Detection and Prevention of DoS and DDoS in IoT

Meetu Sharma and Bhavna Arora

Abstract Internet of Things (IoT) is a network of interconnected devices embedded with software, sensors and essential electronics that allow us to gather and exchange data between them. Through IoT, it is difficult to guarantee the privacy and protection of the users due to various artifacts linked to the Internet. Denial of Service (DoS) and Distribution Denial of Service (DDoS) are among the main security issues in IoT. DoS is a type of attack where attackers try to prevent access by legitimate users to the service. A DDoS is where multiple systems target a single, DoS attack system. This occurs when several systems overload a target system's bandwidth or resources, normally at one or more servers. This is because of resource-constrained IoT network characteristics that have become a big victim. The early detection of DoS and DDoS attacks will prevent the resource-constrained devices from becoming a target and early death. This paper focuses on vulnerabilities in IoT such as Distributed Denial of Services (DDoS). Many privacy-conserving mechanisms have been discovered (such as automatic solution learning, and DDoS warning mechanisms). And, related work is under way. The goal of this paper is to present the detection and prevention of DDoS in IoT and privacy issues faced by the IoT environment and current mechanisms for its security.

Keywords Denial of Service (DoS) · DDoS · Security · Internet of Things (IoT) · Constrained

1 Introduction

IoT is an advanced analytical and automation system that takes advantage of processing, cloud computing, collaboration and machine intelligence technology to create a complete product or service framework. These devices require greater transparency control and effectiveness when added to any industrial environment. The Internet of Things has been introduced in recent decades as an groundbreaking

M. Sharma (✉) · B. Arora
Department of Computer Science and Information Technology, Central University of Jammu, Jammu, Jammu and Kashmir 181143, India

P. K. Singh et al. (eds.), *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*, Lecture Notes in Networks and Systems 203,
https://doi.org/10.1007/978-981-16-0733-2_60

technology which has a significant effect on human life. The Internet of Things is about combining the real and digital world into one ecosystem. It has, however, been a common concern that such revolutionary ideas will cause safety problems. To eliminate the possible risk of people revealing their private information, users need to grasp the concept of multiple attack tactics to eavesdrop the details of the person, with the DoS attack being considered one of the most common methods of attack. There Is also a expensive range of requirements for IoT devices. Monitoring is one of the clearest benefits of IoT. Through this, the exact quantity of equipment, water delivery and use, intelligent energy storage and protection delivery conveniently obtained gives an benefit in understanding items in advance IoT System Architecture. Denial of Service (Dos) is a digital assault that tries to make a computer or associate asset unaccessible to its expected customers by momentarily or unconclusively disrupting Internet-related host administrations. Refusal of administration is typically promoted by overwhelming computer or asset-focused people with needless demands attempting to overburden structures and preventing a few or any specific requirements from being fulfilled. For Distributed Denial of Service DDoS is short. DDoS is a kind of DoS assault in which different negotiated frameworks, which are regularly contaminated with a Trojan, are used to focus on a solitary framework that causes a Denial of Service (DoS) assault. Casualties of a DDoS assault consist of both the end based on the frame and all structures malignantly used and limited by the programmer in the attack conveyed [1]. In a DDoS assault, the approaching traffic flooding the unfortunate casualty starts from a wide range of sources—possibly many at least thousands. This viably makes it difficult to stop the assault just by obstructing a solitary IP address; additionally, it is hard to recognize authentic client traffic from assault traffic when spread across such a significant number of purposes of cause. To maintain a strategic distance from the potential hazard we use Denial of administration (DoS) a sort of assault where aggressors endeavor to keep real clients from getting to the administration. In DoS assault, the aggressor generally sends extreme messages asking the system or server would not have the option to discover the arrival locations of the assailants when sending the validation endorsement, making the server hold up before shutting the association, the aggressor sending more confirmation messages with invalid bring addresses back. Henceforth, the procedure of confirmation and serve holds up will start again helping the system or server occupied. There are various classes of DoS assault happening at sensors and mist hubs of IoT engineering. At mist hubs, there are six regular classes of dos assault that exist at mist layer of IoT design are:

Smurf flooding of ICMP reverberation answer.
Neptune flooding of synchronizing on port(s).
The dark mentioning of URL having numerous backslashes from a webserver.
Tear causing framework reboot or crash utilizing misfragmented UDP bundle.
Case pinging with deformed bundles causing reboot or crash.
Land-sending UDP parcel having a similar source and goal address to a remote host.

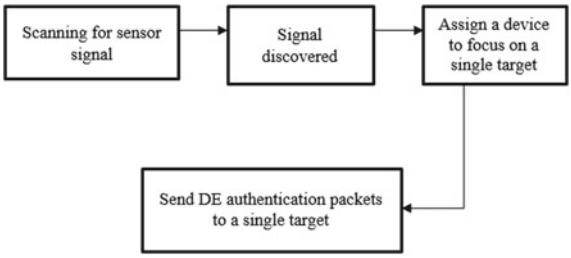

Fig. 1 Process of denial of service

Fatigue assault. A Denial of Service (DoS) assault is not the same as a DDoS assault. Dos assault ordinarily utilizes one PC and one web association with a flood a focused on framework asset.
DDOS utilizes numerous PCs and web associations with flood the objective asset (Fig. 1).

In the DDoS attack, the victim's incoming traffic flood originates from possibly hundreds of thousands or more from several separate outlets. This essentially renders it hard to avoid the assault by merely blocking a specific IP address; however, when scattered over too many points of origin, it becomes very difficult to differentiate valid user traffic from attack traffic.

1.1 Security Concerns in IoT

Internet of Things is a platform of real-world devices that communicate in real time. There are various threats involves in IoT security is shown (Fig. 2).

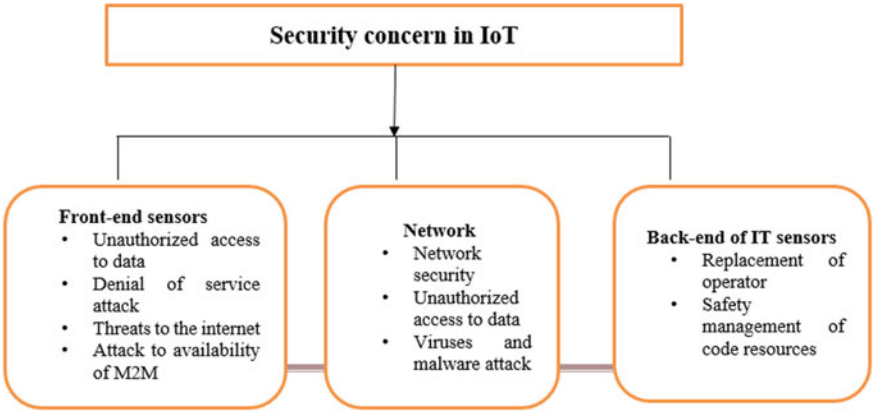

Fig. 2 Security concern in IoT

Front-end sensors

Front-end sensors receive sensors to collect data. The data is then transmitted through modules or computers, thereby undertaking various sensor networking services [1]. However, this approach requires the protection with business installing computers and access to its nodes.

Network

The network plays a crucial role in ensuring interconnection as well as the efficiency of IoT operation. If a large number of machines send data causing congestion in the network, there are a significant range of IoT nodes and classes that may cause service attacks to be declined.

Back-End sensors

These sensors have high-security, middleware and gathering specifications, analyzing sensor data in actual time to improve business understanding. At any time, IoT security has numerous extreme standards of confidentiality, security, safety, data integrity, data confidentiality, and availability.

1.2 Detection of DDoS at Application Layer

There are various faces involved in preventing DDoS attacks in which four phases involved as follows were explained in previous studies.

Prevention. The protection process focuses on shielding a network from attack by installing appropriate security equipment in various locations. In fact, mitigation also preserves server capital and guarantees that the actual client is able to access online services. DoS attacks sent by robotic tools allow multiple programs to approach those Web pages without any human interference. Probable protection of this kind of attack by software design is to grant only authentic consumer to connect web server tools and equipment. Web design should be successful, which the attacker could not delay.

Reduction. The reduction process is also said to mitigation, and this step is enforced when violation happens, with sufficient protection. Countermeasures are performed to deal with the violation or slow down the attack. A reduction technique works by halting the assault. DDoS reduction creation is best regarded if the traffic of attack acknowledged as usual is small, also known as the false-positive limit. In addition to the mitigation technique that is supposed to block an unauthorized traffic source IP address which causes an attack, this method would explicitly guarantee real consumer access to a web service.

Detection. The detection process includes a running machine review to find bad traffic which leads to DDoS attacks. Detection requires a innovatory technique for detecting broad illegal traffic on GET requests opposed to web server. The bulk of the detection strategies was used to form DDoS identification such as matching trends,

clustering, predictive analysis, examining variations, correlations, and similarity. Detection usually development utilizes data background as the primary source to train the data to generate a threshold that will be applied to a parameter using a particular procedure for counting the GET request obtained. The wrong-positive rate.

Monitoring. The monitoring process required, the use of devices, such as network monitoring software, obtains the requisite information about a host or network. Monitoring is carried out in real time, as it is necessary to detect DDoS attacks. If the intruder began a DDoS assault using a botnet installed at various locations around the globe, tracking method becomes complicated. According to, dynamic monitoring is required to shape defenses for attacks. This chart provides a schematic view of the protection's life cycle.

1.3 Limitations and Challenges Faced by DDoS Attack

Associating an identity to a single person is a hazard because this can result in profiling and monitoring. Therefore, disallowing these activities in IoT and taking some preventive steps is one of the biggest challenges. Localization and monitoring attempt to establish and monitor the location of the person through space and time. The major challenge is developing protocols that inhibit IoT interactions such activity. In e-commerce applications, profiling information relating to a specific person to infer preferences through correlation with other profiles and data is very common. The major challenge is to align business interests in profiling and data collection with the privacy requirements of users. Many difficulties of maintaining privacy in IoT include distributing data safely via a shared channel without shielding the general network users, avoiding unwanted collection of information regarding the nature and characteristics of personal items.

2 Recent Detection Methods for DDoS in IoT

Hasan et al. [2] presented a paper which uses machine learning approaches to predict an attack and anomaly in IoT sensors. The algorithms for machine learning were used which are logistic regression (LR), support vector machine (SVM), logistic regression (LR), and artificial neural network (ANN). The measurement criterion used in the performance comparison is precision, precision, f1, and field under the characteristic curve controlled by the receiver. The program obtained test accuracy of 99.4% for the decision tree, random forest, and ANN. While the [3] accuracy of these techniques is the same, another metric shows that random forest performs comparatively better.

Bakhtiar et al. [3] introduced an IDS with a lightweight algorithm for DoS detection. J48 learning machine algorithm has been checked as reliable for use in restricted

applications, so in this study, we have fitted the middleware with a lightweight J48-based IDS to solve the DoS threat. The test results said 75% of network packets could be identified by the IDS. Kajwadkar et al. [4] introduced a novel method, early prevention and detection algorithm for DoS and DDoS attacks. The algorithm was designed to fit in with the limited setting. In addition, the proposed algorithm can be equated with more research, and deep analysis can be carried out.

de Lima Filho et al. [5] has introduced the intelligent identification program (smart detection system) algorithm, the web solution for detecting DDoS attacks. He employed various machine learning methods. He observed Denial of Service attacks utilizing specific algorithms. The software used the random forest tree algorithm to classify network traffic based on flow protocol samples taken directly from network computers. Several experiments were conducted to calibrate the unit and to calculate its performance. Evidence suggested the approach proposed is possible and shows better performance compared with some recent and applicable approaches to literature. The proposed system was tested on three intrusion detection systems. While the system has achieved significant results within its reach, some improvements are needed, such as improved hit rates between attack classes and an automated parameter adjustment mechanism to maximize the rate of attack detection.

Daud et al. [6] concluded that the purpose of this paper has been accomplished with success. The results of this experiment show he is vulnerable to DoS attack by the IoT sensor node. Therefore, taking other security measures to counter the below susceptibility, for example, the deployment of numerous intrusion detection systems to identify DoS attack trends and signatures, and the clustering of sensor nodes to maximize the lifetime of the network, ensuring the efficiency of the IoT sensor node. To increase the lifespan of the IoT network for more study and creation on the use of clustering techniques for the IoT sensor node.

Santosh Kumar et al. [7] presented a paper on the identification of Dos attacks. He suggested a topology management method (TMM) in his paper for the recovery of the attack. The proposed TMM used the network to recover and compared it to current approaches. Further analyzes are to identify stealth denial of service attacks. Additionally, it is possible to evaluate several other fields of the IEEE 802.11 protocol frame and extract new features to reduce the time taken to detect the attack and increase analytical performance.

Cui Y et al. [8] demonstrated that the online hacking and attacking on Dos attack evaluated in IoT devices posed a threat to net health. The Internet of Things (IoT) will cause serious losses of property as an important component of the information era once it is targeted. This experiment aims to use three devices to replicate the Denial of Service (DOS) assault concept. Kali Linux initiated the attack in a variety of different ways. In his paper, he described the experiment's modified variables and showed how they can affect the effect.

Guleria A et al. [9] presented a paper for the given idea of also getting their influence for community holding webpage guests concerning certain DDOS attacks. Here, a DDOS assault was investigated to investigate the transmission of believing group holding website guests would specifically capture such general party movement. Only

this paper needs to claim flood hit. This paper also mentioned a strategy with reminiscent anomalies clinched alongside visitors to the group's website, fundamentally based on an unrestrained α-strong model.

Ladislav Huraj et al. [10] suggested these IoT devices and their rapid development of the Internet would cause many security issues. This article presents the effectiveness of selected real-world IoT devices in demonstrating the UDP-based distributed reflective DoS attack, as a particular form of DDoS attack led to the layer of transport. The experiments display this type of attack on four heterogeneous IoT platforms representatives: IP camera, Raspberry Pi single-board machine, network printer, and smart lights. The experiment findings indicate the ability to be used in the DRDoS (Distribution Reflection Denial of Service) attack on all investigated IoT devices.

3 Comparison of Techniques of Different Researchers for Dos and DDos Based on Parameters

See Table 1.

4 Detection and Prevention Methods for DDoS in IoT

4.1 Detection Techniques

Detection of a DDoS attack is performed in network context by different strategies to prevent the serious injury. DDoS detection techniques for attacks have a workflow which tends to diagnose the impact of DDoS assaults [1] (Fig. 3).

Honey net cloud is a diverse group of various sub-networks. It includes honeypots. Honeypots are usually traffic controlled and alert HTTP, FTP, and UDP protocols. Toggle Bridge sends question that comes after passing dynamic supply board. The IP address is given to it, and it varies at regular time intervals for each and every honeypot and board. Stop fingerprinting methods. By utilizing this strategy, the intruder thereby is confused. What is it? Any request from a suspect node shall enter honeynet, dynamic framework of provisioning defines the sum of malicious order comes in request analysis is as loading is opposed to preset load threshold honeypot [2].

Fog computing-based security system (FOCUS)

From the recent improvement on fog computing, FOCUS has been developed and is a protection framework focused on fog computing. Fog computing is close the computers and end-users dependent on IoT. FOCUS offers a security mechanism on two occasions. A VPN is implemented at first level to secure the contact channel, and then, a challenge answer authentication mechanism is used to identify the unlawful traffic from DDoS attack [3]. FOCUS is a great strategy because it has less reaction

Table 1 Comparison study of DoS and DDoS in IoT

No.	Title	Parameter	DDOS-level identification	Evaluation method	Data set	Matrix performance
1	HADEC: live DDoS detection system, based on Hadoop [11]	Timestamp, source network, IP address, packet protocol, and packet header	DDoS high rate: TCP SYN, http post, UDP, and ICMP	Experiment	Dataset experiments	Measure utilization, processor and memory
2	D-FACE: a collaborative anomaly-based approach to early identification of DDoS threats and flash events [12]	Time window size, packet header, and generalized parameter	High intensity and low rate assault and a bunch of memories	Experiment	MTT Lincoln, CAIDA and FIFA	Precise classification, false-positive rate, *F*-measurement and precision
3	Defending HTTP web servers against attacking DDoS by detection of duration dependent attack flow [13]	Threshold whitelist and blacklist	High rate DDOS attack	Simulation (OPNET experiment)	Experiment dataset	Detection speed
4	Real-time prevention of DDoS threats using FPGA [14]	Origin IPs, variable indexing of origin IPs, and volume of packets	High rate HTTP DDoS	Experiments	CAIDA, TUIDS, and DARPA	Level of identification, accuracy, false positive and false negatives
5	FHSD: an advanced tool for spoof detection of network DDoS attacks [15]	Hop count, source MAC address, OS passive fingerprinting	High rate HTTP DDoS	Experiments	DARPA LLDOS inside 1.0 and experiment dataset	Detection rate, accuracy, and false positive
6	Detection of cloud based HTTP DDoS attacks using matrix covariance approach [16]	List of covariances and the TCP channel header	High rate HTTP DDoS	Simulation (MATLAB)	KDD cup 99 and experiment dataset	Level of identification, accuracy, false positive and false negatives

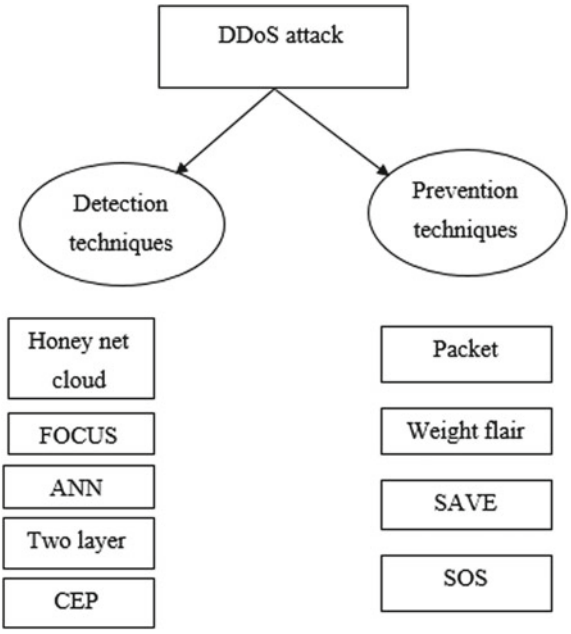

Fig. 3 Detection and prevention techniques for DDoS in IoT

time and less use of bandwidth. However, it includes precise description of network traffic from traffic analysis device.

ANN IDS-based artificial neural network is used to evaluate the risks IoT faces. To capture and interpret information from several IoT devices and identify a DDoS attack inside the IoT network, it is implemented as an offline framework for detecting some kind of intrusion. They suggested an intrusion prevention method focused on a neural network to identify DDoS assaults. The identification or reconnaissance method was focused on classifying normal traffic patterns and malignant patterns. For this ANN model, the presentation demonstrated more than 99% precision. It effectively identifies DDoS attacks with greater precision for unauthorized IoT network traffic. It also increases network reliability but is not particularly successful in real-time response.

Two-Layer approach There are two major forms of DDoS attacks, high rate traffic that triggers massive traffic spikes and low-rate traffic attacks that are more equal to regular real traffic attacks. Detecting them all at the same time is difficult because this technique uses two-layer approach to identify all threats. There are three levels to complete. At first point, the device named detection with average filters (DAF) is passed through to filter high-intensity DDoS attack metrics. The remaining metrics are transferred by (DDFT), which is identification of low-rate DDoS attacks with differential Fourier transformation. It detects both low-rate and high-rate DDoS attacks. However, it is hard to distinguish when low-rate and high rate are similar. The CEP architecture consists of three primary layers: event generator, event processor and action system. The incident detector scans and tracks the network traffic as soon

as an accident happens. Event generator contains two modules: (i) packet analyzer and (ii) software for attack detection. Both of these modules evaluate the form of DDoS attack and also examine incoming packet properties.

4.2 Prevention Methods/Techniques

For protection against DDoS attacks, protective measures are often ideal. It is a shame that once the assault is initiated and made effective it will seriously damage the computer of the victim. Prevention methods often aim to handle the majority of threat traffic and hence aid to avoid the assault by DDoS. In this manner, victim computer is not impacted by assault and continues its normal operations.

Packet filtering Every counteractive measure is equivalent to a patch in any situation. Preventive approaches aim to address defense vulnerabilities that are regulated by DDoS assaults. Packet filtering strategy is one of the strategies for avoidance of DDoS attacks that decrease harmful incoming packets.

Weight-fair throttling: Weight-fair throttling mechanism prevents a web server at upstream router from DDoS attack. This mechanism is weight-fair since the leaky bucket at the router controls the traffic anticipated for the server. On the basis of connection count, congestion control algorithm regulates the bucket count of network traffic capacity sent for the traffic server. In this mechanism, even if some of the routers are compromised, then system can still be in working condition. The routers are disabled, but the device will still run.

SAVE: In this process, the source position sends messages regularly to all locations with valid IP addresses. This approach helps routers to easily identify specific paths and IP address ranges as well. Router already knows the intended ranges of IP addresses, routers take valid addresses from routing tables, and then routers block the packets with one based on that knowledge. Routers block address packets that are not within predefined IP address set. The paradigm being introduced is constructive as it avoids packets with null addresses. It filters inappropriately presented packets properly, but legitimate packets may also be lost during the transient time because it is not efficient against intelligent IP spoofing.

5 Conclusion

This paper provides a study of recent methods of identification in the application layer detecting and preventing DoS and DDoS attacks. Research related to the DDoS attack has gained significant interest, particularly those occurring at the application layer. DDoS attack identification is very difficult because the traffic occurs because of other system types which can be influenced by botnet, such as IoT devices and the presence of DDoS as utilities may be considerably complex in detecting such an attack. The latest methods used to detect an assault on DDoS in IoT have developed various

strategies for detection purposes. The DoS and DDoS attacks can lead to jamming of networks and can disrupt any network environment. Early detection and prevention of these attacks can lead to a better network service environment. As future work, the proposed methods can be compared with more works and its deep analysis can be done.

References

1. Singh K, Singh P, Kumar K (2017) Application layer HTTP-GET flood DDoS attacks: research landscape and challenges. Comput Secur 65:344–372
2. Hasan M, Islam M, Zarif II, Hashem MMA (2019) Internet of things attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet Things 7:
3. Bakhtiar FA, Pramukantoro ES, Nihri H (2019) A lightweight IDS based on J48 algorithm for detecting DoS attacks on IoT middleware. In: 2019 IEEE 1st global conference life sciences technology, pp 41–42
4. Kajwadkar S (2018) A novel algorithm for DoS and DDoS attack detection in internet of things. In: 2018 Conference on information communication and technology, pp 1–4
5. de Lima Filho FS, Silveira FAF, de Medeiros Brito Junior A, Vargas-Solar G, Silveira LF (2019) Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Secur Commun Networks 2019:1–15
6. Daud M, Rasiah R, George M, Asirvatham D, Rahman AFA, Halim AA (2018) Denial of service: (DoS) impact on sensors. In: 2018 4th International conference on information management ICIM, pp 270–274
7. Santhosh Kumar S (2017) An anomaly behavior-based detection and prevention of DoS attack in IoT environment. In: 2017 Ninth international conference advanced computing, pp 287–292
8. Guo K, Wang D, Zhi H, Lu Y, Jiao Z (2020) A trusted resource-based routing algorithm with entropy estimation in integrated space-terrestrial network. IEEE Access 8:122456–122468
9. Irum A, Khan MA, Noor A, Shabir B (2020) DDoS detection and prevention in internet of things
10. Alqahtani H, Sarker IH, Kalim A, Hossain SM, Ikhlaq S, Hossain S (2020) Cyber intrusion detection using machine
11. Cui Y, Liu Q, Zheng K, Huang X (2018) Evaluation of several denial of service attack methods for IoT system. In: 2018 9th International conference on information technology in medicine and education, pp 794–798
12. Guleria A, Kalra E, Gupta K (2019) Detection and prevention of DoS attacks on network systems. In: 2019 International conference on machine learning, big data, cloud parallel computing, pp 544–548
13. Huraj L (2018) IoT measuring of UDP-based distributed reflective DoS attack. In: 2018 IEEE 16th international symposium on intelligent systems and informatics, pp 209–214
14. Ali U (2018) Open access HADEC : hadoop-based live DDoS detection framework
15. Behal S, Kumar K, Sachdeva M (2018) D-FACE: an anomaly-based distributed approach for early detection of DDoS attacks and flash events. J Netw Comput Appl 111:49–63
16. Fox MR (1981) Cover letter PC-24(4)