used in the router and specifies that only valid users can access the system. There are many techniques used under filtering described below:

- *Ingress/egress filtering* this filter stops the spoofed IP used by the attacker. It allows only the pre-defined IP range prefix. But the main drawback is that it provides valid IP with botnet used by the attacker.
- *Martian address filtering and source address validation:*it applies to the router and ensures that it cannot forward any invalid IP address or destination address. The invalid IP may be special IP, unreserved IP, unallocated range IP etc.
- *Router-based packet filtering:*it is similar to ingress filtering, but it uses the service of the main router and connects every link with it. It ensures that every link access only limited traffic.

There are many other techniques that we can use to avoid the attack, such as source-address validity enforcement protocol, hop-count filtering, history-based filtering, path identifier, packet score, etc.

2) Secure overlay technique:

It protects the sub-node of the network and is applied on the top of the IP address. This network connects the protected network and outside network. In this technique, we use the firewall in the overlay network to ensure that only trusted IPs can enter the protected network. But this is only useful for private networks.

3) Honeypots:

Honey-net is a less secure network. It can be easily attacked. Using honey-net can mislead the attacker so that the attacker will think that they attacked the correct system, but we can protect the main system with this. It acts as a kind of shield.

4) Load balancing:

This is another method to mitigate the DDoS attack. The main work of this technique is to maintain the balance so that there will be no system overloaded.

5) Prevention based on awareness:

IoT systems are less secure, but there are many DDoS attacks that we can deal with the general awareness. Like changing IP address, disabling exceptional service, applying security patches, etc.

6. FUTURE OF DDOS ATTACKS

Recent trends indicate that DDoS assaults will grow more common, huge, and successful. The growth of IoT devices and the rapid deployment of 5G capabilities worldwide will be a lethal mix. Furthermore, the increasing digitalization of enterprises has taken a significant jump due to the COVID-19 epidemic. As a result, businesses of all sizes have significant assets online, making them ideal targets.

The current situation does not look good when it comes to DDoS defense. Hackers employing cloud technology are already being carried out very efficiently DDoS attacks. Businesses must swiftly adapt and begin using comparable solutions in their security stacks. However, hackers always appear to be one step ahead regarding methods, tools, and strategies.

There were approximately 4.83 million DDoS assaults in only the first half of 2021. This figure is a significant rise above the already concerning figures for 2020. From March to July, the early lockdown months saw the most activity. We can only anticipate that the tendency will continue in 2022 and beyond.

7. CONCLUSION

This paper presents the basic information of DDoS attacks, their types, how we can detect them, their security, and ways to avoid them. There has recently been a plethora of safety solutions available to combat DDoS assaults—a good security combination of firewall, network infrastructure, sensor etc., in DDoS attacks. DDoS assaults create a networked system or service inaccessible to legitimate users. These assaults are annoyances at best and maybe quite devastating if a critical system is a principal victim. Its main effect is seen in time loss and economic loss. DDoS assaults should be mitigated by developing solutions

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] IEEE Standards Association, IoT Architecture - Internet of Things (IoT) Architecture, https://standards.ieee.org/develop/wg/IoT_Architecture.html (Accessed: 02/2017) (2016).

[2] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q Deng and S. Ray et al., "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, 2017

[3] Aris, S. Oktug and T. Voigt, "Security of Internet of Things for a Reliable Internet of Service", Autonomous Control for a Reliable Internet of Service, pp. 337 – 370, 2018

[4] U. Javaid, A. Siang, M. Aman and B. Sikdar, "Mitigating IoT Device based DDoS Attacks using Blockchain", CryBlock'18, pp. 71-76, Germany, 2018

[5] K. Bhardwaj, J. Miranda and A. Gavrilovska, "Towards IoT – DDoS Prevention Using Edge Computing",Phys. Rev. 47, 777-780, 2018

[6] H. Sedjelmaci and M. Feham, "Novel, Hybrid Intrusion Detection System for Clustered Wireless Sensor Network," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011, vol. 3, no. 4, pp. 1–14, 2011.

[7] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Manuel Mazzara. 2017. AntibIoTic: Protecting IoT Devices Against DDoS Attacks. CoRR abs/1708.05050 (2017).

[8] Fabrice J. Ryba, Matthew Orlinski, Matthias Wählisch, Christian Rossow, and Thomas C. Schmidt. 2015. Amplification and DRDoS Attack Defense - A Survey and New Perspectives. CoRR abs/1505.07892 (2015)

[9] H. Suo, J. Wan, C. Zou, and J. Liu. 2012. Security in the Internet of Things: A Review. In 2012 International Conference on Computer Science and Electronics Engineering, Vol. 3. 648–651, 2012.

[10] Amiri, I. S. and Soltanian, M. R. K.. "Theoretical and Experimental Methods for Defending Against DDoS Attacks". Syngress(2015).

[11] A. Srivastava, B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, "A recent survey on DDoS attacks and defense mechanisms," in Advances in Parallel Distributed Computing. Springer, pp. 570–580,2011.

[12] S. Jin and D. S. Yeung, "A covariance analysis model for DDoS attack detection," in Communications, 2004 IEEE International Conference on, vol. 4. IEEE, 2004, pp. 1882–1886.

[13] M. C. M. Patel and A. P. V. H. Borisagar, "Survey on taxonomy of DDoS attacks with impact and mitigation techniques," in International Journal of Engineering Research and Technology, vol. 1, no. 9 (November-2012). ESRSA Publications, 2012.

[14] R. Arun and S. Selvakumar, "Distributed denial-ofservice (DDoS) threat in collaborative environment - A survey on DDoS attack tools and traceback mechanisms," in Proceedings of IEEE International Conference on Advance Computing, pp. 1275–1280, 2009.

[15] H. Kaur, S. Behal, and K. Kumar, "Characterization and comparison of distributed denial of service attack tools," in Proceedings of IEEE International Conference on Green Computing and Internet of Things (ICGCIoT'15), pp. 1139–1145, 2015.

[16] D. Peraković, M. Periša and I. Cvitić, "Analysis of the IoT Impact on Volume of DDoS Attacks", PosTel 2015, Belgrade, December, 2015

[17] N. Tripachi and B. Mehtre, "Dos and DDoS Attacks: Impact, Analysis and Countermeasures", National Conference on Advances in Computing, Networking and Security, 2013.