Volume 65, Issue 5, 2021
Journal of Scientific Research
of
The Banaras Hindu University

Taxonomy of DDoS attacks and their defense mechanisms in IoT

Nimisha Pandey*[1], and Pramod Kumar Mishra[2],

*[1]Department of Computer Science, Institute of Science, Banaras Hindu University, Varanasi, U.P. 221005 India, nimisha.pandey17@bhu.ac.in

[2]Department of Computer Science, Institute of Science, Banaras Hindu University, Varanasi, U.P. 221005 India, mishra@bhu.ac.in

***Abstract*—IoT promised great involvement in the industry as per the earlier predictions of many researchers but IoT did not pierce various industries to that extent. IoT has many security issues which make IoT systems very vulnerable to the attackers. Recently, there have been many DDoS attacks using IoT devices opening the possibility of DDoS attacks on the IoT systems vastly. DDoS attacks have not been able to affect the lives of people directly. But with IoT systems as their target, attackers can cause serious impact on the lives of people. So, the DDoS vulnerability of IoT systems need to be addressed so that proper solutions can be created for IoT.**

***Index Terms*—DDoS, IoT, IoT security**

I. Introduction

IoT is basically providing a more connected world by using machine to machine communication connecting devices and thereby making the interaction between the human and machine achieve more results. Advancement in electronics, computing power and introduction of ipv6 addressing scheme has made it possible to connect electronic items to the Internet. There has been some ground-breaking research in this area since past years. This has led to various industries leveraging this opportunity to create innovative devices and providing lucrative services to the user. Various researchers and enthusiasts have also designed different innovative systems that use this technology in overcoming societal challenges. Since IoT is vital component of all these new products and ideas coming in the market, it is also vulnerable to security threats. Security threats should be evaded before monetizing these products because in the long run it will be important that the technology is away from security threats. It is also noted that the security risk can never be completely evaded but the current security issues need to be solved and research must be done on upcoming issues.

A denial of service attack is when an attacker sends huge traffic to a victim in order to exhaust the victim's resources so that it denies service to a legitimate user. A DoS attack carried out by a huge number of devices is known as distributed denial of service attack. Distributed Denial of Service(DDoS) attacks are occurring frequently and have become an issue for security professionals. Recently, Amazon Web Services(AWS) has been invaded by a three days long DDoS attack[1]. Mirai botnet, unveiled in 2016, uses IoT devices to launch massive DDoS attacks on big enterprises. IoT devices are lucrative for attackers because they have limited security standards due to their resource-constrained nature. IoT devices can be used to launch the attacks on other victims preserving the anonymity of the attacker. IoT devices are mostly used to ease the hassle of repetitive tasks for the user. Therefore, a lot of people can be troubled by denying their services to the users. Important services like fire and theft detection, home care of older adults and patients with memory disorders are realized through IoT. These systems can be crippled to undergo fatal disasters using these attacks. These factors make IoT devices vulnerable to attackers.

There have been other advancements like development of botnets and release of codes of their associated malwares on the Internet. It has contributed to the frequent occurrences of such attacks. Additionally, easily accessible tools are available on the Internet that facilitate carrying out of the attack as discussed later in the paper. These attacks have caused huge financial losses to the enterprises. In the remaining paper, section II deals with the related work and section IV deals with the classification of DDoS attacks. Section V discusses the tools that have been used to carry out DDoS attacks and the botnets that are also used in launching the DDoS attacks. Section VI categorizes the defense mechanisms of DDoS attacks. Section VII discusses the various network simulators that can be used to study DDoS attacks in IoT. Section VIII discusses the datasets available in this area that have been studied in the past wile the section IX concludes the paper.

II. Related Work

Kaur et al. discussed distributed denial of service(DDoS) attacks, and their classification [11]. DDoS attacks are divided

DOI: 10.37398/JSR.2021.650523

into flooding attacks and vulnerability attacks. Flooding attacks can be further divided into Direct DDoS attacks and indirect DDoS attacks. On the basis of target layers, flooding attacks can be divided into Network/Transport level DDoS attacks and application-level DDoS attacks. Some examples of flooding attacks are SYN flood, ICMP Ping, smurf attack, Get request, UDP Flood, DNS amplification attack, frag flooding. Bhattacharyya and Kalita have classified the types of DDoS defence systems on the basis of different criteria, namely, approach, nature of control, defense infrastructure, and the defence location [15].

Sharafaldin et al.[14] have presented a taxonomy of DDoS attacks and majorly divided them into reflection-based attacks and exploitation-based attacks. They further divided these two types into TCP based attacks, UDP-based attacks and TCP/UDP based attacks. In this way, they have classified 13 attacks into a total of five fine-grained classes. The attacks are MSSQL, SSDP, DNS, LDAP, NETBIOS, SNMP, PORTMAP, CharGen, NTP, TFTP, SYN Flood, UDP Flood, UDP-Lag.

Mirkovic and Reiher[16] have proposed detailed taxonomies for DDoS attacks and its defense mechanisms. They have classified the attacks in eight categories, namely, degree of automation, exploited vulnerability, source address validity, attack rate dynamics, persistence of agent set, possibility of characterization, victim type, and impact on the victim. They have classified the defense mechanisms by activity level, cooperation degree, deployment location, and attack response strategy.

Asosheh and Ramezani[17] have also introduced taxonomies for DDoS attacks and its detection. They have classified the DDoS attacks on the basis of eight parameters. They are architecture, degree of automation, impact, exploited vulnerability, attack rate dynamics, propagation strategy, scanning strategy, and packet contents. They have broadly classified the defense mechanism into prevention-based and detection-based mechanisms. Further, they classify them into target network, intermediate network and source network. They have also proposed a framework to detect different DDoS attacks, classify them and then invoke corresponding defense mechanism automatically.

Another pair of taxonomies is proposed by Tariq et al.[18] for DDoS attack and its defense. They have categorized the DDoS attacks on the basis of level of computerization, attack network, oppressed vulnerabilities, influence, and attack intensity dynamics. They have classified the defense mechanisms on four basis, namely submissive defense mechanism, active defense mechanism categorization by action and defense deployment position. Figure 1 shows the features used by the previous papers. Four circles show the four papers which have been referenced appropriately earlier. Figure 2 also shows the features used by different authors in defining the taxonomy of defense mechanisms of DDoS attacks. While making the venn diagrams, the fact has been considered that different terms are used by different researchers for the same entities. Further, Table I shows some key points from different surveys on IoT security.

III. Motivation

A. DDoS Attacks in the recent past

There have been many instances of DDoS attacks in the past. These attacks have increased tremendously in volume and frequency with passing years. As they have attacked many small and big companies, they have created troubles for the security professionals also. These attackers have also tried to induce terror in the society by launching attacks due to political reasons too. Some of the attacks have been shown in table II.

B. Societal impact of DDoS attacks in IoT

IoT devices portray a calm and pervasive technology that aims to change the definition of comfort and ease in the user's lifestyle. As these devices aim to bring revolutionary changes in the user's lifestyle, malfunctioning of such systems will also tremendously impact the users. Figure 3 shows the possible threats from DDoS attacks on various IoT applications. Smart homes represent the collection of technologies that come together to enhance user comfort and facilitate overall connectivity of the home devices thereby increasing accessibility and usability of devices. There are several subsystems in a smart home like comfort monitoring, smart lighting, connectivity of devices etc. All these subsystems can fail in case of a DDoS attack on the home network. It will impact the user.

For a quick disaster management, IoT is being used in disaster management scenarios and military deployments. Smart disaster management is used to monitor the remote disaster-prone areas and perform disaster management before human help can reach. An attack on such system can stop the rescue missions and can be fatal for the victims in such disasters. Smart healthcare deals with the patient care and patient monitoring. There are many devices which can track the patient's data, store it in the cloud and the doctor can monitor the report created from the patient's data from distance. Some devices are used to automatically notify the hospitals when the patient's reports are alarming. Old adults and dementia patients are also being monitored from home through this technology. Although, when these monitoring systems are attacked, they cannot serve the legitimate requests and would not send the patient's data to the doctor. The alarming systems would not send the alarms to the caring units.

Smart environment monitoring uses sensors to monitor the condition of air, the water level of rivers, etc. so that alarms can be set in case of an emergency. Malicious devices carrying DDoS attack on such systems can stop the monitoring and alarm system. In smart logistics, logistics companies can communicate and many inventory services are

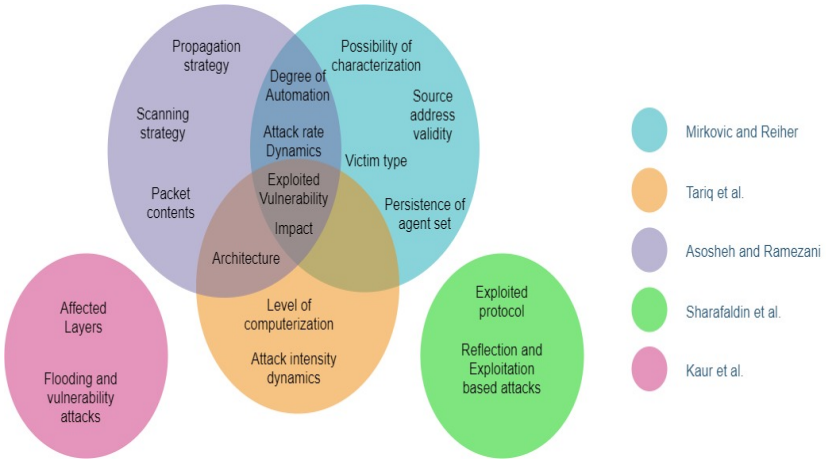

Fig. 1. Venn diagram of features taken in previous DDoS taxonomies

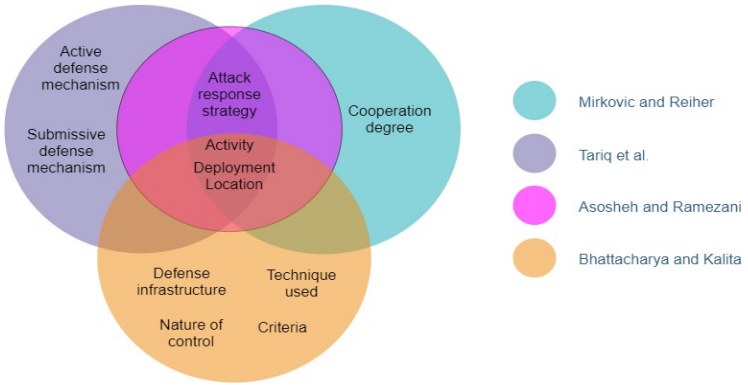

Fig. 2. Venn diagram of features taken in previous defense taxonomies

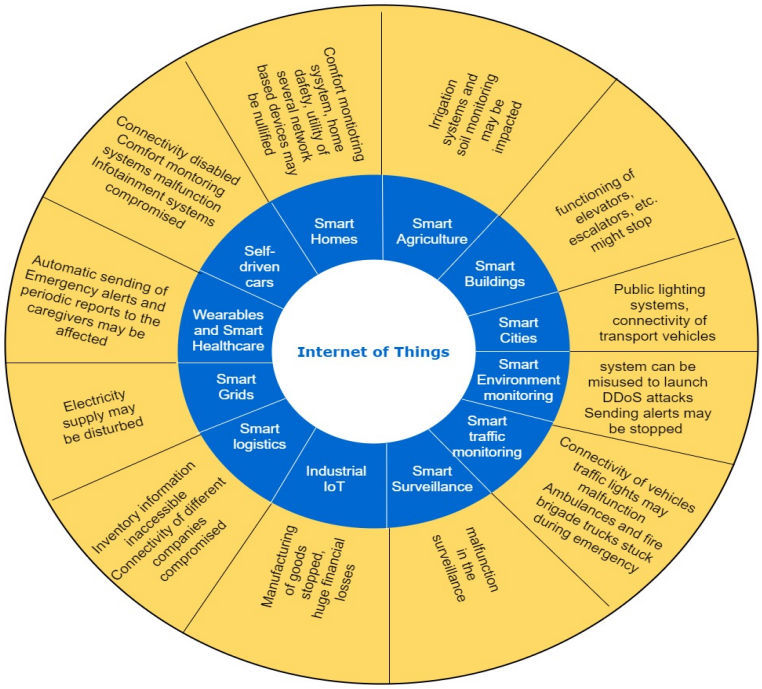

Fig. 3. Applications of IoT vulnerable to DoS attack

TABLE I
SURVEYS FOR IOT SECURITY

Papers	Key Points
[2]	• the different attacks possible on different applications of IoT. • different threats that might come from the hardware, network, and applications in an IoT system.
[3]	• proposed a five-layer architecture for IoT. • The five layers include physical layer, network layer, transport layer, application layer, and data and cloud services layer
[4]	• the current trends in the core requirements of IoT security like authentication, encryption, trust • a detailed layer-wise architecture of IoT security and a thorough list of simulators useful in IoT security research.
[5]	• proposed a tetrahedron model for IoT • discussed its implementation in smart manufacturing
[6]	• categorization of attacks into 3 categories, low-level, intermediate level and high-level attacks • the use of blockchains in IoT security
[7]	• discussed the security requirements and challenges of various IoT applications • reviewed the solutions for confidentiality, privacy, and availability in IoT • the role of blockchains and SDN in IoT security
[8]	• presented the vulnerability of different IoT applications and IoT layers towards different attacks • the use of blockchains in IoT security
[9]	• grouped the IoT applications, vulnerabilities, and security requirements in the context of three layers in IoT namely, application layer, network layer, and edge layer • the attacks and their solutions in each layer.
[10]	• a taxonomy of vulnerability in IoT security which includes layers, attacks against the CIA triad of IoT, mitigation techniques, and security assessment paradigms
[11]	• the detailed classification on DDoS attacks and thorough review on their detection approaches
[12]	• layer-wise possible attacks in IoT • trust management in IoT • issues and solutions of IoT protocols
[13]	• presented a review of machine learning solutions for IoT security. • categorized among network layers the machine learning approaches for IoT security.

brought together. DDoS attack on any such software might be a hindrance in the transportation of goods. Smart grids are vulnerable to DDoS attacks too. Califano et al. [44] have discussed the vulnerability of smart grids from DDoS attacks. Self-driven cars are equipped with the variety of sensors and actuators. These cars were targeted at reducing the number of road accidents but they can also become a problem. A DDoS attack can carry out a massive attack on such vehicles.

Smart cities have been a target of DDoS attacks. Multiple subsystems like traffic monitoring, smart environment monitoring etc. form the smart cities. If a DDoS attack occurs, then subsystems of smart cities are vulnerable to attacks too [45] [46]. Industrial IoT utilizes smart manufacturing of goods. A DDoS attack on such a manufacturing facility may stop the essential network-based services required during the manufacturing process. This may incur heavy losses.

IV. TAXONOMY OF DDOS ATTACKS IN IOT

To devise the appropriate defense mechanism, classification of the large array of DDoS attacks must be done for IoT. We discuss the attacks and sort them on the basis of six features. We classify them on the basis of attack rate, secondary victim, target IoT layers, architecture, impact, and exploited vulnerability. Figure 4 describes the taxonomy of DDoS attacks in IoT.

A. Classification on the basis of attack rate

DDoS attacks on the basis on attack rates are as follows:

- Low-rate DDoS attack: In low rate DDoS attacks, the attacks packets can be sent at a pulsing rate or requests

TABLE II
DDOS ATTACKS IN THE PAST.

Time	Attack	Peak
Oct,2020	PubG Mobile encountered DDoS attack	
Feb, 2020	Amazon Web Services(AWS) was attacked for three days [29]	2.3 terabytes per second
Feb 28, 2018	Github was invaded by a DDoS attack for 20 minutes	1.35 Tbps
2017	A UDP amplification attack on Google for 6 months	2.5Tbps
Feb, 2017	An application layer DDoS attack was carried out on a US College[30] for 54 hours	.
Oct, 2016	Mirai attacked DNS server, Dyn and Internet service stopped there for a day [23]	620Gbps
Sept 20, 2016	the blog of Brian Krebs, a cybersecurity expert was attacked by Mirai botnet [29].	620 Gbps
2014	Occupy Central servers based in Hong Kong were attacked by five botnets	500Gbps.
December, 2015	BBC was attacked with DDoS traffic	600 Gbps
March, 2013	Spamhaus, an organization that leads the spam filtering market was attacked	300 Gbps.
March 12, 2012	Botnet named Brobot assaulted six banks of America generating packets [29]	60Gbps

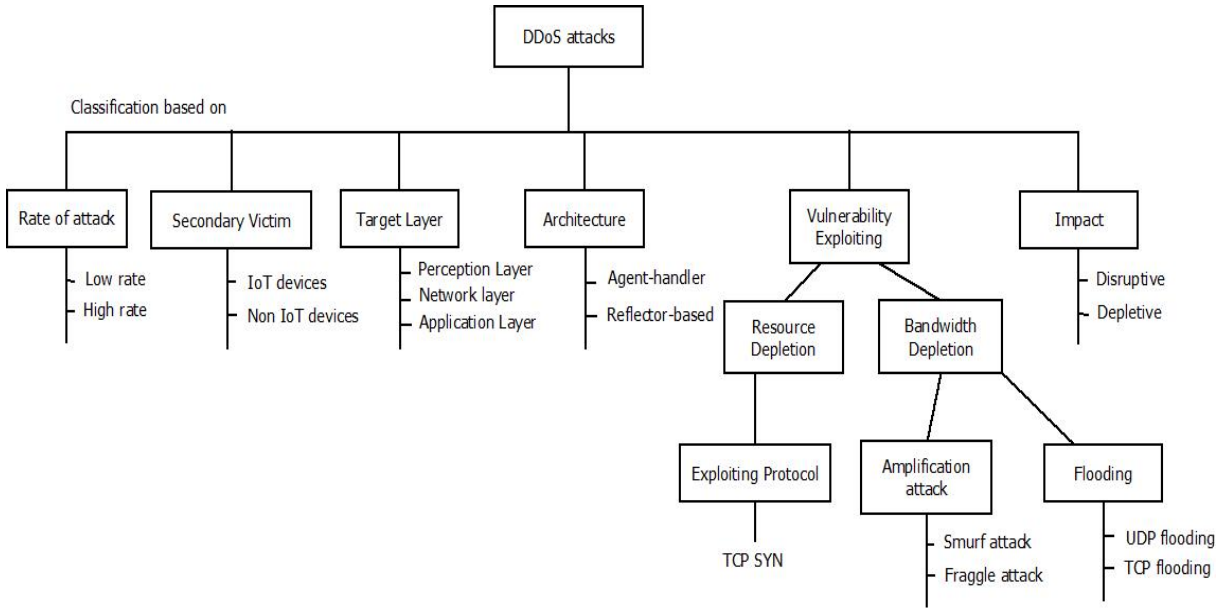

Fig. 4. Taxonomy of DDoS attacks in IoT

for highly computational services can be made at low rate [15]. Sometimes, they would not exhaust the resources of the network but they can compromise the victim's available bandwidth. Detection of this kind of attack is difficult because they look similar to normal traffic. Macia et al. studied the low rate attacks and proposed a mathematical model on them [19] [20]. Xiang et al. studied low rate attacks and presented a detection algorithm for the same [21].

- High-rate DDoS attack: The attack packets come at a very high rate and therefore, this attack traffic is similar to the flash events. Sachdeva et al. have studied and formulated an algorithm to differentiate between high rate DDoS attack and flash events [22].

B. Classification by secondary victim

The scenario of a DoS attack which includes an IoT device might have two possibilities:

- IoT devices as a secondary victim: IoT devices can be used to carry out DDoS attack on other target systems. One such attack was Mirai botnet which was used in October 21, 2016 for a massive DDoS attack on Dyn DNS server. Mirai botnet detected vulnerable devices in the network especially IoT devices and attacked the devices having default or predictable usernames and passwords. This attack affected many giant companies like Amazon, Netflix, Tumbler, Twitter, Spotify. The company faced three waves of DDoS attacks in a day. The volume of attack traffic was 620Gbps and millions of IP addresses were used in the attack [23]. Sam Egbo analyzed this attack and discussed the preventive measures taken by Dyn after the attack [23]. Due to these concrete reasons,

TABLE III
LAYERS AND THE DDOS ATTACKS.

Layer	Protocol	Attack
Perception Layer	6LoWPAN	Resource Exhaustion attacks
Network Layer	TCP, UDP	Flooding attack
Application Layer	CoAP	Flooding attacks, Resource exhaustion attack

security against DDoS attacks becomes a very important aspect in IoT paradigms. Lyu et al. studied the impact of reflective attacks on other networks using the IoT networks [24]. They evaluated the amplification factor for eight IoT devices and use the ports of UDP and TCP for attacks. Foremski et al.[25] have studied these attacks and proposed Autopolicy which restricts the set of IP addresses to which the IoT devices can send traffic, and bandwidth available to them.

- Non-IoT devices as the secondary victim: IoT networks can be an easy target for attackers which have ample resources and can easily bring them down.

C. Classification by target IoT layers

1) Perception layer: Perception layer deals with collection of data from the surroundings using sensors. This layer makes use of technologies like RFID, GPS, etc. This layer uses sensors to collect data and actuators to perform actions according to the data received from sensors. However, these devices come with limited processing capacity, so attackers exploit this constraint in a DoS attack.

2) Network layer: Network layer deals with transmission of messages and information security [2]. It lays out the ubiquitous access framework for the perception layer and sends the data collected by perception layer to the application layer [12]. IoT networks use UDP instead of TCP because of its low latency. But, UDP is less secure due to its connectionless packet delivery. DoS attacks are possible on UDP ports. The authors in [24] have studied the use of UDP ports in IoT networks in reflecting a DoS attack on a traditional network. Similarly, they can be victims of DoS attacks themselves too.

3) Application layer: IoT uses Constrained Application Protocol (CoAP), developed by Internet Engineering Task Force (IETF), in the application layer. " The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained(e.g., low-power, lossy) networks"[26]. In IoT, UDP protocol is used for delay-sensitive applications. Therefore, since UDP is an unreliable protocol and communication takes place through datagrams. Here, datagram transport layer security (DTLS) protocol is used for datagram security [27]. It is mainly used for authentication, DoS detection and decision about cryptographic keys.

Table III shows the IoT layers and some associated DDoS attacks.

D. Classification by Architecture

- Agent-handler: These DDoS attacks are carried out by agents which reside in the bots/infected devices. Agents are the software programs on the bots and handlers command agents to carry out the attack. They are the intermediate link between the attacker and the agents.
- Reflector-based: In this architecture, the DDoS attack is carried out by the reflectors. The reflectors are basically devices used by the botnet in carrying out the attack. This is done in order to avoid detection. They act as another layer of devices to hide the identity of the attacker. Reflectors are sometimes used to amplify the attack.

E. Classification by Impact

- Disruptive: When the DDoS attack volume is high enough to disrupt the service, it is known as disruptive DDoS attack. They can be easy to detect because they produce a high volume of data at particular routers.
- Degrading: When the DDoS is more sophisticated and stealthier and does not create huge traffic, then are called degrading [28]. They are trickier to detect. They do not stop the service but they impact the efficiency of the system.

F. Classification by Exploited Vulnerability

- Resource Depletion: This type of attack considers the vulnerability that the resources in remote IoT systems are limited. So, the goal of such attacks is to deplete or exhaust the resources of the IoT system to deirupt its functioning. Misusing the vulnerabilities of certain protocols in order to occupy the resources for example, TCP SYN attack, come in this category.
- Bandwidth Depletion: It can be further divided into flooding and amplification attacks. Flooding attacks namely UDP flooding, TCP flooding can bombard the link with the packets in order to deplete the bandwidth.

V. DDOS TOOLS AND BOTNETS

A. DDoS tools

1) Trinoo: Trinoo follows an agent-based architecture and utilizes UDP flooding to attack the victim [31]. It targets to deplete the bandwidth and perform remote buffer overrun exploitation. Both encryption and password protection can be used for the communication channel. For further reading, the user can refer to [32]. Trinoo has been thoroughly studied in this paper.

2) Low Orbit Ion Cannon LOIC: LOIC was originally made by a developer called praetox and was used as a stress-testing tool. Many differnet versions of this have been launched into the Internet. The first version was used during the Operation Chanology attack in 2008. Further, two versions came that were posted by abatishchev and NewEraCracker. During September and December months of 2010, an attack called Operation Payback occured and there was a spike in the downloads of these versions of LOIC during the same time [33]. It utilizes the TCP flooding, UDP flooding, and ICMP

flooding. With an agent-based architecture, it is a bandwidth and resource depletion tool. It depletes the resources like storage, CPU time and bandwidth[31]. It utilizes encryption during communication. [34] has stated that it is disruptive in nature.

3) Trinity: It employs UDP flooding, TCP SYN flooding, TCP ACK flooding and TCP NULL packet flooding. It has also utilized other flooding methods using TCP RESET packet, TCP fragment, and TCP random flag packet flooding. It has an IRC-based architecture and is used for resource and bandwidth depletion. In this tool, the communication in the channel is not encrypted.

4) Tribal Flooding Network(TFN): TFN uses an agent-based architecture and is used to deplete the bandwidth and resources on the victim. It utilises UDP flood, TCP SYN flood and smurf attack to bombard the victim. It utilizes CAST-256 algorithm for encryption in communication channel between attackers and handlers.

5) Mstream: MSTREAM is a bandwidth depletion tool that utilises the agent based architecture. It employs TCP ACK floods, TCP SYN flooding, ICMP flooding and RST flooding. It uses spoofing method to avoid detection. However, the communication in the communication channel is not encrypted.

B. Botnets

1) Mirai: Mirai was unveiled by MalwareMustDie in August, 2016 [30][35]. "It is classified as an Executable and Linkable Format(ELF) multi-platform worm and is known as ELF Linux/Mirai [30]." It has a centralized architecture. Mirai botnet consists of bot, C&C server, loader, report collector and bot handler. The bot is coded in C and runs on infected devices[36] [37]. Then, it deletes itself to escape from detection and also prevents it from rebooting. C&C server is implemented in GO and runs remotely. The complete architecture of Mirai is given in [38]. The authors have thoroughly explained the working of Mirai and reported the 10 attacks launched by it. Mirai can perform UDP attack, TCP SYN attack, TCP ACK attack, TCP STOMP attack, Valve Source Engine Attack, GRE IP attack, GRE Ethernet attack, UDP Plain attack, Domain Name Server attack, and HTTP attack.

An infected device scans the IP addresses of vulnerable devices in the scanning phase. It probes the port 23(telnet) and after every ten attempts, it probes port 2323(TCP). As the telnet session starts, a bot handler or an admin handler is allocated and the device's information is sent to the report server. Then in the infection phase, the loader sends the Mirai binary onto the device. Then in the operation phase, the newly infected device similarly scans for other devices upto 128 connections/second. In this way, the botnet expands and grows itself. The Mirai binary contains the complete information about the attack for example, attack duration, attack type, etc. Now, other versions of Mirai have started attacking other ports like $7547, 23231, 5555, 22, 32, 19058, 2222,$ and 37777. Yet, the ports 23 and 2323 are exploited by about 97% of the total scans. The malware eliminates the other worms using memory scrapping due to competition. Mirai can carry out network layer attacks as well as application layer attacks. to avoid detection, the latest strains of Mirai have encrypted communication between the C&C server and the bot.

Mirai code was released on the Internet on Sept 30, 2016 allegedly by Anna-Senpai. After this, the Mirai botnet had infected 500,000 devices worldwide. Mirai has been evolved from other DDoS botnet called Bashlight. Deutsche Telekom Internet Service Provider faced a DDoS attack and about 0.9 million customers were affected by the attack. It sends TCP SYN requests to random IP addresses via telnet ports 23 and 2323. If the device responds, then it immediately starts brute force login phase. It uses hardcoded list of 62 pairs of usernames and passwords. This list contains only 60 unique pairs, 15 unique usernames and 42 unique passwords.

2) Luabot: The first IoT trojan written in the programming language, Lua, was made for ARM architecture IoT Linux machines [30]. It was unveiled on late August, 2016 by the MalwareMustDie [39]. It was called ELF Linux/Luabot. Luabot is autonomous and does not depend on the host. It has a centralized architecture and its main aim is to infect devices for adding them to the botnet. It can carry out application layer DDoS attacks. When a device has been compromised, Luabot stops remote access to it using the modified iptable rules. Luabot hijacks the cable modems, steals their configuration and private certificates to sell them to cloners.

3) Hajime: Hajime was found on October, 2016 by the Rapidity networks. To infiltrate, it attacks port 5358 which is utilized by Web Service on Devices API (WSDAPI). It uses same credentials list as Mirai to gain access but it uses the credentials randomly instead of sequentially. After gaining access, it opens the shell and opens a writeable directory and download and execute a small binary called loader stub. Hajime binaries are supported for different architectures like arm5, arm6, arm7, mipsel and mipsel. If the stub is not present already, then it finds the hardware infrastructure of the victim to download a compatible verson of the stub. It uses BitTorrent DHT protocol for peer discovery and employs uTorrent Transport(uTP) for data exchange[30]. Hajime is compatible with the universal Plug and Play(uPnP) and Internet Gateway Device (IGD) protocol and therefore can infect routers easily. It communicates with its bots through a distributed overlay network which is trackerless, and therefore, it is highly resilient.

4) BrickerBot: BrickerBot, a busybox-based IoT malware was reported by researchers in Radware[30] [40]. It can attack linux/BusyBox-based IoT devices with Permanent Denial of Service attacks(PDoS). To perform the PDoS, it defaces the firmware of the device, deletes the contents of the storage units, reconfigures network connectivity parameters of the operating system kernel, and so on. It does not download any binaries on the device unlike others. Another stealthier variant of BrickerBot does not use BusyBox but it uses Tor

TABLE IV
BOTNETS IN THE PAST.

Botnet	Unveiled by	Unveiled in	Strengths
Mirai	MalwareMustDie	August, 2016	both network-layer and application layer attacks
Hajime	Rapidity Networks	October, 2016	uPnP compatible and can easily infilterate routers
Luabot	MalwareMustDie	August, 2016	application layer attacks
BrickerBot	Radware	2017	permanent DDoS attacks

for ensuring anonymity of its bots. Radware recorded 1895 PDoS attack attempts by BrickerBot in 2017.

C. Detection of botnets

- Monitoring the Telnet ports 23, 2323 looking for repetitive authorization attempts during the infection phase can lead to their detection.
- During the attack, observing a sudden increase in egress traffic is a sign of attack.
- These botnets can be detected by signature-based or rule-based detection approaches also.

D. Mitigation of the botnet attacks

Authors in [38] [30] have presented some simple mitigation strategies for these malwares.

- Ports 23 and 22 must be closed when not in use[38].
- Ingress and egress filtering is applied to drop the TCP egress connections carrying attack traffic.
- Access lists are used for access control.
- Mostly, the infection can be removed by rebooting the router/gateway.
- uPnP should be disabled on the IoT devices.
- IoT devices must run the updated operating systems and softwares.
- The default passwords must be changed[38].

Authors in [41] have proposed a detection model using Bidirectional Long Short Term Memory based Recurrent Neural Network(BLSTM-RNN). To evaluate its performance, they detected four types of attacks namely, UDP flood, DNS flood, ACK flood, and SYN flood attacks of Mirai. They achieved 99%, 98%, 98% accuracy and validation loss metrics of 0.000809, 0.125630, 0.116453 for Mirai, UDP and DNS respectively. Ahmed et al.[42] have proposed a detection approach for Mirai botnet based on blockchains. Table IV shows the botnet, the organizations which revealed them and its time.

VI. TAXONOMY OF DEFENSE MECHANISMS OF DDOS ATTACKS

Figure 5 describes the taxonomy of DDoS attacks defense mechanisms in IoT.

A. Classification on the basis of action

1) Detection mechanisms: According to the authors in [11], the DDoS detection mechanisms can be broadly categorized as signature-based detection, anomaly-based detection, and hybrid detection. Moreover, they discussed different ways to create attack signatures in signature-based detection and further classified anomaly-based detection into point anomaly-based detection, contextual anomaly-based detection, and collective anomaly-based detection. They discussed different detection approaches for all the classes of detection mechanisms. They defined functional classes of detection approach namely, core-end detection, source-end detection, victim-end detection, supervised mode, semi-supervised mode, unsupervised mode, net-DDoS detection, App-DDoS detection, HDDoS detection, LDDoS detection, profiling based, model-based, one-class setting, and multi-class setting. Furthermore, the authors analysed the performance of signature-based, anomaly-based, and hybrid detection mechanisms based on different evaluation metrics.

Anomaly-based detection mechanisms can also be divided into two parts i.e. threshold-based and AI-based mechanisms. Entropy-based detection belongs to the category of threshold-based detection. Here, the model can be only as much different from the standard model as the threshold allows. Anomaly detection has been discussed in detail in later sections.

Some approaches use both of signature and anomaly detection in the detection. Cephali et al. have presented a hybrid IDS called H-IDS that uses combines the results of both these approaches and then predicts the occurrence of attack [47].

2) Prevention mechanisms: There are two prevention mechanisms, namely resource multiplication and resource accounting.

- Resource Accounting: Based on the user privileges and its activity, these mechanisms provide the user access to the resources. In these mechanisms, the user's identity is verified to prevent the theft of identity. They provide fair access to legitimate users.
- Resource Multiplication: In this approach, the resources like memory, computation power are increased abundantly to lower the impact of the DDoS attack on the target network.

3) Response: Based on the response activity, the defense can be divided into four categories, namely, rate-limiting, agent identification, filtering, and reconfiguring [16].

- Rate limiting: The rate of malicious traffic from a stream is limited in this approach. This approach is used when there are chances of false positives and the reported malicious stream does not need to be entirely shut.
- Filtering: Filtering is used to shut the DoS attack streams completely. In case of a false positive, a legitimate user can also be mistakenly denied the service.
- Reconfiguration: In these mechanisms, the network topology of the victim network or the intermediate network is changed to mitigate the attack. By changing it, more resources are added or the malicious devices are identified.
- Agent identification: In this approach, the attackers are identified from the whole network. IP traceback is one

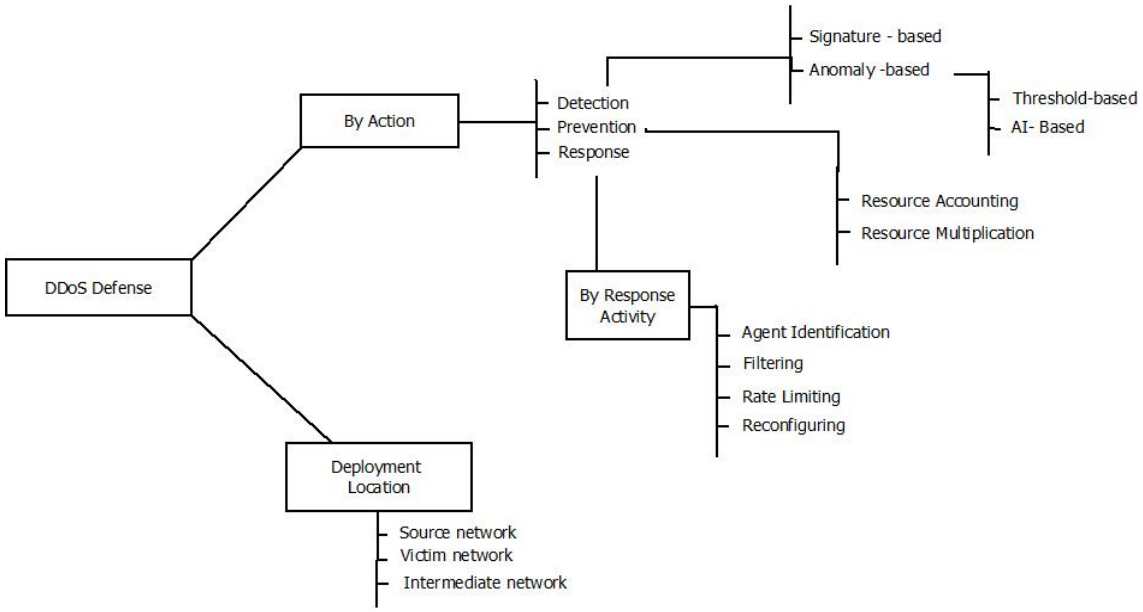

Fig. 5. Taxonomy of defense mechanisms for DDoS attacks in IoT

example of this mechanism. After knowing the identity of the attacker, other response approaches can be used to mitigate the attack.

B. Classification on the basis of Deployment Location

On the basis of deployment location, [15] classified the DDoS defense mechanisms in three categories, namely, source-end, victim-end, and intermediate network. Bhuyan et al. discussed one more category, namely, distributed [48]. They proposed that victim-end deployment of the system is better because" it can closely observe the victim system or host to analyse the network traffic in near real-time, is easy to deploy and is cheaper to detect DDoS attacks than other mechanisms". Table **??** presents a comparison of deployment sites of DDoS defense [48] [49].

VII. Network Simulators and Emulators

A. COOJA

Authors in [50] have proposed COOJA, a simulator that introduces the cross-level simulations. COOJA supports three levels of simulation, viz. network level, operating system level and machine code instruction set level. It runs with the support of Contiki OS which is proposed by [51] for resource- constrained devices. Implemented in C, it has been made for different microcontroller architectures like Atmel AVR and Texas Instruments MSP430. Contiki facilitates "dynamic loading and unloading of individual programs and services[51]." It has event-driven kernel and also provides pre-emptive multi-threading as a library that when the base system is lightweight and compact in a resource constrained environment it is feasible to dynamically load and unload services and programs.

B. Netsim

It is a JAVA-based simulator. Netsim facilitates discrete-event simulation through event-graph modelling. The features of Netsim are as follows:

- use of graphical interface for editing and manipulation of the model.
- facilitates user control in execution of the model.
- the output provided is numerical as well as animated.
- Java-based simulator provides object-oriented code which facilitates the re-use and easy modification of code and reduces the memory usage.
- Being a Java-based tool, it is platform independent and compatible with other Java-based tools.

C. OMNET++

Based on Eclipse platform, it has a C++ simulation framework and library. It is based on a network simulation model which is object oriented and incorporates discrete events. It can be utilized free of cost for teaching and research.

VIII. Available Datasets

There are various datasets available for studying DDoS attacks. CAIDA data collection 2007 was given by Center for Applied Internet Data Analysis. The CAIDA DDoS attack 2007 dataset has an hour of traffic traces in pcap format. A single key CrytoPAn prefic-preserving anonymization has been done on the traces. All the packages have had the payload removed. TUIDS DDoS dataset was created by Tezpur University [52]. The attack traffic was generated by 22 attack types. The coordinated scan dataset was generated by six attacks. The DDoS attack was created by six attacks. In this dataset, DDoS attack was carried out in two scenarios i.e., once by using Agent-handler network and then by using

IRC botnet.

1998 DARPA Intrusion Detection Evaluation Dataset created by MIT Lincoln Laboratory. This dataset has two parts: off-line evaluation and real-time evaluation. The off-line evaluation was done utilizing the network traffic and audit logs accumulated on a simulated network. For the offline evaluation, three weeks of training data were generated. Out of the three weeks, no attacks were carried out on the first and third weeks. Attacks are contained in the second week of the dataset. The two weeks long testing data has 201 instances of 52 types of network-based attacks along with normal data. The real-time evaluation of the intrusion detection system is done by Air Force Research Laboratory (AFRL).

2000 DARPA dataset [53] constitutes of three datasets which are generated in concurrence with the Wisconsin Re-Think meeting and July 2000 Hawaii PI meeting[14]. This dataset comprises of three datasets, namely LLDoS 1.0, LLDOS 2.0.2, and windows NT Attack Dataset. The first one was collected when a novice attacker is against a naive defender. The second one consists of the scenario when the attacker is more stealthy but still novice and the defender is naive. The third dataset comprises of NT auditing of traffic of one day and attack striking the NT machine.

2009 DARPA DDOS Dataset was created by the Colarado State University. The dataset contains data of ten days from November 3, 2009 to November 12, 2009. It shows the traffic between the Internet and a /16 subnet and contains SMTP, synthetic HTTP, and DNS background traffic. For DDoS attacks two smaller datasets were obtained from the main dataset namely, DARPA-2009 DDoS Attack-20091105 and DARPA- 2009 malware- DDoS attack-20091104. The first one shows a SYN flood DDoS attack carried out by 100 IP addresses on a single target. This contains six minutes of traffic data. In the second one, compromised hosts from a local subnet were used to carry out a malware based DDoS attack. This attack was targeted at a non-local victim. This dataset also comprises of six minutes of traffic data.

CICDDoS 2019 has been generated by University of Brunswick, Canadian Institute for Cybersecurity [14]. It has included even new attacks for example, UDP-Lag attack. All the attacks can be classified into two sections, reflection attacks and exploitation attacks. Reflection attacks include MSSQL, SSDP, DNS, LDAP, NETBIOS, SNMP, PORTMAP, CharGen, NTP, TFTP attack. The exploitation attacks include SYN flood, UDP flood and UDP-Lag.

IX. Conclusion and Future Scope

IoT devices have constraints like limited power, memory, and small computational capability. These challenges can be exploited by the attackers. In addition, neglected open ports, inadequate software updates, outdated security patches, and weak programming practices help the attackers put malwares on such systems. DDoS attacks in IoT can have major hinderance to the acceptance of IoT in the society. This paper aims to address all the issues regarding DDoS attacks in IoT. In this paper, we have presented a taxonomy of DDoS attacks and their detection mechanisms in the context of internet of things.

References

[1] P. Nicholson, "Aws hit by largest reported ddos attack of 2.3 tbps," Jun 2020. [Online]. Available: https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-tbps/

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, no. March, pp. 10–28, 2017.

[3] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors (Switzerland)*, vol. 20, no. 13, pp. 1–20, 2020.

[4] M. binti Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019. [Online]. Available: https://doi.org/10.1016/j.comnet.2018.11.025

[5] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[6] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[7] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[8] V. Hassija, V. Chamola, V. Saxena, and D. Jain, "A Survey on IoT Security : Application Areas , Security Threats , and Solution Architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[9] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, no. xxxx, p. 100129, 2019. [Online]. Available: https://doi.org/10.1016/j.iot.2019.100129

[10] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[11] P. Kaur, M. Kumar, and A. Bhandari, "A review of detection approaches for distributed denial of service attacks," *Systems Science & Control Engineering*, vol. 5, no. 1, pp. 301–320, 2017.

[12] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of things journal*, vol. 5, no. 4, pp. 2483–2495, 2017.

[13] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, 2020.

[14] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2019, pp. 1–8.

[15] D. K. Bhattacharyya and J. K. Kalita, *DDoS attacks: evolution, detection, prevention, reaction, and tolerance*. CRC Press, 2016.

[16] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[17] A. Asosheh and N. Ramezani, "A comprehensive taxonomy of ddos attacks and defense mechanism applying in a smart classification," *WSEAS Transactions on Computers*, vol. 7, no. 4, pp. 281–290, 2008.

[18] U. Tariq, M. Hong, and K.-s. Lhee, "A comprehensive categorization of ddos attack and ddos defense techniques," in *International Conference on Advanced Data Mining and Applications*. Springer, 2006, pp. 1025–1036.

[19] G. Maciá-Fernández, J. E. D\'\iaz-Verdejo, and P. Garc\'\ia-Teodoro, "Mathematical model for low-rate DoS attacks against application servers," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 519–529, 2009.

[20] ——, "Evaluation of a low-rate DoS attack against application servers," *computers & security*, vol. 27, no. 7-8, pp. 335–354, 2008.

[21] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," *IEEE transactions on information forensics and security*, vol. 6, no. 2, pp. 426–437, 2011.

[22] M. Sachdeva, K. Kumar, and G. Singh, "A comprehensive approach to discriminate DDoS attacks from flash events," *Journal of Information Security and Applications*, vol. 26, pp. 8–22, 2016.

[23] S. Egbo, *The 2016 Dyn DDOS Cyber Attack Analysis: The Attack That Broke the Internet for a Day*. North Charleston, SC, USA: CreateSpace Independent Publishing Platform, 2018.

[24] M. Lyu, D. Sherratt, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Quantifying the reflective DDoS attack capability of household IoT devices," *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2017*, pp. 46–51, 2017.

[25] P. Foremski, S. Nowak, P. Fröhlich, J. L. Hernández-Ramos, and G. Baldini, "Autopolicy: Automated traffic policing for improved iot network security," *Sensors (Switzerland)*, vol. 20, no. 15, pp. 1–19, 2020.

[26] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," 2014.

[27] E. Rescorla and N. Modadugu, "RFC 6347: datagram transport layer security version 1.2," *IETF, Tech. Rep., January 2012*, 2017.

[28] K. Doshi, Y. Yilmaz, and S. Uludag, "Timely detection and mitigation of stealthy ddos attacks via iot networks," *IEEE Transactions on Dependable and Secure Computing*, 2021.

[29] P. Nicholson, "Five most famous ddos attacks and then some," Jul 2020. [Online]. Available: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

[30] G. Kambourakis, C. Kolias, and A. Stavrou, "The mirai botnet and the iot zombie armies," in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017, pp. 267–272.

[31] B. Nagpal, P. Sharma, N. Chauhan, and A. Panesar, "DDoS tools: Classification, analysis and comparison," *2015 International Conference on Computing for Sustainable Global Development, INDIACom 2015*, pp. 342–346, 2015.

[32] D. Dittrich, "The dos project's 'trinoo'distributed denial of service attack tool," 1999.

[33] M. Sauter, ""LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks," *American Behavioral Scientist*, vol. 57, no. 7, pp. 983–1007, 2013.

[34] S. Acharya and N. Tiwari, "Survey Of DDoS Attacks Based On TCP / IP Protocol Vulnerabilities Related papers," *IOSR-Journal of Computer Engineering*, vol. 18, no. 3, pp. 68–76, 2016.

[35] MalwareMustDie, "Linux/mirai, how an old elf malcode is recycled.." https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html.

[36] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, and Y. Liu, "The impact of dos attacks onresource-constrained iot devices: A study on the mirai attack," *arXiv preprint arXiv:2104.09041*, 2021.

[37] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[38] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," *Proceedings - 2017 International Conference on Software Security and Assurance, ICSSA 2017*, pp. 6–12, 2018.

[39] MalwareMustDie, "Linux/luabot - iot botnet as service," https://blog.malwaremustdie.org/2016/09/mmd-0057-2016-new-elf-botnet-linuxluabot.html.

[40] radware, ""brickerbot" results in permanent denial-of-service," https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/.

[41] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *Proceedings of the International Joint Conference on Neural Networks*, vol. 2018-July, pp. 1–8, 2018.

[42] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, "Protecting IoTs from mirai botnet attacks using blockchains," *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*, vol. 2019-Septe, pp. 1–6, 2019.

[43] ZDNET, "Hackers are hijacking smart building access systems to launch ddos attacks," https://www.zdnet.com/article/hackers-are-hijacking-smart-building-access-systems-to-launch-ddos-attacks/.

[44] A. Califano, E. Dincelli, and S. Goel, "Using features of cloud computing to defend smart grid against ddos attacks," in *10th Annual symposium on information assurance (Asia 15), ALBANY*, 2015, pp. 44–50.

[45] W. Chen, S. Xiao, L. Liu, X. Jiang, and Z. Tang, "A DDoS attacks traceback scheme for SDN-based smart city," *Computers and Electrical Engineering*, vol. 81, 2020.

[46] N. Z. Bawany and J. A. Shamsi, "Application layer ddos attack defense framework for smart city using sdn," in *The Third International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM2016)*, 2016, p. 1.

[47] Ö. Cepheli, S. Büyükçorak, and G. Karabulut Kurt, "Hybrid intrusion detection system for ddos attacks," *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[48] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection," *Pattern Recognition Letters*, vol. 51, pp. 1–7, 2015.

[49] M. Sachdeva, "A Distributed approach for defending web service against ddos attacks," Ph.D. dissertation, Guru Nanak Dev University, 2012.

[50] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Proceedings. 2006 31st IEEE conference on local computer networks*. IEEE, 2006, pp. 641–648.

[51] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki-a lightweight and flexible operating system for tiny networked sensors," in *29th annual IEEE international conference on local computer networks*. IEEE, 2004, pp. 455–462.

[52] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Towards generating real-life datasets for network intrusion detection," *International Journal of Network Security*, vol. 17, no. 6, pp. 683–701, 2015.

[53] "Darpa 2000 intrustion detection scenario specific data sets," https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-data-sets, accessed by July, 2021.