




# A survey of DDoS attacking techniques and defence mechanisms in the IoT network

Ruchi Vishwakarma<sup>1</sup> · Ankit Kumar Jain<sup>1</sup> 

Published online: 29 July 2019  
© Springer Science+Business Media, LLC, part of Springer Nature 2019

## Abstract

Internet-of-things has emerged out as an important invention towards employing the tremendous power of wireless media in the real world. We can control our surroundings by interacting with numerous smart applications running independently on different platforms, almost everywhere in the world. IoT, with such a ubiquitous popularity often serve itself as a potential platform for escalating malicious entities. These entities get an access to the legitimate devices by exploiting IoT vulnerabilities which results from several constraints like limited resources, weaker security, etc. and can further take form of various attacks. Distributed Denial-of-service (DDoS) in IoT network is an attack which targets the availability of the servers by flooding the communication channel with impersonated requests coming from distributed IoT devices. Defending DDoS in IoT has now become an exigent area of research due to the recent incidents of demolition of some renowned servers, reported in previous few years. In this paper, we discuss the concept of malware and botnets working behind ‘Distributed’ DoS in IoT. The various DDoS defence techniques are broadly described and compared in order to identify the security gaps present in them. Moreover, we list out the open research issues and challenges that need to be addressed for a stronger as well as smarter DDoS defence.

**Keywords** IoT · DDoS · Botnet · Malware detection · Machine learning

## 1 Introduction

Internet of things is a massive network of those things which are capable of being connected to each other and to the internet to exchange data and services with each other but without having any human intervention [1]. Formally, it can be defined as a system of interconnected devices (i.e. things) which can be identified uniquely in a network and capable of transferring the data without human intervention [2]. It allows us to interact, contribute and collaborate to things without getting involved in the process, unlike other traditional networks. IoT is preferable over all other traditional networks mainly because of its non-interference, wider scope, and scalability features [3].

In today’s world, IoT has become the largest network encompassing millions of devices interacting with each other to make human operations simpler and easier. According

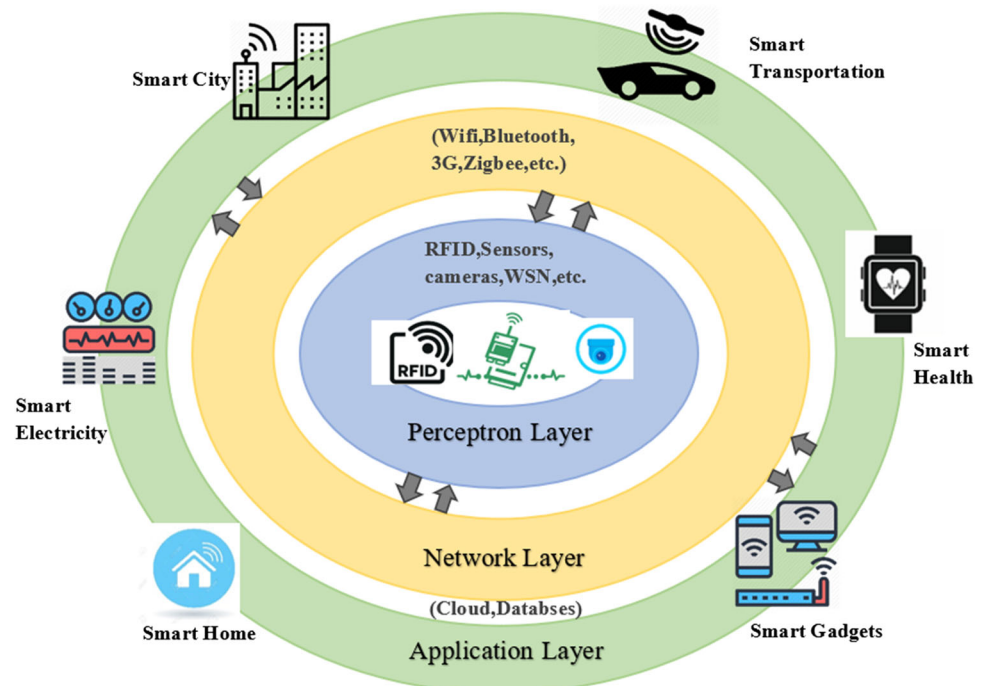
to a recent survey, 22 million Amazon Echos, 310.4 million dollars of wearable devices have been sold out till 2017 [4]. Moreover, for the future explosion, 30.73 billion of IoT devices are expected by 2020 and will continue to increase to double up the number in just next 5 years [5].

Different functions are performed at different levels in the whole IoT working span to achieve the desired objective of any smart application. Many reference models or frameworks for IoT have been proposed in the literature to understand IoT working profoundly [6]. The basic model shown in Fig. 1 includes three layer which depicts three different functionalities. The first layer is about collecting the data using several sensing devices like sensors, RFID readers, smart controllers, etc. The data collected here must be in a standardized form so that it becomes operable in different protocols used in the network [7]. This layer generally called a perceptual layer or edge device layer. The second layer is about networking which takes the responsibility of the communication between the application and the edge devices through which data is sensed. The wireless medium is used to carry the collected data e.g. Bluetooth, WIFI, Zigbee, etc. This layer is called the network layer. The outermost and final layer is called the

✉ Ankit Kumar Jain  
ankitjain@nitkkr.ac.in

<sup>1</sup> National Institute of Technology, Kurukshetra, Kurukshetra, India

**Fig. 1** Layered architecture of IoT network



Application layer. There is a number of smart applications using IoT as a medium like smart city, smart home, smart grid, etc. [8].

Though it has a very straightforward definition, it becomes much more complicated and substantial when dealing with its security and privacy issues. Due to unreliable networking protocols used and less human intervention, it becomes much more vulnerable to various security threats. Another major reason is being limited in terms of both power resources and memory which make it intolerant to today's highly technical security attacks.

### 1.1 Security issues in IoT

Securing IoT from a variety of possible attacks is a quite complicated task. However, it becomes manageable to some extent when referenced under its layered architecture as discussed in the previous section. Every layer has its own limitations and vulnerabilities that need to be identified to ensure its security by preventing it from different types of attacks [9]. Preventing such attacks needs a proper security system which addresses existing vulnerabilities present in an IoT device. For that we need to first zoom in the term vulnerability and how does it contribute to an attack. A vulnerability in a system represents the incompetency of the system that enables the attacker to find out the scope to invade the system security. It can lead to a threat that in turn lead to an attack when get ignored. Table 1 presents the list of vulnerabilities [5] along with its contributing factors which actually are

accountable for the occurrence of any cyber-attack on IoT devices:

Most of the vulnerabilities are just the outcomes of our irresponsible and careless behavior towards IoT device handling. Therefore, above all such measures, there is a very important one that can easily be taken care of by ourselves on our own, and that is called Self Awareness. The user should be completely aware of all the risks involved and necessary steps that should be taken in case of any unknown activity in their IoT devices.

The current security system needs to get complemented with functionalities like intrusion detection system, content filtering, firewalls, inspection technologies and application whitelisting to cope with newer and smarter variants of launching the attack [10].

### 1.2 DDoS attack in IoT

As happens in the case of simple DoS attack where the targeted device or server denies serving any request from its clients due to excessive flooding of data in the communication channel consuming all the bandwidth unnecessarily and as an effect, makes the server inaccessible for further requests. This overflow of data is intentionally targeted by the attacker against the server in the form of false requests due to which legitimate requests also get suffered and are dropped before completion [11]. The consequent of such violation in a distributed environment i.e. where the transfer of data is carried out among different network devices distributed across the network without having any centralized control

**Table 1** List of current IoT vulnerabilities with their corresponding weak points

Vulnerability	Responsible weak points
Lack of sufficient authentication and authorization	Default feeble passwords, weak password retrieval systems, insecure protected credentials, and lack of granular access control may enable an attacker to access a particular interface
Unreliable user interfaces	Weak login credentials, plain-text credentials, weak password retrieval systems, and absence of transport encryption may be used to access data or controls
Insecure network services	Susceptible networks services may be used to attack a device or bounce an attack off of a device
Privacy issues	Unreliable interfaces, weak authentication, insufficient transport encryption, and insecure network services all allow an attacker to access weakly protected data and may have been collected unnecessarily
Insufficient transport encryption/integrity verification	The lack of transport encryption allows an attacker to view data being passed over the network
The inadequacy of the security configuration	A lack of granular permissions, lack of encryption or password options may allow a hacker to access system information and controls. A cybercriminal could come from any device in an IoT system
Poor physical security	USB ports, memory cards, and other peripheral/storage device may allow cybercriminal to access data and OS

is generally known as a DDoS Attack [12]. This is one of those attacks that take place at both application layer and infrastructure layer (i.e., Network and Transport layers) of the network architecture.

There are some awestricken facts and figures [13] about recently recorded incidents of server crashes. It really makes us hard to believe how deeply this attack has shaken the foundations of IT security using IoT as a weapon:

- In the last three years, the DDoS attacks frequently have been observed with 2.5 increasing rates [14].
- The average amount of data it has used to flood the whole network has been approached to 1Gbps and its still going to increase [15].
- 86% of the total attacks that have been launched in the year 2017 are observed to be of multiple type's means composed of different types of variations possible in firing a DDoS attack, hence making it difficult to identify and mitigate [16].
- DDoS attacks get more attracted towards the gaming applications and are accountable for 30% of the gaming traffic.
- This attack has become a matter of business in today's competitive world. It has now become as easy as performing a quick online search and as cheaper as 5 dollars per 300 s server down period [17].
- More than 100% increase in the number of DDoS attacks is observed in year 2017 from the previous year recorded data [18].
- The types of potential victims or targets of the DDoS attack can range from private organization to the Government healthcare, education, and financial institutions, regardless of the nature of the organization. From the surveyed data

in 2018, Financial services, IT services/Cloud/SAAS and Telecom industry are come out to be the most targeted industries [19, 20].

- A DDoS attack can render the server unreachable for few hours to several days.

The actual destruction caused by an attack does not just result into server crash or flooded websites rather it also leads to a loss in consumer trust and confidence in the concerned serving industry.

The remainder of the section is organized as: Sect. 2 presents the related work. Section 3 discusses weaponizing the distributed DoS attack i.e. about botnets along with an overview of some recently discovered botnets. Further, Sect. 4 defines the taxonomies in DDoS Attacks based on the affected layers of network architecture along with current statistics. Taxonomies of DDoS defence mechanisms have been described in Sect. 5 followed by the comparison table on their advantages and disadvantages in Sect. 6. Moreover, the whole discussion will be incomplete without throwing lights on some open research issues and challenges that need to be addressed for coming up with an overall protected defence against DDoS, as described in Sect. 7. Section 8 concludes the whole discussion on the DDoS attack in IoT.

## 2 Related work

Number of surveys have been carried out in the past on DDoS attacks. However, most of them have discussed about a typical DDoS attack, it's types and defence mechanisms for the traditional networks. There is lot of information avail-

**Table 2** Comparison among several survey on DDoS attack in IoT

Existing surveys	Security issues in IoT	Taxonomy of DDoS attacks	Role of current IoT Botnets and Malware	Taxonomy of DDoS defence mechanisms	Comparison among defence mechanisms	Open challenges and issues
Zargar et al. [21]	✗	✓	✓ (newer malware variants not covered)	✓ (no IoT-specific defence mechanism)	✓ (for traditional methods only)	✓
Sonar et al. [74]	✓	✗	✗	✗	✗	✗
Zhang et al. [75]	✓	✗	✗	✓	✗	✗
Yang et al. [76]	✓	✓	✓ (newer malware variants not covered)	✗	✗	✗
Abdul-Ghani et al. [77]	✓	✓	✓ (newer malware variants not covered)	✗	✗	✓
Our paper	✓	✓	✓	✓	✓	✓

✗ not covered; ✓ covered; ✓ partially covered

able in the literature about defending DDoS attacks that can be effectively utilized to prepare a base model for a defence to deal with today's DDoS attack in an IoT network. Zargar et al. [21] presented a survey which discusses different types of DDoS flooding attacks including botnet-based DDoS attacks and their types but it lacks in terms of discussing the new malwares variants. Our survey does not just describe the traditional ways to mitigate DDoS attacks but also presents the current trends and scenarios in the area of DDoS in context of IoT specifically. Recent attacks in DDoS has brought up newer malware attacking techniques in the picture. Therefore, it has become mandatory to learn about some recently discovered malware variants and their features for building a stronger defence system against such attacks. Table 2. compares our survey with other recent surveys that have been performed under DDoS attack. We collected surveys on DDoS attack in IoT specifically to obtain the better knowledge about the content that needs to be covered. However, most of them are truly based on traditional DDoS attacks and their defences.

To summarise, our main contribution towards through this survey are listed as follows:

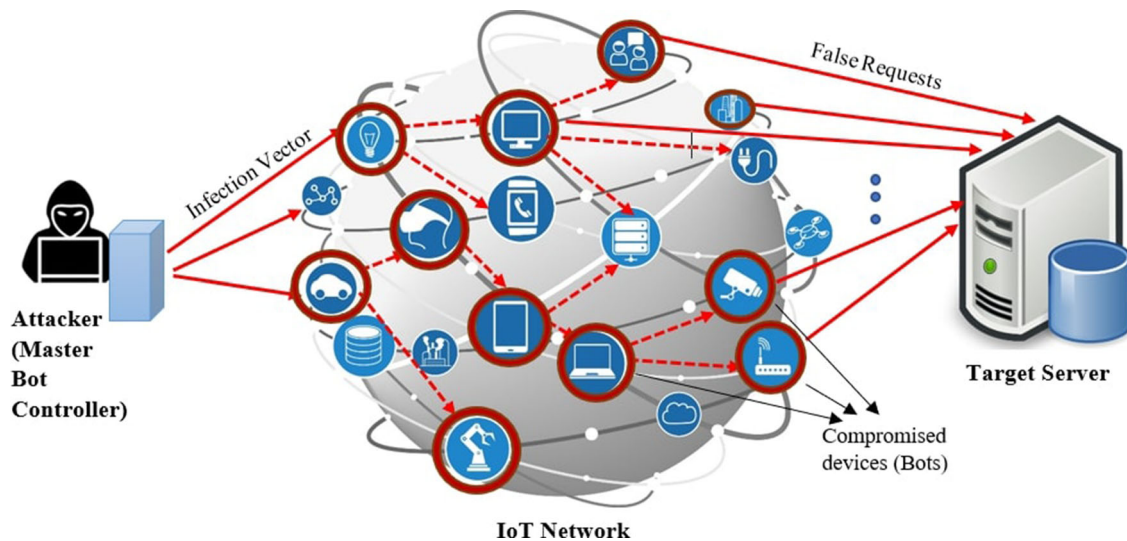
- (i) There are number of surveys on the topic of defending DDoS attacks in traditional networks, however there are only few on defending DDoS in IoT network. Our survey discusses all those main defence mechanisms which have employed distinct approaches to defend DDoS attack in both traditional as well as IoT network specifically, in detail. We have categorised all

such defence mechanisms into prevention, detection, and mitigation based depending on the methods and approaches they have taken to defend DDoS (Sect. 5).

- (ii) Apart from defence mechanisms, our paper also seeks the attention towards the main cause for the today's trend in DDoS attacks in IoT i.e. Botnets and Malware. We have briefly described about the famous IoT malware that had targeted some of the well-known servers in the recent years (Sects. 3, 4).
- (iii) Our comprehensive comparative analysis among several defence mechanisms has led us to come up with open challenges and issues which are need to be addressed to achieve an optimal solution against DDoS attack in an IoT environment (Sects. 6, 7).

### 3 Role of IoT botnets in DDoS attack

IoT that used to be considered a boon to the technology now heading towards becoming a bane to it by contributing to DDoS attack on a large scale. As the number of IoT devices is increasing, their possibility of becoming the victim of the DDoS attack is also increasing. These attacks work on the basis of malware infections that get transmitted over the network by compromising different IoT devices. The intensity of such an attack depends directly on the number of infected IoT devices the attacker has used to trigger the attack. These compromised IoT devices are known as 'bots' in the hacking community [22]. The conversion from a normal IoT device to a



**Fig. 2** DDoS attack using IoT as a weapon

bot takes place through the installation of malicious software (malware) on victim device by invading its security system without letting the user get aware of it. Moreover, the server that controls such bots is called ‘Master Bot Controller’. The mode of communication used by the master bots to control their infected machines can be IRC (Internet Relay Chat) based, Peer-To Peer-based and HTTP based. IRC based botnets are having a client–server architecture with default channels for communication whereas HTTP based botnets use HTTP protocol that works on the bit level of the data being communicated, hence making it harder to track and detect. Moreover, with repetition of such infection, millions of bots get created under the Master Bot and form a network known as ‘Botnet’. However, a traditional botnet platform contains master bot controller to create new bots (Malware) and differs slightly from the today’s IoT botnets in terms of their reach and scope. Traditional botnets are only able to compromise computer systems to the limited number. IoT botnets are much advanced in terms of targeting a larger number of IoT devices because these devices normally tend to remain on and connected to the internet for the much longer time (almost 24/7/365). Once a botnet is formed, all the bots are then treated as slaves of attacker’s master bot controller and then every bot is instructed to send bogus packets to the targeted web server at the same time making the targeted server system inaccessible to further legitimate packets also as shown in Fig. 2. Thus, botnets are the main reason why such attacks are becoming successful to such a widespread realm [23].

Now, the question arises how IoT devices get easily stuck into such traps. The reason lies in our negligence towards securing simple IoT devices. We are always much concerned about the security of those devices which are costlier and carry significant importance in our daily life like the lock system of our vaults, cars and other precious things [24].

In securing these things we often neglect those small and insignificant devices which are cheaper and doesn’t attract our attention towards even on assuring its basic level of security like web cameras, smart TVs, music systems etc. Our such ignorance towards securing these devices is enough to grab the attention of the attacker’s trap. Most of these devices don’t have any security system or have weaker one i.e. authenticated only with help of default username and passwords that can easily get cracked by the attacker’s malware by brute-forcing with possible pairs of username and passwords.

Nowadays, this has become a matter of business in the corporate world. The bot masters gain financial benefits by selling their attack services [25]. Such competition among different rivalries of IT and business has led the invention of new variants of botnets in the digital market. Some recently discovered botnets are:

### 3.1 Mirai

One of the malware gaining popularity these days due to its irrefutable impact in 2016’s DDoS Attack, is called Mirai which means ‘the future’ in Japanese [7]. It is Linux based malware and has converted millions of Linux running systems and other IoT devices into a bot. It is responsible for the largest DDoS attack recorded till now, comprising up to 15 million of IoT devices with a flooding speed of 1 Tbps, against a French hosting Provider. The most amazing and the challenging thing about it is that its source code is openly available on the internet and hence giving chances of other such unethical practices by improvising the code [10]. It has 62–68 default pairs of usernames and passwords defined in its code that are used for attempting to brute force the login module for getting entry to unsecured IoT devices.



### 3.2 Wirex

Recently, multiple Content Delivery Network (CDNs) and Content providers were targeted to become victims of a DDoS Attack that had been executed with the help of a botnet called Dubbed Wirex. It is named on one of the delimiter strings in its command and control protocol. It had comprised thousands of Android devices running applications which seemed to be legitimate but actually were malware. Akamai, Cloudflare, Flashpoint, Google, Oracle Dyn, and other organization researchers cooperated to combat this botnet. Google has already removed hundreds of applications cum malware from a number of devices that were there on the Play Store [26].

### 3.3 Reaper

As Mirai was only able to exploit devices with default credentials, just to increase the reachability, Reaper Botnet is able to exploit other plentiful vulnerabilities present in the IoT devices [27]. Several well-known routers of Cisco Linksys, Netgear, D-link, and internet connected surveillance cameras, have been victims of this botnet.

### 3.4 Torii

Torii is another malware that recently has been spotted by Dr. Bontchev on his honeypot via 'Tor' exit nodes (hence the name came as 'Torii') [28]. It was able to target most of today's modern computers, smartphones, tablets with having architectures like x86(64-bit), x86, ARM, MIPS, etc. Like Mirai, it also first looks for a telnet port for breaking through weak credentials but it is much sophisticated than other IoT malware due to its capability to download the appropriate payload to infect others having common architectures.

### 3.5 3ve-2018

3ve is the most sophisticated digital ad fraud schemes that have recently been shut down by the joint operation including Google, the FBI, WhiteOps and other ad fraud fighting companies in the fall down of this year [29]. It has infected over 1.7 million PCs to make fake clicks used to defraud online advertisers for years leading to business with a revenue of more than 10 million. It was different from other botnets as it was able to create its own botnet, creating fake versions for both websites as well as visitors, hiding its IP address using proxies, and hijacking Border Gateway Protocol (BGP) IP addresses and selling ad fraudulent ad inventories to advertisers to earn money.

To cope up with the level of these newer and much-sophisticated variants of malware, a stronger DDoS defence is needed that can fight against a wide range of variations in attacking methods.

## 4 Taxonomy of DDoS attacks in IoT network

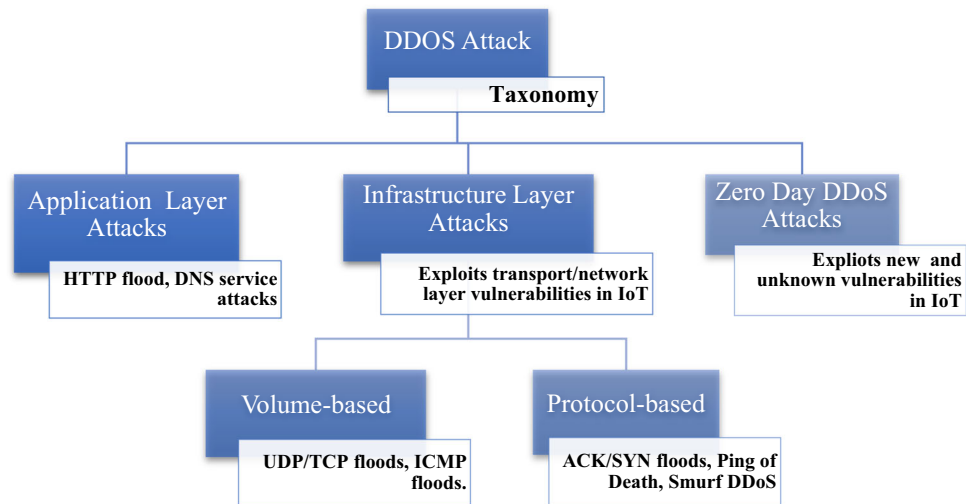
DDoS attacks have shown a number of variations in terms of their attacking methods in past years and still getting experimented with a number of possibilities. There is not much difference in IoT specific DDoS attacking methods and traditional DDoS attacking methods. They employ similar techniques to exploit the vulnerabilities exist either in conventional systems or in an IoT device. However, IoT specific DDoS attacks are more diverse and sophisticated due to heterogeneity involved in IoT devices. All such attacks can be broadly categorized into three types of attacks on the basis of their attacking techniques as shown in Fig. 3 [30].

One of the important points is to be noted here about the classification basis of DDoS attacks is that it completely depends upon the impact of the attack on the sever site in an IoT network. IoT specific DDoS attack types are similar to the traditional DDoS attack types except considering the corresponding network architecture as a reference model. However, we can have another class of DDoS attack type based on the ways of the generating number of pseudo requests from an IoT source to the targeted server. The only way that has been discovered yet to trigger such a huge number of false requests that utilises the power of IoT network is based on bots and malwares as described in detail in Sect. 3.

As discussed above, we will refer here the basic IoT network layered architecture to classify the DDoS attacks. Each layer can be targeted explicitly to invade the security of an IoT network-based application server. Thus, the attacks can be broadly categorised into Application layer attacks and Infrastructure layer attacks.

*Application layer attacks* [31] are those attacks which try to invade application layer of IoT network infrastructure where the packets are dropped at the rate of request per second (hence measured in Rps) due to flooding of application or web server by HTTP(Get/Post) requests, and other requests that target the system software like Windows, Apache, OpenBSD, etc. These attacks are harder to detect and mitigate as they tend to generate the traffic at a lower rate and the request generated seems to be legitimate but they actually trigger the back-end process that makes the resources unavailable. These include HTTP flood, DNS service-based attacks, etc.

*Infrastructure layer attacks* [32] are intended to render the target system inaccessible by exploiting the vulnerabilities present at the transport or network layer of the IoT architecture. These attacks can be of two types, protocol-based and volume-based attacks [33]. They usually employ reflection or amplification techniques to fire the attack. In reflection, the attacker uses IP address spoofing to reflect the sent request as an unrequested reply to the victim that leads to the congestion at the victim network. Amplification is also a reflection having larger replies for smaller requests which also unneces-

**Fig. 3** Taxonomy of DDoS attacks in IoT

sarily consumes the bandwidth. *Protocol-based attacks*, also known as *Resource Depletion attacks*, are responsible for consuming the actual server resources along with intermediate communication equipments like firewalls, load balancers, etc. [34]. They are measured in packets per second (Pps). Examples are SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, etc. *Volumetric attacks* also known as *Bandwidth Depletion attacks* saturate the bandwidth of the target system by generating excessive traffic in bits per second (Bps). These are simplest to employ as they use amplification and reflection techniques to launch the attack. It has been studied that up to 65% of attacks are only volume-based attacks. The examples of such attacks are UDP/TCP floods, ICMP floods.

In spite of having such a categorization, attacks can take the amalgamated form of aforementioned infrastructure layer attack types. IoT network intruders, now, are becoming smarter enough and have started experimenting with newer ways to launch the attack to overpower the security of even some renowned web servers too. One of the recent examples of such a case was Dyn DNS Outage, which was a combination of an application and protocol-based attack on DNS service that was expanded into a volumetric attack [30]. Followings are some well-known DDoS attacks that become common these days:

#### 4.1 ACK and SYN flood attack

ACK flood attack takes place during the TCP three-way handshaking process for establishing the connection between the attacker and the target device. The three-way handshake process starts with sending an SYN packet [32, 35]. Then SYN + ACK packet is received as an answer from the device it needs to be connected and in turn, it's gets answered by ACK packet that ends the whole phase of connection establishment. But in case of any maleficent intention, the attacker sends ACK

bit enabled packet having forged source address which gets dropped by the target device as it does not have any established connection to the host having spoofed IP address. This requires processing of each incoming packet which, in turn, leads to resource depletion.

In SYN flood, the attacker sends SYN packet to the targeted device at the high rate for starting up the three-way handshake process [31, 35]. He gets answered by SYN + ACK packet in response from the targeted device. However, the attacker does not send the required ACK packet intentionally, making the whole connection as half open and targeted server is made to wait until there is ACK packet from the desired source address.

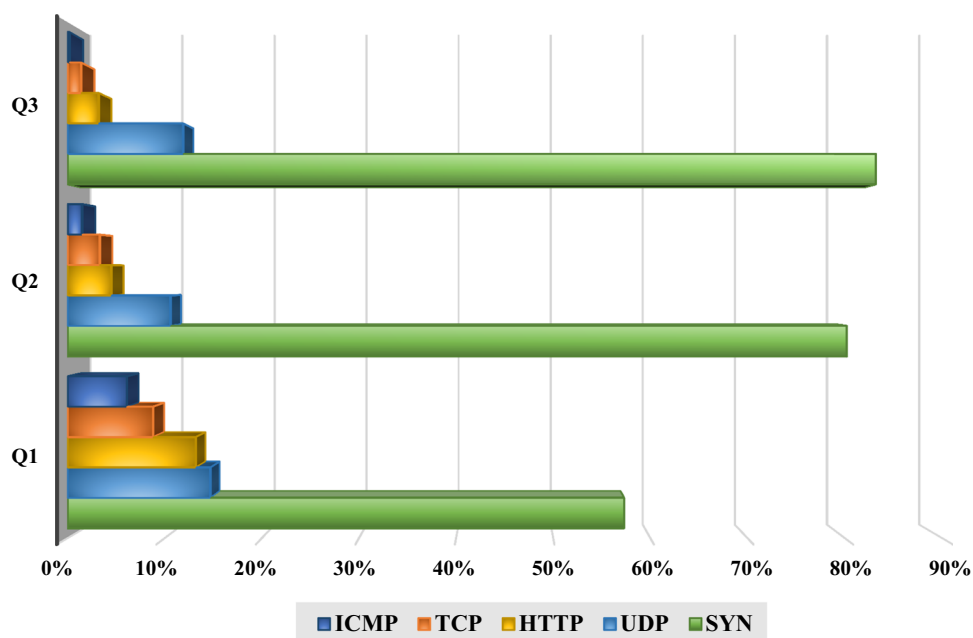
#### 4.2 Domain name server (DNS) amplification attack

In a DNS amplification attack, attackers use open DNS resolvers. They send DNS lookup requests with a spoofed source address to these resolvers. The DNS resolver responds to these packets by sending a DNS record response, which is sent to the target device instead of the device of the attacker [36]. Such a response is generally much larger than the query, which contains only the domain. A response can include many different records of information for a domain.

#### 4.3 Network time protocol (NTP) amplification attack

NTP protocol is used to synchronize the local and global clock over the internet. However, it can be used for launching DDoS attacks by requesting a query having a spoofed source address [37]. The address demands for the larger sized response like the list of last 600 connected hosts to the server which is used to determine the actual time in UTC. Such larger responses when generated frequently results into

**Fig. 4** Distribution of different types of DDoS attacks Quarter-wise (Q1, Q2, and Q3) in 2018



flooding and the server starts denying the further requests [37].

#### 4.4 UDP fragment attack

In this attack, the intruder sends false packets having a size big enough to fragment and then reassemble at the destination. The unsuccessful attempts to make these bogus packets reassembled and fragmented, make the device overloaded and hence the server denies to process other packets. This type of attack is sometimes termed as *Ping of Death* attack [38] as the attacker keeps on sending multiple malformed pings which when reassembled after getting fragmented exceeds the maximum length of the IP packet at the data link layer, hence making the memory buffers overflow causing a Denial-of-Service attack [31, 39].

#### 4.5 UDP flood attack

In this attack, intruder continuously tries to send the UDP packets to random ports at the target device anonymously. The target device is then forced to check each port to listen to the corresponding application but there is no such application, therefore it responds with an ICMP destination unreachable packet. This whole process makes the target device unreachable due to busy waiting.

#### 4.6 HTTP flood attack

In this attack, the cybercriminal abuses genuine HTTP GET or POST requests to perform DDoS attack [31, 32]. These attacks do not use spoofing or reflection techniques and hence

requires less bandwidth compared to other attacks to get fired into the targeted server.

#### 4.7 ICMP flood attack

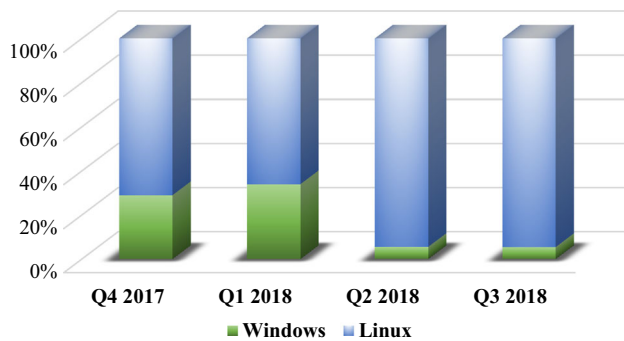
ICMP is usually responsible for generating error messages to inform the source about any failure that has occurred in the network or at the destination, like when the gateway is unable to buffer the data, or when a packet is not reachable to its destination. Ping function is performed in ICMP which initiates an echo request which is answered with an echo reply. If this reply is not received, it indicates that the other host is not active or does not have ping functionality. In that scenario, echo requests keep on being sent without waiting for the echo reply and flood the network by consuming the bandwidth unnecessarily [32]. It is also known as *smurf attack* [39].

#### 4.8 Zero-day DDoS attacks

This new term has recently introduced as one of the categories to separate out those unknown or new DDoS attacks which exploit the vulnerabilities present in the system. Now days, this attack has become popular amongst the member of the cybercriminals community [40, 41].

Figure 4 shows the statistics on distribution of most common types of DDoS attacks that have been recorded quarterly in the year 2018 [42]. Quartile 1 (Q1) has higher number of percentages for attacks namely ICMP, TCP, HTTP, UDP and SYN attacks as compared to Quartile 2 (Q2) and Quartile 3 (Q3). These data have been recorded by each quarter to obtain some comparable results. These attacks have targeted





**Fig. 5** Windows and Linux based botnet attacks quarter-wise (Q1, Q2, Q3 and Q4) in 2017–2018

millions of IoT devices to isolate the renowned servers which often covers large area of networks. Such incidents affect the reputation of the serving authority and become questionable on providing secure and reliable services to the users.

The infrastructure layer DDoS attacks like SYN, UDP, TCP flood attacks have got the highest percentage as compared to the application layer DDoS attacks. But on the scale of growth, HTTP GET flood attacks have shown the exigent rise from the previous year records.

Moreover, for the botnets that target devices running on some specific platforms like Windows, Linux, Android, etc., it has been recorded that Linux-based botnets DDoS attacks are getting more common in year 2018 as compared to the year 2017. Quartile 1 (Q1), Quartile 2 (Q2) and Quartile 3 (Q3) of the year 2018 show the significant decrease in the windows-based DDoS attacks subsequently in Fig. 5. This doesn't mean Linux lacks security as compared to other platforms. The Linux kernel and other components are also regularly updated to meet the latest threats like other system software [43]. In fact, being an open source software, it becomes easier to identify such threats. The main reason is that the vendors often release routers, consumer electronics, and IoT gear with outdated Linux kernels with either no or limited security protection. Moreover, IoT vendors do not offer kernel updates often, and if they do, there's usually no over-the-air (OTA) mechanism. In such cases, user must be sufficiently aware and motivated to keep their devices updated on their own [43].

## 5 Taxonomy of DDoS defence mechanisms in IoT network

There has been a number of proposals on defence mechanisms against DDoS attack from traditional defences to IoT based, specifically after seeing its wide range of variations in the recent past years. All such defence mechanisms for defending DDoS can be categorized into *Traditional DDoS defences* and *IoT specific DDoS defences* [44] as shown in Fig. 6. Traditional DDoS defences are applied on the target

server and the conventional systems basically homogeneous systems. IoT-specific defences [24], on the other hand, are applied to the IoT devices that are vulnerable to several IoT threats. These defence mechanisms are more sophisticated as they compromise of heterogenous IoT devices distributed across the network. Detection techniques are applied on both types of defence mechanisms to find out any abnormal activity either on the host or in the network. However, IoT specific defence is much focused towards detecting the intrusion by a malware which can result into formation of IoT botnets. Traditional DDoS defence also detects the presence of any such malicious software responsible for converting the host into a compromised host (Zombies) [38]. They also detect the unusual network traffic that leads to flooding in the network. Honeypots-based [45] and anomaly detection-based defence mechanisms employ host-based detection schemes whereas Learning automata [46] and software-defined networking methods [47] can be used for detecting the unusual traffic. *Prevention based defence* mechanism is concerned towards avoiding any malicious intrusion into the IoT device. Regulatory solutions [25] and IoT middleware solution are the examples of prevention based DDoS defence. *Mitigation* techniques intend to reduce the effect of flooding of the network. They do not focus on the origin of the problem, hence do not employ any sophisticated detection technique rather concentrates on lessening the problem size by elimination.

### 5.1 Learning automata based DDoS defence [46]

Learning Automaton based solution was proposed to prevent DDoS attacks in IoT networks that work on a Service-oriented Architecture (SOA), that is used as a system model. A cross-layer model has also been proposed for dealing with such attacks at each level of network architecture.

This approach uses three phases for prevention DDoS Attack: (i) DDoS Detection, (ii) Attacker Identification, (iii) DDoS Defence. The first phase detects the attack by defining a threshold value that is a maximum value of servicing capability determined as per the computational resource availability. If the number of service requests surpasses the limit, a DALERT (DDoS Alert) is issued which gets propagated with help of immediate neighbors. That starts the next phase which identifies the attacking device by finding out the device id sending a much greater number of requests than others. Moreover, this entire hacker's information is transmitted using a packet which embarks the next phase to defend it against the attack. Now after having all the information about the attacker, all the incoming packets from the attacker's device easily get discarded if it fails to be legitimate during sampling. The packets are sampled to determine the authenticity of the whole range of packets. Due to the unfeasibility of checking all the incoming packets, sampling is performed by using a learning automata concept which

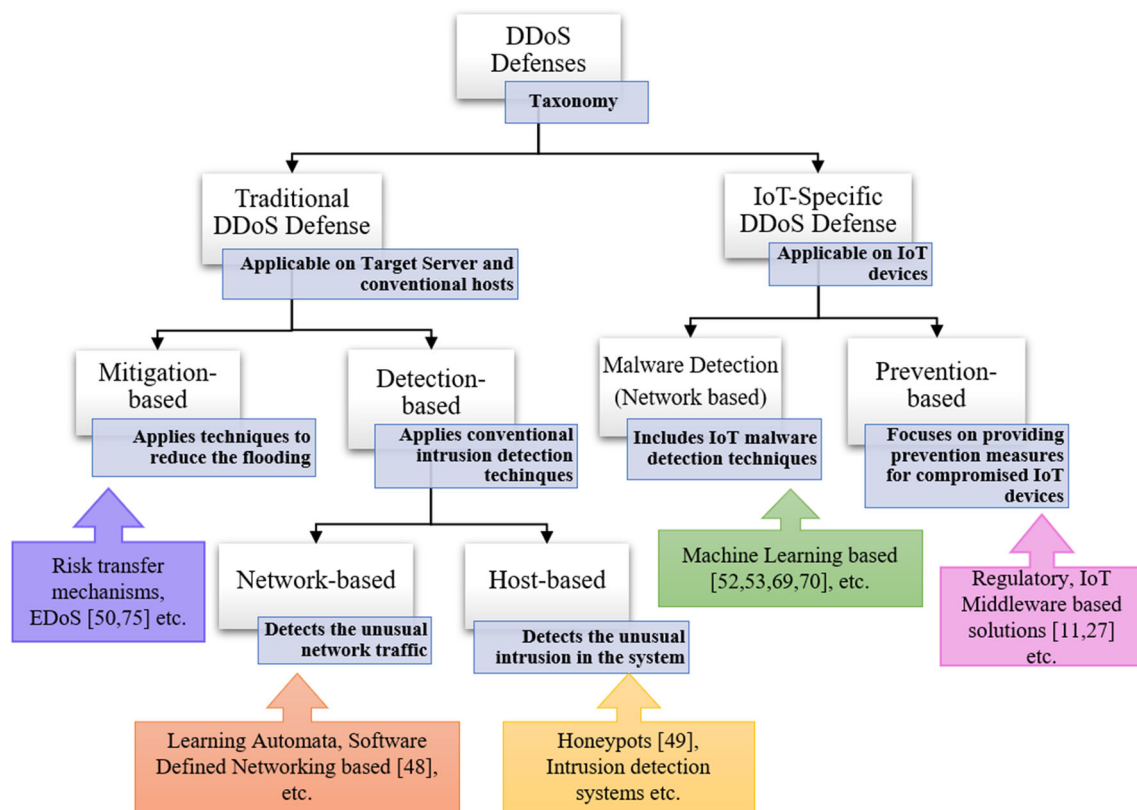


Fig. 6 Taxonomy of DDoS defence mechanisms

is used for establishing the optimum sampling rate. Due to the rejection of requests sent by an attacker during sampling number of requests at the server get reduced and hence nullifying the effect of the DDoS attack.

## 5.2 Honeypots based DDoS defence [45]

In this proposed scheme, honeypots are used as a trap for the intruders intending to harm the security of the system. A honeypot, as its name suggests, used for luring in attackers with an intention to observe and analyse their method of launching an attack by capturing information about the attacking agent like malware [45]. The whole model is described by two scenarios in case of any DDoS attack is suspected as shown in Fig. 7. The first scenario depicts the detection of the presence of anomalies in the incoming request to the server with the help of the intrusion detection system and if any such request is found, then it is targeted to the honeypot instead of the main server. The information about the suspect (which can be an attacker) containing its IP address, MAC address, etc., is stored as logs in the database with the help of honeypot. Once the logs get collected in the database, on further detection of any such request by IDS, the information of client request is checked against stored log files. Based on the results, a verification request is made on the behalf of the

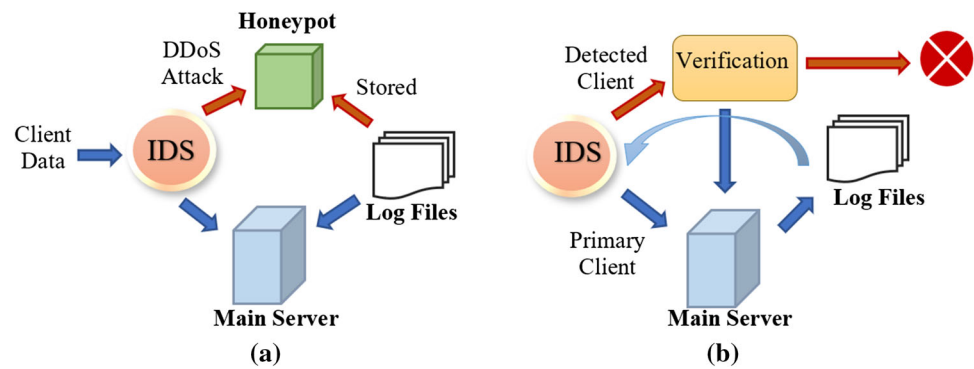
main server to the client for checking its authenticity. If it comes out as a spam, the client is blocked completely by the main server at the requesting stage itself. On the other hand, if the client is passed, the request is proceeded to next stage i.e. it gets serviced by the main server.

## 5.3 Risk transfer mechanism-based defence [48]

A risk transfer algorithm was proposed for handling the risks involved during the DDoS attack in a smart home environment. It constitutes a third party which is responsible for transferring the risk to its own in case of any such attacks get identified in the network, especially for the largely scaled attacks. The inclusion of the third party should only be made on an economic incentive-based agreement between the IoT device owner and the third party. This mechanism was centered towards high rated attacks to which normal IoT device is not able to counter due to its resource constraints characteristics and inadequate security mechanisms [49]. Low rated attacks can easily be handled at gateway router level by dropping such packets instantly before it reaches to all the connected devices, which is a very traditional way of defending DoS attacks.

A risk transfer algorithm is implemented on the gateway router as a defence mechanism for high rate attacks.

**Fig. 7 a** Honeypot is used to collect attack features into log files in case of DDoS attack.  
**b** Log files are used for matching against further suspected intrusions



The detected malicious packets for which the gateway router becomes incapable to handle, get transferred to an Economic Denial-of-Service (EDoS) Mitigation server under the third party. The whole simulation was modeled using PN2Sim.

#### 5.4 Blockchain based DDoS defence [50]

This proposed method uses the blockchain which is an online distributed ledger having a list of blocks containing a hash of the previous block along with an orderly recorded timestamp. These blockchains are used for the self-executable computer programs called Smart contracts. The smart contract in the system is responsible for facilitating secure communication between the IoT devices and the distributed servers. One of such smart contracts is called Ethereum, one of the largest online established software platforms. It allows smart contracts and decentralized applications (DApps) to be built on blockchains along with their state. State in Ethereum refers to the data present in the blockchain and a state transition occurs when a transaction happens. Ethereum has a gas limit attribute to ensure that no further resources can be consumed once the limit is exceeded. This limit is set for each transition processed through it which prevents the system from getting overloaded. The word ‘gas’ used here is analogous to the word “resource” in Ethereum terms i.e. a certain amount of gas for a function refers to the number of resources a function has for its execution.

Blockchain has been used here because of its transparent and decentralized approach of storing the data all across the network. Figure 8 shows the IoT blockchain system for defending DDoS [51].

#### 5.5 Software defined networking based defence [47]

In the row of defending DDoS mechanisms at initial stages, a yet another mitigation technique has been proposed that uses the concept of software-defined networking-based infrastructure in order to control the propagation of DDoS attacking agents before reaching to endpoints firewalls or other anomaly detection systems itself. The efficiency of the SDN

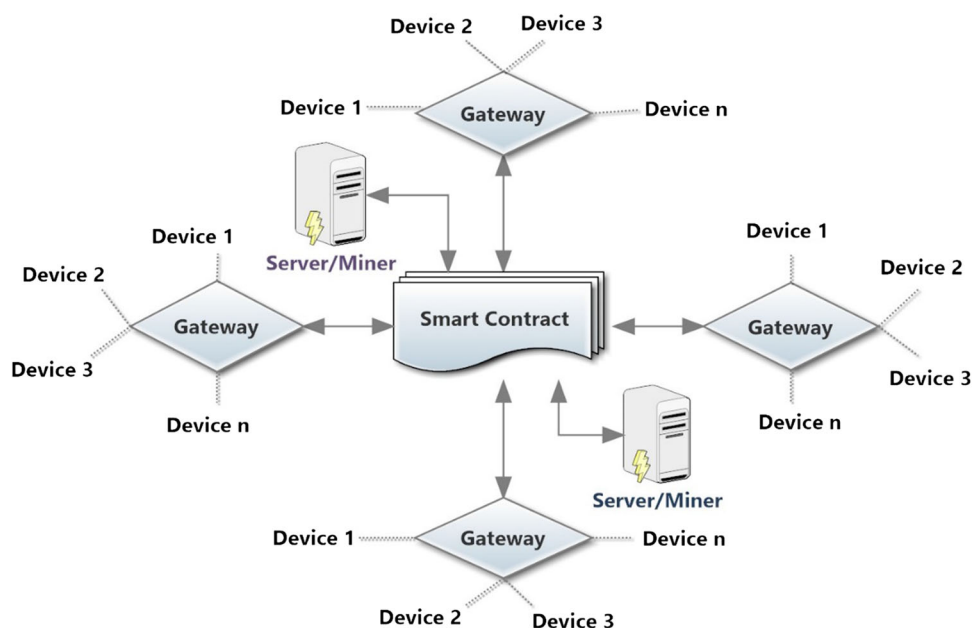
infrastructure lies in its features like software-based analysis, local centralized control, dynamic flow insertion, etc., which in all contribute to an effective DDoS mitigation system. It also helps in reducing the network congestion and prevents malicious IoT devices from amplifying the attack at compromised server/host. The SDN architecture works differently from the traditional network infrastructure by isolating the network control from data (forwarding information). Thus, making the network control to be able to be programmed directly as shown in Fig. 9. The control intelligence is taken care by a centralized controller that is capable of understanding the complete topology of the network. Unlike, tradition routing where the incoming packets get destined by looking up into the routing table, the SDN architecture has the ability to dynamically manipulate the traffic flows or packets flowing in the network with help of a controller. The SDN infrastructure can be extended to SDNi in order to interface between multiple SDN domains so that information sharing can take place among SDN controllers of multiple domains. An open flow protocol is used to allow open flow enabled switches (OF-switch) containing internal flow tables, to be managed by the controller. In case, the flow entry of a packet is present in the flow table of OF-switch, it gets forwarded normally, otherwise, sent to the controller for further analysis. SDN controllers have the reasonable computational power to monitor traffic flows. Traffic analysis can be performed in real time using machine learning algorithms (Support Vector Machines (SVMs), Gaussian Mixture Models (GMM), Artificial Neural Networks (ANNs)), databases and any other software tool.

Different types of DDoS attacks mitigation have been described using SDN architecture:

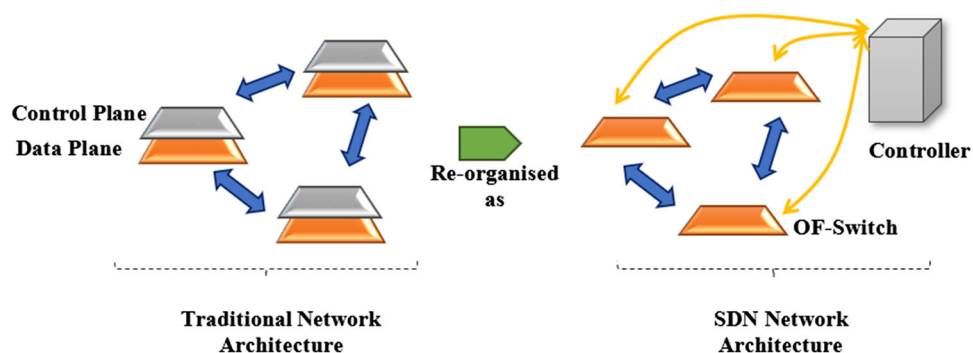
For *Source based attack*, SDN controllers can be used to detect the anomaly in the traffic and can alter the packet near the ingress of the network correspondingly.

For *Network attacks*, controllers, also called network operating systems (NOS) can be used to control the whole SDN network globally in terms of the packet flow. Any deviation from the normal behavior in the network traffic flow among the devices can easily be detected by the controller and gets

**Fig. 8** IoT blockchain system model



**Fig. 9** Traditional network architecture versus SDN network architecture



followed by the application of the pre-emptive measures to prevent the attack.

For *cross-domain attacks* that involve transitioning from one network infrastructure to another, SDN infrastructure exists parallelly with tradition IP network to exchange reachability information and to forward traffic along with other cooperative functions. Hence, detection of such attacks triggered from geographically located IoT devices becomes effective and easier to mitigate.

### 5.6 An IoT middleware based DDoS defence [12]

The defence is specifically designed for IoT devices. The architecture proposed includes a flexible and working cross-domain middleware, called as NetwOrked Smart Object (NOS). NOS is responsible for receiving the open data feed from the remote sources in an IoT environment in real time as shown in Fig. 10. It is composed of a typical IoT system having nodes that may be taken as heterogeneous data sources like RFID, NFC, actuators, sensors, etc., and the users who interact with the IoT system by accessing the data through

IoT devices. It provides a lightweight and secure information exchange based on an authenticated publish and subscribe mechanisms, using the Message Queue Telemetry Transport (MQTT) protocol. In order to ensure that the established policies have been applied correctly, the whole process under NOS is monitored by the Enhancement framework. The interaction among the components of NOS takes place through an openly accessible RESTful interfaces. Node.js platform is used for developing NOS's core operations.

Apart from traditional networks like WSN's and MANET'S for which several ad hoc solutions have been proposed, this particular solution is proposed specifically for IoT platform and its resources. The whole process has been described by taking help of different scenarios. The general scenario is composed of multiple NOSs as depicted in Fig. 11 deployed in a wide area that makes heterogeneously located data sources to connect to the closer NOS easily. For a source that wants to send data to one of the NOS, it has to connect itself to the public port.

These public ports are constituted by each NOS has in order to allow the data connectivity using HTTP. Positive



Fig. 10 NOS architecture

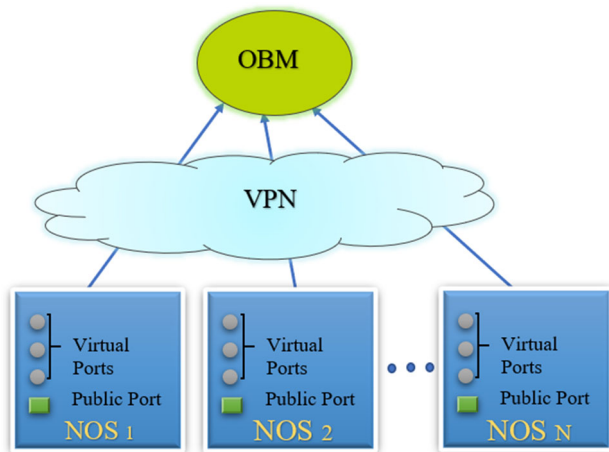
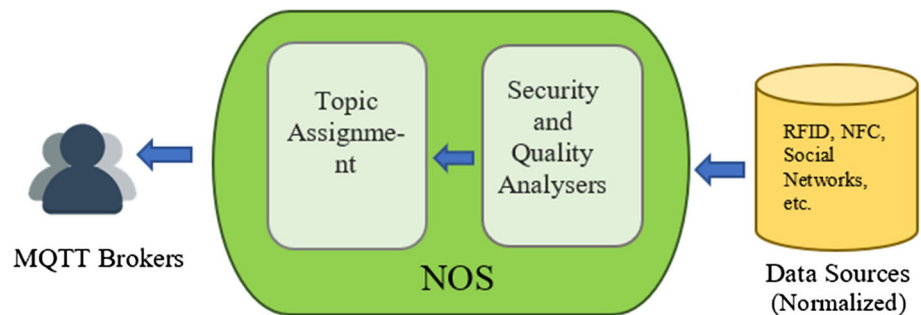


Fig. 11 General scenario for multiple NOS's

response received from the NOS, in turn, will allow the source to provide its information in encrypted form, in case if it is a registered source. To prevent the resources from getting waste unnecessarily in case of a DDOS attack, a number of dynamic ports depending upon the number of connections, are created on each NOS. These virtual ports are used for switching among the set of active connections. A unique identifier is randomly generated (UID) and assigned to each NOS by another new IoT network component called Overload Balance Manager (OBM). OBM act as a remote server which is connected to all the NOSs in IoT network system by mean of a secure virtual private network (VPN). This UID when gets bound up with the name of the virtual port results into a unique address that is much more complex to guess by the malicious entities. Altogether, each NOS can react to following cases of attempting a DDoS attack as described as:

*Case 1: Number of connection requests increases:* The connection requests are denied by NOS throwing an exception regarding unavailability of resources if the number of connection requests exceeds the certain dynamically calculated threshold.

*Case 2: Number of packets sent increases:* For this case too, packets sent towards the same port address of NOS

by the same requester are denied for a certain threshold. In this way, useless information is avoided from getting unnecessarily analyzed and processed.

*Case 3: Malicious entity knows the whole address of the ports:* If some sources continue to overload the network with the useless traffic on the known port address even after dropping of those and closing of sessions, then all the active connections are exterminated on that particular port and the port is renamed by providing it with a new port number.

*Case 4: Malicious entity knows UID:* If an attacker somehow got to know about the UID of one of the ports only, then it is quite possible to derive more than one active virtual ports by just concatenating it with the name of the virtual port which, in general, is just a sequential number that can be revealed by brute force. To handle such situations, the actual victim i.e. the NOS, itself is allowed to move to another location aided by OBM to start up a new instance of same NOS by replacing the UID with a new one.

*Case 5: Compromised sources continue to consume the network's resources:* Besides having above-mentioned countermeasures, the compromised sources do have enough potential to exhaust the network resources (bandwidth, CPU, and memory) by generating the bogus packets or not sending the requests to the NOS directly, etc. In order to deal with it, the solution under case 4 can be extended to get the solution for this case. As soon as the OBM gets informed about any benevolent activity, it starts up a new instance of the NOS, but this time situated on the physically separated network with respect to the previous one, hence isolating the compromised network from NOS network.

These situations reveal possible vulnerabilities of the NOS system. Hence, there is a need to explore out straightforward and more organized ways to detect and prevent the various attempts of DDoS attacks to IoT system.

## 5.7 Machine learning detection based DDoS defence models

Due to advance benefits of using machine learning approaches for classification, it's now has become one of the



most prominent detection techniques used for malware detection in DDoS. Following are the recently proposed detection techniques that can be used for an effective DDoS defence:

### 5.7.1 Image training to detect IoT malware botnets [52]

A light-weight approach for detecting DDoS malware is proposed specially which are evolving in the IoT environment. The concept of image processing is used to recognize and then analyze different malware behaviors. The process starts by first extracting one-channel gray-scale images converted from binary files of malware, and then utilizing a lightweight convolutional neural network to distinguish among different IoT malware families. IoT malware somewhat behaves differently from the regular malware by the fact that it tries to kill other malware to capture enough computational resources for itself.

For a lightweight classification system, convolutional neural network (CNN) is used as it doesn't use any training data unlike other classifiers like SVM and K-nearest neighbors. Cloud servers have been used for deploying malware filters to overcome the IoT constraint of being limited by resources as well as by memory [53]. Another advantage is that cloud servers provide better protection against node failures due to DDoS attacks and frequent malware database updates would also take place easily as compared to in IoT devices. Therefore, a two-tier detection architecture has been provided with the remote cloud-based classification system that first recognizes the suspicious programs (binaries) locally then it is forwarded to the remote cloud server to analyze it deeply. Cloud servers are also responsible for updating and distributing newly trained detectors to the clients periodically.

In order to perform the classification, a binary image of malware is reformatted as an 8-bit sequence and then converted to a grayscale image having one channel and pixel values ranging from 0 to 255. The resultant image is then provided to the machine learning image classifiers as an input. The process is shown with the help of a sequence diagram in Fig. 12.

This machine learning method is much better than a traditional signature matching method for detection due to its fast processing as it only requires the 8-bit vector convert the malware binaries to the corresponding images as an input to the CNN. CNN has come out as better and efficient classifier amongst other kinds of classifiers due to its deep learning based automatic feature extraction process along with having a better test efficiency compared to other algorithms.

### 5.7.2 An IoT middlebox with machine learning based detection [54]

This proposed machine learning solution for defending DDoS has incorporated smart Home LAN with a gateway

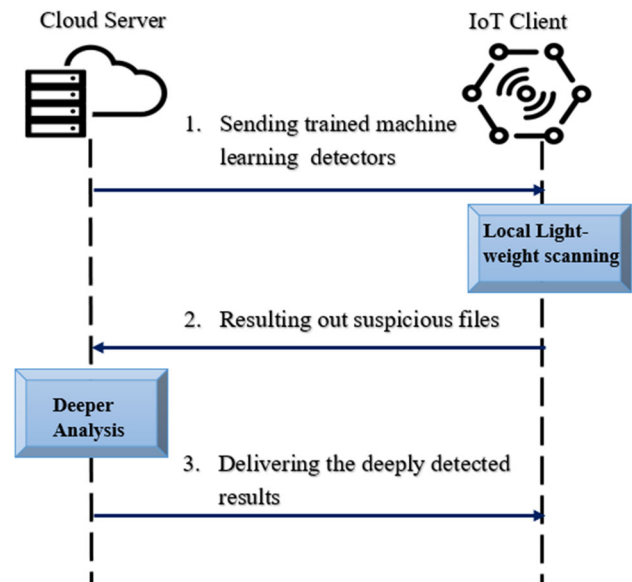


Fig. 12 A lightweight malware detection sequence

router (middlebox) to observe the traffic between the consumer IoT devices and the internet. It has utilized IoT specific network behaviors like the limited number of endpoints, the regular time interval between packets, etc. to perform feature selection process to achieve the higher accuracy in detecting DDoS in IoT network traffic with the assistance of various machine learning algorithms, including neural networks. Anomaly detection is the process that goes via different phases starting from *Traffic Capture*, then on *Grouping* the packets by device and time, and then coming on the *Feature Extraction* phase and finally ends on *Binary Classification* phase. The traffic capture process is about recording the source IP address, source port, destination IP address, destination port, packet size, and timestamp of all sent IP packets from IoT device that is a part of some smart home application. This task of collecting the DDoS traffic is actually a quite challenging task due to some involved security risks and complexity. The proposed method has simulated the three most common variations of DDoS attack i.e. a TCP SYN flood, a UDP flood, and an HTTP GET flood.

Grouping is performed on packets from IoT devices on the basis of source IP address which is further divided into nonoverlapping timestamps which were recorded at the earlier stage.

The feature extraction process is responsible for generating stateless and stateful features for each packet depending upon the IoT device behavior. Stateless features are lightweight features derived from flow independent characteristics of each sent packet i.e. they are actually generated without splitting the incoming traffic stream by IP source. On the other hand, stateful features are about capturing the aggregated flow information in the network traffic with respect to

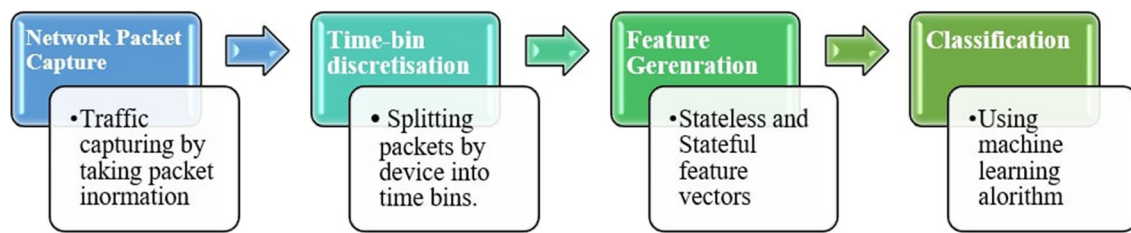


Fig. 13 Process flow for machine learning based DDoS detection

the short time spans. Packet size and inter-packet interval are considered as stateless features whereas bandwidth and IP address cardinality and novelty are called stateful features. At last, binary classification is processed using different classification algorithms like K-nearest neighbors, random forests, support vector machines and deep neural networks to distinguish the normal traffic from the DDoS traffic flow [55]. Among which k-nearest neighbours and decision tree algorithms were found to be most accurate. Figure 13 shows the complete flow of the processes involved.

### 5.7.3 Network based anomaly detection in IoT using deep learning [56]

This recently proposed method uses the deep learning models to detect the anomalies out of the IoT network. Deep learning models are considered best among most of the classification algorithms in terms of the accuracy and precision because of its dense and complex architecture with multiple layers to train, test, and predict the units [57]. Hence, this method can be taken as an extended version of machine learning based defence techniques. To incorporate these techniques in an IoT network, deep autoencoders [58] are used for each type of IoT devices separately in the network. These autoencoders are able to learn the behaviour of different IoT devices with different functionalities effectively with help of their statistical features in the form of snapshots. The advantage of using autoencoders is its ability to encode and compress data which fits perfectly in the picture when dealing with IoT constraints. The captured snapshots of the usual IoT traffic gets compressed by autoencoders. The suspicion in the traffic is detected when autoencoder is unable to reconstruct the recorded snapshot back to the original form. The proposed method was able to achieve lesser false positives in compared to other machine learning algorithms.

## 5.8 Some other DDoS defence approaches

There are many other ideas and concepts that have been evolved as having an adequate potential to fight against DDoS attacks. An IoT DDoS defence algorithm was proposed for IoT end network to prevent, measure and avoid DDoS attacks [59]. As per this algorithm, all the nodes in a typical IoT

end network can be broadly categorized into working nodes, monitoring nodes, legitimate and attacker nodes. Working node, which is normally closer to the end user, is responsible for collecting data and executing simple related tasks. However, this approach has used working node itself to detect malicious requests objected towards the target device. The functions of this node are redefined keeping it's all constraints in view like limited memory, storage, and power supply characteristics. Light weighted and inexpensive attack detecting mechanism is incorporated with it and is carried out in two stages called request serving stage and defending itself from attacks stage. In request serving stage, working node serves the validated requests while rejecting other requests waiting for the service. In addition, it doesn't allow queuing of rejected requests to provide simplicity in the process. As a result, it leads to open up the competition over a limited service that is to be won by the user who requests frequently. The frequent user could be an attacker in case of a DDoS attack. In the next stage, the working node needs to distinguish between malicious and legitimate request by observing the content of the requests. If the content is meaningless and coming from the same sender, it gets blocked by the working node itself and the bandwidth is freed to serve other legitimate requests. The implementation of the proposed solution includes maintaining a list of records of the served request containing details like sender address, the most recent request content, and a flag to mark whether a sender has been determined as an attacker. On detecting the repeated request content or true flag, the request gets refuted by the working node, hence making the bandwidth free for other requests.

Another approach [60] used to identify DDoS attacks in IoT network is by availing the services to legitimate users and blocking unwanted ones. It has used agents cum software-based managers between the network and gateway or border router. These agents were responsible for identifying the attack by maintaining two special access control lists, greylist, and blacklist that get updated every 40 s and 300 s respectively with giving or revoke access toward IoT network either temporarily or parentally. Updating the greylist takes quickly to easily remove if any false identification has been made from the temporary blocked state to make it able to access the resource again.

Some *regulatory solution* [25] to the IoT security has also been proposed that uses the openly available Mirai's botnet code [61]. Modifications to the code are done to make it work against the attacker's intent. The piece of code which was previously there to terminate the other botnets and the one which was kept there to hide the running bot from the owner of the device, are removed for the sake of simplicity. To identify the bot as law enforcement or government proxy, a clear text string is added, and some code is inserted to log this string to the local information Syslog facility. The code associated with attack functions is also removed in the Mirai derived bot. The scanning code is left intact. The server code is modified to nullify the attacker's ability to use the botnet as an attack platform. In fact, when a new vulnerable device is reported by bot, with getting compromised by command and control server, it also gets added to the server's database. Thus, information stored is used by a government agency or law enforcement for notifying the concerned network owner of the vulnerability of the discovered device in the network via an email or any other secured communication medium. The concerned network administrator can then take necessary actions for combatting against incoming threat to the vulnerable device. A written notification of the number of devices in violation is then also sent to each manufacturer by the appropriate government authority. Hence, the modified botnet is designed and operated in such a way that it can be used by government and law enforcement agencies to motivate internet service providers (ISPs), manufacturers, and owners of IoT devices with an intention to inform them about their vulnerabilities prior to any attack.

Defending against attacks at early stages i.e. before it reaches to end level IoT devices, is always preferred than tackling with it in later stages. Another solution [62] that incorporated the above idea for securing IoT devices connected to the personal or specific network via a border router. It consisted of two components named analysis and monitoring. During analysis, it observes the incoming traffic to decide the authenticity of the packets and while monitoring, it categorizes the suspected traffic into DoS or DDoS attacks. The algorithm is designed to work on two levels. The first is about performing several checks on the incoming traffic and then at the second level, the suspected packet gets monitored by another component i.e. Monitoring. To defend severe and high amplitude attacks, Economic DOS (EDoS) server [63], i.e. a risk transfer mechanism [48] with the cooperation of a third party, is introduced to overcome the restrictions of an IoT environment in case of high amplitude attacks. All the packets received from the external network at the border router get accessed by the analysis component and the packets from the blacklisted sources are dropped. For the packets from non-blacklisted sources, the bit rate is checked to allow those having a standard bit rate. Rest of the packets are treated as malicious and are handed over to the EDoS

server. The monitoring module gets invoked by the analysis module in two cases, first when the incoming packets are from grey listed sources i.e. exceeding the threshold payload size. If these suspected set of packets are originating from the single IP address and have repeating characteristics, then they are considered as part of a Denial of service attack and consequently, the corresponding IP address will get added to the blacklist. In the case of the suspected set of packets having similar characteristics and are coming from different sources, the scenario is acknowledged as a distributed DoS attack. The corresponding IP will get added to the greylist after dropping these packets. This is the second level when the packet gets passed to monitoring module confirming to an attack on basis of the similarity between current and previous packets from the suspected IP that leads to moving it to the blacklist finally.

The solutions discussed in this section are distinctive in their approaches as well as are limited in terms of their applicability and scope, hence needed refinements to cover more attack scenarios. The use of EDoS server discussed above in one of the solutions in this section, is just an instance of risk transfer mechanism (Sect. 5.3). However, regulatory solution which uses Mirai's bot code is included in our comparison we made amongst main and effective DDoS defence approaches as we found it one of the innovative approaches against the biggest Mirai's DDoS attack recorded yet (refer Sect. 3.1).

## 6 Comparative analysis of existing main DDoS defence and detection mechanisms

In order to derive insights required for an optimal defence solution against DDoS, all defence mechanism that we have discussed in the Sect. 4 need to be critically analyzed. Table 3 presents the defence solution with their proposed system model, advantages as their key points and vulnerabilities to decide their future scopes in defending the newer trends in DDoS attack. Moreover, the types of attack which are targeted by these defence mechanisms are also mentioned in the table. Most of the traditional methods are not able enough to detect and mitigate application layer attacks whereas machine learning based solutions work on such attacks actively with the help of efficient and light weighted classification algorithms. This is the main reason why machine learning solutions perfectly fits to the current needs of IoT security.

Machine learning based defence models have become a trend in defending against an DDoS attack. Due to their ability to detect and predict against millions of network intrusions accurately with compared to other mitigation and prevention-based defence mechanisms, they are capable enough to deal even with IoT vulnerabilities effectively. The recent researches in the context have experimented numer-

**Table 3** Comparison of recently proposed defence mechanisms for DDoS attack

Defence mechanisms	System model used	Key points	Vulnerabilities	Main target attack types
1. Learning Automata based DDoS Defence [46]	Service Oriented Architecture (SOA) along with a cross-layer model for adaptability to all the layers of the network model	Learning automata are used for determining optimum sampling rate Applicable to all the layers of the network model due to its cross-layered architecture	The solution is more focused over achieving optimality in sampling but it somewhere lacks in dealing the attack Sampling is a lossy and a biased process for predicting entire network traffic	Replication and amplification attacks (UDP/TCP floods, ICMP floods)
2. Honeypots based DDoS Defence [45]	Intrusion detection system with a decoy computer system called a honeypot	Anomalies get redirected to the honeypots instead of the main server Can be used for understanding the nature and attack vectors for unknown malware	The framework discussed can't be implemented over a real-time environment but can be achieved using microcontrollers interfaced with a central server Incapable of handling DDoS attacks incorporating botnets	HTTP flood, DNS service attacks Protocol-based Attacks (ACK/SYN floods, Ping of Death, Smurf DDoS)
3. A risk Transfer mechanism as a DDoS Defence [48]	A smart home environment with an inclusion of an authorized third party (Economic DoS Server)	Low rated attacks get resolved at router level itself High rated attacks are transferred to the third party treating them as possible threats	Specifically concentrated over the smart home environment	Protocol-based Attacks (ACK/SYN floods, Ping of Death, Smurf DDoS)
4. Blockchain concept-based Defence [50]	Blockchains are used as the self-executable computer programs called Smart contracts	It allows smart contracts and decentralized applications (DApps) to be built on blockchains along with their state	Gateways/routers are assumed to be uncompromised which is unrealistic in case of IoT DDoS attacks Incapable of handling advance versions of botnets	Application Layer Attacks (HTTP flood, DNS service attacks)
5. An IoT Middleware based DDoS Defence [12]	An IoT architecture with a working cross-domain middleware called NetwOrked Smart Object (NOS)	NOS receives the open data feed from the remote and heterogeneous IoT sources in real time Lightweight and secured information exchange based on an authenticated publish and subscribe mechanisms, using the Message Queue Telemetry Transport (MQTT) protocol	Lacks in a more complex environment, composed of multiple NOSs having a huge number of data sources and malicious entities	Protocol-based Attacks (ACK/SYN floods, Ping of Death, Smurf DDoS)
6. Software Defined Networking based Defence [47]	Software-defined networking-based Infrastructure with an extended version SDNi for dealing with multiple SDN domains	Prevents the attack from reaching it to the endpoint firewalls or other anomaly detection systems Reduces the network congestion Prevents malicious IoT devices from amplifying the attack at compromised server/host	Poses a security threat due to its centralized control paradigm	Application Layer Attacks (HTTP flood, DNS service attacks)



Table 3 continued

Defence mechanisms	System model used	Key points	Vulnerabilities	Main target attack types
7. Regulatory solution to the IoT Security using Mirai's botnet code [25]	The openly available source code of Mirai's botnet (i.e. injection of Mirai malware) and some government agency or law enforcement to regulate the behavior of the code	Modifications are performed in the code such that the authorized government body can detect the compromised IoT device Notifications are sent to the concerned owner about its vulnerability	Requires a proper placement of an appropriate legal framework in the respective administration along with updating the redressal methods used by administrators specific to the underlying concept	Protocol-based Attacks (ACK/SYN floods, Ping of Death, Smurf DDoS)
8. Machine learning based defence models [52, 54, 56, 58]	Supervised and unsupervised learning models [78] along with neural networks to detect and predict the anomalous behaviour in the network	Ability to predict the future attacks with a smaller number of false positives/negatives comparatively with other defence models Suitable for detecting both traditional as well as IoT malware due to various kinds of classification algorithms	Accuracy or precision is directly proportional to the quantity and quality of datasets used to train the model	IoT botnet-based Attacks, and other malware attacks

ous detection techniques using different machine learning classification algorithms like K-nearest neighbours, SVMs, Deep Learning, Random Forest, Neural networks etc. [54, 56]. Table 4 presents the comparison among some of the recent and efficient DDoS defence models with respect to the two key processes in the machine learning flow i.e. Feature extraction and classification along with their limitations:

Detection is the crucial part of any defence model as it becomes the basis of further classification of anomalies in the network. As per the discussed taxonomy of defence mechanisms in Sect. 5, detection-based defence systems are most capable to deal with the attack because they are less dependent on any other parameter like third party or any regulatory system as in other two types of defence mechanisms. They can prevent any harm to the system by detecting and boycotting any unusual activity on their own. Moreover, when we talk about IoT specific DDoS defences, we are much concerned with the malware detection rather than any anomaly detection. Anomaly detection is different from malware detection from the fact that anomaly is just an alteration in the normal behaviour whereas the malware has its own features and characteristics which may be similar to that of the system and needs to be identified with proper detection technique. The above-mentioned defence methods use different detection and classification methods for the DDoS anomalies in the traditional network as well as in the IoT network. Table 5 presents the various detection techniques that have been employed in these defence systems:

## 7 Open research issues and challenges

DDoS detection and its defence are now emerging as an active area to research out possibilities on how to deal with today's modernized world embellished with Internet-of-things. Researchers and security analysts are now more focused on putting their best efforts for finding the new possible ways to fill the existing security gaps in IoT by confronting the evolving issues and challenges [64]. Following are some issues and challenges that should be taken into account when upgrading the security mechanism for DDoS defence in IoT:

### (a) The realization of real-time scenarios of an IoT environment:

Most of the proposed methods of mitigating DDoS do overlook the real-time scenarios in an IoT environment in achieving the desired efficiency. Such a trade-off should not be appreciated when defending the IoT device against DDoS malware [65]. Algorithms are needed to be designed by keeping as many as possible of the IoT constraints and vulnerabilities in view, to better capture the real-time conditions to improve its applicability to various possible situations.



**Table 4** Comparison of recent machine learning based defence models for DDoS attack

DDoS defence models	Features extraction process	Classification algorithms	Limitation
1. Image processing based training [52]	A grayscale image converted from the 8-bit vector from the binaries of the malware is used as input to the CNN	A Lightweight Convolution Neural Network (CNN) used to detect malware	Network optimization is needed to reduce the complexity created due to unnecessary links More detailed features should be selected in order to improve accuracy
2. Network based anomaly detection in IoT using deep learning [56, 58]	Use of statistical features of a benign IoT network traffic Ability to compress the captures features into snapshots make it suitable for IoT devices	Deep autoencoders are used to train themselves on their own with the normal IoT traffic network behaviour Accurate results due to its multi layered architecture	Results into overhead in maintaining autoencoders for each type of IoT device separately
3. An IoT middlebox with machine learning detection [54]	Smart Home LAN with a gateway router (middlebox) to observe the traffic between the consumer IoT devices and the internet Use of stateful and stateless features based on network behavior Routers having lightweight features to handle high bandwidth traffic	K-nearest neighbours and decision tree algorithms were found to be most accurate Flexibility with a variety of protocols (e.g. TCP, UDP, HTTP, etc.) Low Memory Implementation of routers	Use of smaller datasets in an un-realistic environment Use of less accurate machine learning algorithm

**Table 5** Detection techniques used in various defence mechanisms for DDoS attack

Detection techniques	Benefits	Limitations	Used in (defence mechanisms)
1. Network Flow Sampling [46]: This technique uses sampling of one per N packets (depending upon sampling rate) in the typical network configuration. Based on the header properties it detects the abnormal flow	Due to its <i>storage efficiency</i> (considers only header data), it is useful for the analysis of common patterns of the malware infected packets in the long run [79]	Sampling fails in the <i>IoT network configuration</i> as one infected IoT device will send one packet per sampling session which is a lossy process for predicting the entire network traffic Capturing only the header data make it incapable of detection today's <i>new malware variants</i>	Learning Automata based defence mechanism [46]
2. Packet Capturing: The whole packet is captured to store all the network-based properties of malware infection [80]	Useful in analysing <i>Darknet</i> traffic as packet size is less with no privacy concerns	Requires enough resources and storage space to store all the captured information Costlier process	TCP/SYN Flood DDoS Attack Defence, Botnet specific DDoS defence [54, 58]
3. Machine Learning Algorithms [52, 54, 56] Machine learning models are used for detection of abnormalities with desired accuracy	This works even without specific labels of classifications due to unsupervised learning Faster as compared to rule-based detection	Desired accuracy and precision can be achieved but at the cost of increased memory space and resources	Machine learning based and image processing based defence models [52, 54, 56]
4. Honeypots (Traditional/IoT) Honeypot which imitates the real vulnerable system to attract the malware intentionally, is used to detect the malware attacks [47]	Appropriate for capturing the newer coming variants of malware behaviours, especially IoT malware	Low interaction honeypots can be easily identified by any high featured malware Installation of high interaction honeypots requires significant number of resources	Honeypots based DDoS defence systems [47]

### (b) Dependency on network conditions and other user parameters

Designing the defence algorithms with least reliability on network conditions as well as on user parameters is another issue [66]. The number of assumptions on network conditions should be kept a minimum in order to consume the more realistic aspects of IoT.

### (c) Quantity and quality of datasets used

The existing methods especially those which are based on a machine learning approach are mostly dependent on the quality as well as the number of datasets used for training and testing the algorithm [67]. Therefore, assuring the sufficient amount and the high quality of the data would help to improve the accuracy of the results for the detection of anomalies and reduce its influence on the performance of the proposed solution.

### (d) Lack of standardization in IoT framework.

There is no standardized framework for IoT which has a very vital role in understanding the organization and operation involved clearly [68]. Though there has been the number of proposed frameworks that have layered architecture, a proper reference is needed in order to deeply understand the existing vulnerabilities and initiate as well as evaluate the process of finding the possible solution.

### (e) Protocol-based detection for anomalies.

Most of the surveyed defence mechanisms till date are based on protocol oriented and hence they are only capable of dealing with the attacks that make use of some fixed protocols [69]. These methods become specific to some selected protocols and therefore become incapable of handling other types.

### (f) Ability to detect and mitigate unknown attacks in IoT

Applicability of the most of the defence solutions for DDoS to the Zero-Day category of the attacks [70] which is the category of unknown attacks is yet another question on mitigating DDoS effectively as we cannot predict the behavior due to lack of training in the detectors for these attacks, especially in machine learning solutions [71]. Adaptability to such attacks is also needed to make the defence much stronger and dynamic.

### (g) Cost effectivity with assurance on QoS.

The cost factor is another important issue to needs a focus when designing a defence solution as after all it is linked to IoT which is extensively used by today's common people, that's why the corresponding defence should also be affordable otherwise it will be of no use regardless of how strong protection it is providing [72]. Moreover, affordability should not be adjusted with Quality of service, it should be in direct proportion with QoS.

### (h) Complete protection

Defending DDoS should not be just a one-step process, it should include preventive measures at all involved stages right from taking precautions like regular updates on security system of IoT devices to applying the appropriate defence mechanism against the compromised device. Most of the methods are specifically designed for defending DDoS in a compromised network by application of their same proposed solution at each level of severity. A complete defence solution to DDoS tries to minimize the chances of the device becoming victim right at the initial stage, even if somehow the device gets attacked under DDoS then the security system will first perform checks on the level of its severity depending upon which it applies the appropriate defence against it [73]. There are some Défense mechanisms which divide the kinds of DDoS attacks into the low rate and high rate according to the frequencies of the packet sent across the network and therefore, apply the defence method accordingly.

## 8 Conclusion

Denial-of-service attacks behaves differently from other attacks as it often does not show any initial signs on the targeted device of its failure, rather, it gradually depletes all the available resources consuming whole network bandwidth that finally results into a server shut down. In this survey, we have discussed the concepts involved in defending a DDoS attack from traditional methods to IoT specific ones. However, we have focussed our study to the DDoS attacks in IoT as per the current trends. Role of IoT botnets and malware and their new variants have been discussed thoroughly to better understand the attacking mechanism. The diversity of such attacks is explained through defining taxonomies on both DDoS attacks as well as DDoS defence mechanisms. For a complete comparative analysis amongst all main defence mechanisms in the recent past years, a categorical description is provided based on their system models used, key points and shortcomings as their vulnerabilities.

Even though the research development under DDoS mitigation in IoT is progressing with a good pace and researchers are coming up with their much more efficient and innovative ideas, there are still open issues and challenges that have been discussed above to provide an ideal picture of a DDoS Defence System. In a nutshell, now the defence in IoT has to get smarter enough than the IoT itself.

## References

1. Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., et al. (2018). Internet-of-Things security and vulnerabilities: Taxonomy,

- challenges, and practice. *Journal of Hardware and Systems Security*, 2(2), 97–110.
2. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, 6(2), 1606–1616.
  3. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266–2279.
  4. Million Amazon Echo Smart Speakers to Be Sold In 2017, Driving US Smart Home Adoption. <https://www.forbes.com/sites/gilpress/2017/10/29/22-million-amazon-echo-smart-speakers-to-be-sold-in-2017-driving-us-smart-home-adoption/#5328961c481a>. Accessed 15 December 2018.
  5. Top IoT Vulnerabilities. [https://www.owasp.org/index.php/Top\\_IoT\\_Vulnerabilities](https://www.owasp.org/index.php/Top_IoT_Vulnerabilities). Accessed 04 March 2019.
  6. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7), 1645–1660.
  7. Lee, J. H., & Kim, H. (2017). Security and privacy challenges in the internet of things [security and privacy matters]. *IEEE Consumer Electronics Magazine*, 6(3), 134–136.
  8. Fortino, G., & Trunfio, P. (Eds.). (2014). *Internet of things based on smart objects: Technology, middleware, and applications*. Berlin: Springer.
  9. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *2013 9th international conference on computational intelligence and security (CIS)* (pp. 663–667). IEEE.
  10. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), 80–84.
  11. Lohachab, A., & Karambir, B. (2018). Critical analysis of DDoS—An emerging security threat over IoT networks. *Journal of Communications and Information Networks*, 3(3), 57–78.
  12. Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2018). REATO: REActing TO Denial of Service attacks in the Internet of Things. *Computer Networks*, 137, 37–48.
  13. DDoS Statistics That Should Concern Business Leaders. <https://www.coxblue.com/12-ddos-statistics-that-should-concern-business-leaders/>. Accessed 29 October 2018.
  14. Akamai's State of The Internet Security Q3 2016 Report. <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf>. Accessed 14 December 2018.
  15. New Report Points to Alarming DDoS Attack Statistics and Projections. <https://www.corero.com/blog/736-new-report-points-to-alarming-ddos-attack-statistics-and-projections.html>. Accessed 14 December 2018.
  16. Kaspersky Lab DDoS Intelligence Report: Long-lasting Attacks, Amplification Attacks and Old Botnets Make a Comeback. [https://usa.kaspersky.com/about/press-releases/2018\\_kaspersky-lab-ddos-intelligence-report-long-lasting-attacks-amplification-attacks-and-old-botnets-make-a-comeback](https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-ddos-intelligence-report-long-lasting-attacks-amplification-attacks-and-old-botnets-make-a-comeback). Accessed 14 December 2018.
  17. Cisco Visual Networking Index: Forecast and Trends, 2017–2022. <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html>. Accessed 14 December 2018.
  18. Statistics That Demonstrate the Need for DDoS Mitigation. <https://www.cdnetworks.com/en/news/10-statistics-that-demonstrate-the-need-for-ddos-mitigation/4234>. Accessed 14 December 2018.
  19. The average DDoS attack cost for businesses rises to over \$2.5 million. <https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/>. Accessed 14 December 2018.
  20. DDoS is a most common cyberattack on financial institutions. <https://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions>. Accessed 14 December 2018.
  21. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defence mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, 15(4), 2046–2069.
  22. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. arXiv preprint [arXiv:1707.01879](https://arxiv.org/abs/1707.01879).
  23. McDermott, C. D., Petrovski, A. V., & Majdani, F. (2018, June). Towards situational awareness of botnet activity in the internet of things. In *2018 International conference on cyber situational awareness, data analytics and assessment (Cyber SA)* (pp. 1–8). IEEE.
  24. Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, 2, 76–79.
  25. Jerkins, J. A. (2017). Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)* (pp. 1–5). IEEE.
  26. The Wirex Botnet. <https://blog.cloudflare.com/the-wirex-botnet/>. Accessed 04 December 2018.
  27. The Reaper IoT Botnet Has Already Infected A Million Networks. <https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/>. Accessed 05 December 2018.
  28. New Vicious Torii IoT Botnet Discovered. <https://www.csoonline.com/article/3310222/security/new-vicious-torii-iot-botnet-discovered.html>. Accessed 14 December 2018.
  29. Alert (TA18-331A) 3ve—Major Online Ad Fraud Operation. <https://www.us-cert.gov/ncas/alerts/TA18-331A>. Accessed 14 December 2018.
  30. Three Types of DDOS Attacks. <https://blog.thousandeyes.com/three-types-ddos-attacks/>. Accessed 04 December 2018.
  31. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defence mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39–53.
  32. Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfari, R. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint [arXiv:1208.0403](https://arxiv.org/abs/1208.0403).
  33. Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 5(4), 586–602.
  34. Specht, S. M., & Lee, R. B. (2004). Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In *ISCA PDCS* (pp. 543–550).
  35. Lemon, J. (2002, February). Resisting SYN flood DoS attacks with a SYN Cache. In *BSDCon* (Vol. 2002, pp. 89–97).
  36. Kambourakis, G., Moschos, T., Geneiatakis, D., & Gritzalis, S. (2007, October). Detecting DNS amplification attacks. In *International workshop on critical information infrastructures security* (pp. 185–196). Berlin: Springer.
  37. Kührer, M., Hupperich, T., Rossow, C., & Holz, T. (2014). Exit from hell? Reducing the impact of amplification DDoS attacks. In *USENIX Security Symposium* (pp. 111–125).
  38. Douligieris, C., & Mitrokotsa, A. (2004). DDoS attacks and defence mechanisms: Classification and state-of-the-art. *Computer Networks*, 44(5), 643–666.
  39. Lau, F., Rubin, S. H., Smith, M. H., & Trajkovic, L. (2000). Distributed denial of service attacks. In *2000 IEEE international conference on systems, man, and cybernetics* (Vol. 3, pp. 2275–2280). IEEE.
  40. Types of DDoS Attacks. <https://www.esecurityplanet.com/network-security/types-of-ddos-attacks.html>. Accessed 14 December 2018.

41. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23–40.
42. DDOS Report in 2018. <https://securelist.com/ddos-report-in-q3-2018/88617/>. Accessed 04 December 2018.
43. Linux Malware on the Rise: A Look at Recent Threats. <https://www.linux.com/news/2017/7/linux-malware-rise-look-recent-threats>. Accessed 29 March 2018
44. Mergendahl, S., Sisodia, D., Li, J., & Cam, H. (2017). Source-end DDoS defence in IoT environments. In *Proceedings of the 2017 workshop on internet of things security and privacy* (pp. 63–64). ACM.
45. Anirudh, M., Thileeban, S. A., & Nallathambi, D. J. (2017, January). Use of honeypots for mitigating DoS attacks targeted on IoT networks. In *2017 International conference on computer, communication and signal processing (ICCCSP)* (pp. 1–4). IEEE.
46. Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011). A learning automata-based solution for preventing distributed denial of service in Internet of things. In *2011 international conference on internet of things and 4th international conference on cyber, physical and social computing* (pp. 114–122). IEEE.
47. Ahmed, M. E., & Kim, H. (2017). DDoS attack mitigation in Internet of Things using software defined networking. In *2017 IEEE third international conference on big data computing service and applications (BigDataService)* (pp. 271–276). IEEE.
48. Adat, V., Gupta, B. B., & Yamaguchi, S. (2017, November). Risk transfer mechanism to defend DDoS attacks in IoT scenario. In *2017 IEEE international symposium on consumer electronics (ISCE)* (pp. 37–40). IEEE.
49. Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, 62, 64–83.
50. Javaid, U., Siang, A. K., Aman, M. N., & Sikdar, B. (June 2018). Mitigating IoT device based DDoS attacks using blockchain. In *Proceedings of the 1st workshop on cryptocurrencies and blockchains for distributed systems* (pp. 71–76). ACM.
51. Sagirlar, G., Carminati, B., & Ferrari, E. (2018, October). Auto-BotCatcher: blockchain-based P2P botnet detection for the internet of things. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)* (pp. 1–8). IEEE.
52. Su, J., Vargas, D. V., Prasad, S., Sgandurra, D., Feng, Y., & Sakurai, K. (2018). Lightweight classification of IoT malware based on image recognition. arXiv preprint [arXiv:1802.03714](https://arxiv.org/abs/1802.03714).
53. Zhou, L., Guo, H., & Deng, G. (2019). A fog computing-based approach to DDoS mitigation in IoT systems. *Computers & Security*, 85, 51–62.
54. Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. arXiv preprint [arXiv:1804.04159](https://arxiv.org/abs/1804.04159).
55. Singh, K., Guntuku, S. C., Thakur, A., & Hota, C. (2014). Big data analytics framework for peer-to-peer botnet detection using random forests. *Information Sciences*, 278, 488–497.
56. Haddad Pajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, 85, 88–96.
57. McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018, July). Botnet detection in the internet of things using deep learning approaches. In *2018 international joint conference on neural networks (IJCNN)* (pp. 1–8). IEEE.
58. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., et al. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3), 12–22.
59. Zhang, C., & Green, R. (2015). Communication security on the internet of thing: Preventive measure and avoid DDoS attack over IoT network. In *Proceedings of the 18th symposium on communications and networking* (pp. 8–15). Society for Computer Simulation International.
60. Sonar, K., & Upadhyay, H. (2016). An approach to secure internet of things against DDoS. In *Proceedings of international conference on ICT for sustainable development* (pp. 367–376). Singapore: Springer.
61. De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-capable IoT malwares: Comparative analysis and Mirai investigation. In *Security and Communication Networks, 2018*.
62. Adat, V., & Gupta, B. B. (2017, April). A DDoS attack mitigation framework for the internet of things. In *2017 international conference on communication and signal processing (ICCSP)* (pp. 2036–2041). IEEE.
63. Adat, V., Dahiya, A., & Gupta, B. B. (2018, January). Economic incentive-based solution against distributed denial of service attacks for IoT customers. In *2018 IEEE international conference on consumer electronics (ICCE)* (pp. 1–5). IEEE.
64. Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's intranet of things to a future internet of things: A wireless- and mobility-related view. *IEEE Wireless Communications*, 17(6), 44–51.
65. Dou, W., Chen, Q., & Chen, J. (2013). A confidence-based filtering method for DDoS attack defence in cloud environment. *Future Generation Computer Systems*, 29(7), 1838–1850.
66. Afek, Y., Bremner-Barr, A., & Tuitou, D. (2010). U.S. Patent No. 7,707,305. Washington, DC: U.S. Patent and Trademark Office.
67. Alpaydin, E. (2009). *Introduction to machine learning*. Cambridge: MIT Press.
68. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, 1–31.
69. Mirkovic, J., Prier, G., & Reiher, P. (2002, November). Attacking DDoS at the source. In *Proceedings. 10th IEEE International Conference on Network Protocols, 2002* (pp. 312–321). IEEE.
70. Musca, C., Mirica, E., & Deaconescu, R. (2013). Detecting and analyzing zero-day attacks using honeypots. In *2013 19th international conference on control systems and computer science (CSCS)* (pp. 543–548). IEEE.
71. Casas, P., Mazel, J., & Owezarski, P. (2012). Unsupervised network intrusion detection systems: Detecting the unknown without knowledge. *Computer Communications*, 35(7), 772–783.
72. Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks*, 81, 308–319.
73. François, J., Aib, I., & Boutaba, R. (2012). FireCol: A collaborative protection network for the detection of flooding DDoS attacks. *IEEE/ACM Transactions on Networking (TON)*, 20(6), 1828–1841.
74. Sonar, K., & Upadhyay, H. (2014). A survey: DDoS attack on Internet of Things. *International Journal of Engineering Research and Development*, 10(11), 58–63.
75. Zhang, C., & Green, R. (2015, April). Communication security in internet of thing: Preventive measure and avoid DDoS attack over IoT network. In *Proceedings of the 18th symposium on communications and networking* (pp. 8–15). Society for Computer Simulation International.
76. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250–1258.
77. Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications (IJACSA)*. <https://doi.org/10.14569/IJACSA.2018.090349>.



78. Dougherty, J., Kohavi, R., & Sahami, M. (1995). Supervised and unsupervised discretization of continuous features. In *Machine learning proceedings 1995* (pp. 194–202).
79. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, 100, 779–796.
80. Li, L., & Lee, G. (2005). DDoS attack detection and wavelets. *Telecommunication Systems*, 28(3–4), 435–451.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Ruchi Vishwakarma** has received her M.Tech. degree in Computer Engineering (Specialization in Computer Engineering) from National Institute of Technology, Kurukshetra, Haryana, India. Currently she is working as Software Engineer in MAQ Software, Hyderabad, India. Her research interest includes Network security, IoT security, Machine learning and DDoS Detection.



**Ankit Kumar Jain** is presently working as Assistant Professor in National Institute of Technology, Kurukshetra, India. He received Master of technology from Indian Institute of Information Technology Allahabad (IIIT) India and Ph.D. degree from National Institute of Technology, Kurukshetra. His general research interest is in the area of Information and Cyber security, Phishing Website Detection, Web security, Mobile Security, IoT security, Online Social Network and Machine Learning.

He has published many papers in reputed journals and conferences.