EasyChair Preprint

№ 2486

DDoS Detection and Prevention In Internet of Things

Ammarah Irum, Muazzam A. Khan, Amna Noor and Balawal Shabir

January 29, 2020

DDoS Detection and Prevention In Internet of Things

Ammarah Irum[1], Muazzam A. Khan[2], Amna Noor[1], Balawal Shabir[1]

[1]Department of Computing, School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan.
[2]Department of Computer Science, Quaid-i-Azam University, Islamabad, Pakistan.
Email: airum.msit18seecs@seecs.edu.pk, muazzam.khattak@seecs.edu.pk, anoor.msit18seecs@seecs.edu.pk, bilawalshabir@gmail.com

Abstract—Internet of Things (IoT) has appeared to be a continuously-growing networking field in the technological era that is based on a wireless network that connects a large number of smart devices and people. It is a machine to machine communication network and it reduces the human aspect of maintenance. With the rapid development in this emerging world, where devices are smart and communicate with each other, they become vulnerable to different attacks against their security and privacy. Among these attacks, Distributed Denial of Service (DDoS) is an attack that infiltrates from different sources and it is responsible for blocking the internet usage for legitimate user, making network resources unavailable along with unnecessary bandwidth consumption and network congestion, which is more disruptive for IoT environment. This paper intends to discuss and review different detection and prevention techniques against DDoS attacks in IoT.

Index Terms—IoT, DDoS, prevention, detection, IDS, techniques.

1 Introduction

The Internet of Things (IoT) is an ever-growing network paradigm that comprises of the wide ranged objects including computers, mobile devices, watches, wearable devices, and many other smart devices. Billions of devices are part of this network and tend to make physical objects, devices and many other deployment areas smarter. Besides the inherent security risk, it is estimated that by 2020, number of IoT devices will be around 20.4 billion [1]. IoT will become one of the imperative building blocks of future Internet of Services (IoS). However, besides the advantages that IoT is offering, it comes along with numerous security challenges as well.

Increased social dependence on the information and communication technology has resulted in enhanced vulnerability to the plethora of critical cyber oriented attacks. One such attack is the cyber-attack infamously called Distributed Denial of Service (DDoS). It is one of the critical problem for the IT professionals and security administrators. It tends to be the most recurrent network disturbance attacks. For instance, In September 2016, a botnet Mirai, which is a potential DDoS tool capable to manage over 300,000 IoT device bots conveniently, infected above 100,000 devices and became one of the largest DDoS attacks in internet history [2] by brute forcing merely 62 pairs of standard credentials [3]. Afterwards, the Mirai's source code was released, and the risk of more DDoS attack significantly increased [4]. Since the day when first DDoS attack was launched, an increased annual impact, not only in the number but also in the type and rigorousness of DDoS incidents, has been observed. In fact, nowadays, DDoS attacks are considered to be one of the most severe threats to the stability of the entire Internet, particularly IoT.

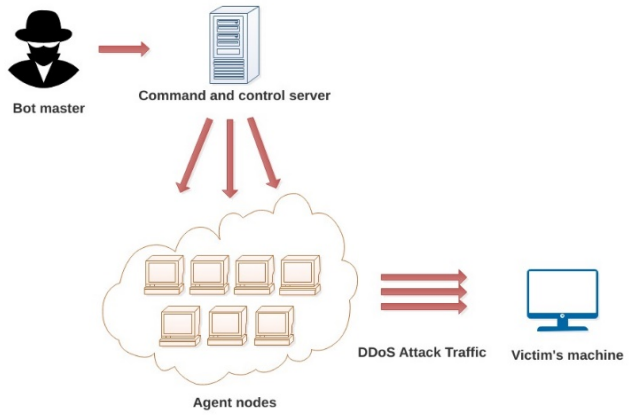

Fig. 1: DDos Attack Scenario

Distributed Denial of Service (DDoS) attacks pose a prominent security threat to modern era's Internet. The said attack especially targets the Internet of Things (IoT) environment as the IoT devices are said to have less memory, computing power and security measures to prevent DoS attacks. DDoS attacks are the acute attacks against IoT connected devices and exacerbate the network performance. It reduces the network and computing resources such a s CPU, memory or network bandwidth [5] [6]. The said attack gets benefit of hosts residing on the networks which are poorly

secured or even those which do not bear security. The DDoS attack is usually two-phased. Firstly, attackers try to exploit numerous vulnerabilities in significant number of devices, making them work as bots. Secondly, these bots are ordered by attackers to send bulk of requests to the target due to which the victim's computational resources are exhausted [7]. For instance, if home automation system gets affected by DDoS attack, then all home appliances along with the home locking system will get inaccessible. Even such a small example clearly tells security situation in IoT domain [8]. For manufacturers of IoT devices, it is also difficult to maintain standardized IoT devices as the process of manufacturing is rapid and cheap [9]. Numerous defense mechanisms for DDoS have been proposed in order to defend against these fatal attacks but no completely effective solution is available so far. However, following DDoS defense methods are used to lessen and ultimately remove the effect of DDoS attacks:

- Detection mechanism
- Prevention mechanism

In networks, DDoS attack detection and prevention is done either by using dedicated and expensive infrastructure or by relying on some third party service providers. Both of these approaches are centralized and are risked by single point of failure [10]. However, both traditional and latest techniques work well in different attack scenarios. In this survey paper, we deeply analyze the various prevention and detection techniques for DDoS attack in IoT environment. Rest of this survey paper is structured as following: In Section II, extensive literature review is done. The section III contains comparative analysis. In Section IV, we present justifications by taking into account the assessment based on certain evaluation parameters. Recommendations are given in Section V. Future work along with conclusion is presented in Section VI.

2 LITERATURE REVIEW

An extensive literature study has been conducted and the findings have been categorized into Detection, Prevention and Hybrid techniques. Furthermore, we illustrate the various detection and prevention techniques that are widely used to cater the DDoS attacks. Some techniques only perform the process of detection of DDoS attacks while some techniques prevent the IoT networks from being attacked by a DDoS source. However, there are some hybrid techniques as well that are capable of detecting and preventing the IoT network from DDoS attacks.

2.1 Detection Techniques:

In network environment, detecting a DDoS attack is done through various techniques in order to avoid the consequences of severe damage. DDoS attack detection techniques has a workflow that tends to diagnose the effect of DDoS attacks

2.1.1 Honeynet Cloud

Honeynet cloud is a diverse group of different subnets that consist of honeypots. Honeypots tend to handle the traffic of HTTP, FTP and UDP protocols carefully [11]. Filtering bridge sends request that arrives after passing over the dynamic provisioning module. The IP address is allotted to each and every honeypot and module changes it at periodic time intervals. Fingerprinting techniques are avoided by using this technique, thus puzzling the attacker. When any request from a suspicious node reaches honeynet, the dynamic provisioning module determines the quantity of incoming malicious request. The processing of request is done once load is compared to preset threshold load at the honeypot.

2.1.2 FOCUS: Fog-Computing based Security System

In [12], to improve scalability and processing time, some cloud-based techniques were proposed to counter malicious attacks but they were not as efficient as they may cause some delay in response due to long latency. So based on the recent improvements on fog computing, FOCUS was proposed which is a Fog Computing based Security System. Fog computing is near to the IoT based devices and end user. FOCUS provides a two level protection system. At first stage a VPN is applied to protect the communication channel and after that a challenge response authentication method is used to detect the illegitimate traffic from DDoS attack. FOCUS is a better technique as it has less response time and less bandwidth consumption. However, it needs accurate network traffic classification from traffic analysis unit.

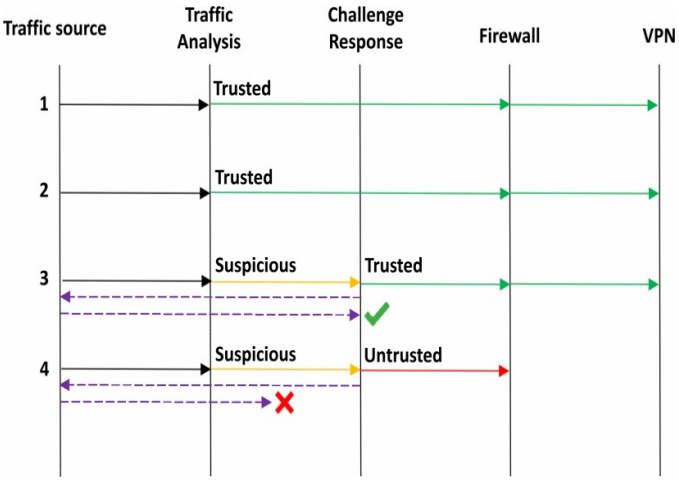

Fig. 2: FOCUS workflow [8]

2.1.3 Artificial Neural Network Intrusion Detection System:

In [13], Artificial Neural Network based IDS is used for the analysis of the threats that IoT is facing. It is deployed as an offline system for detecting any kind of intrusion in order to collect and analyze information from several IoT devices and detect a DDoS attack within IoT network. They proposed an approach based on neural network for intrusion detection to detect DDoS attacks. The process of detection or recognition was based on classification of regular traffic patterns and malign patterns. The demonstration showed over 99 percnt accuracy for this ANN model. It successfully detects DDoS attacks for illegitimate IoT network traffic with greater accuracy. It also improves stability of network but real-time response is not highly efficient.

2.1.4 Two Layer Approach for Mixed High-Rate and Low-Rate DDoS Attacks

In [14], the authors proposed a two layer approach where two metrics are normally used to detect DDoS attacks, in metric 1 victim router counts the packets at small interval and transforms it into a signal. Metric 2 Records the difference between arrival time of packets and transform into signals. There are two main types of DDoS attacks, high-rate traffic which cause the rise in prompt traffic and low-rate traffic attacks that is almost comparable to normal genuine traffic. It is challenging to detect them both at the same time so this method uses two-layer approach to detect both attacks. There are total three stages. At first stage, to filter high rate DDoS attack metrics are passed through the unit called detection with average filters (DAF). The remaining metrics are passed through (DDFT) which is detection with discrete Fourier Transformation that detects low rate DDoS attacks. It detects both low rate and high rate DDoS attacks. However, it is difficult to detect when low-rate and high-rate are close enough, and there's high overhead as well.

2.1.5 Complex Event Processing:

In [15], Adeilson et al proposed a real time DDoS detection system for DDoS in IoT environment. They have proposed a mechanism based on detecting intrusions in such a way that makes use of a growing technology called "Complex Event Processing" (CEP). CEP identifies significant events and reacts to them. The CEP

architecture has 3 main layers named as: Event Filter, Event Processor and Action Engine. As soon as an event occurs, the Event Filter checks and monitors the network traffic. Event Processor consists of two modules: (i) Packet Analyzer and (ii) Attack detection modules. Both of these modules determine the type of DDoS attack and also analyze the properties of incoming packets. Finally, the Action Engine handles the suspected attack activity and blocks access to related services. CEP based DDoS detection method detects DDoS attacks with greater accuracy and improves real-time performance. However, the lost packet rate is around 8%, so, it is not much reliable. Accurately distinguishes normal and DDoS attack traffic from consumer IoT devices but lost packet rate isn't reasonable.

2.2 Prevention Techniques:

Preventive mechanisms are always desirable for defense against DDoS attacks.It is beacuse of the fact that once the attack is launched and is rendered successful, it can significantly compromise victim's machine. Prevention techniques also tend to manage bulk of attack traffic and therefore help to cease DDoS attack [16]. In such a way, victim machine does not get affected by attack and continue to do its normal operations.

2.2.1 Packet Filtering Techniques:

Any counteractive action is in every case superior to a fix. Prevention-oriented methods incline to solve security liabilities which are dominated by DDoS attacks. Packet filtering technique is one of the DDoS attack prevention methods that drops malicious incoming packets. Senie et al. [2] proposed a filtering technique called ingress/egress. Network Ingress Filtering is a mechanism that doesn't allow an edge-level router to receive the packets whose source address is not reachable. The ingress filtering prevents the packets to enter the protected network from spoofed sources. The firewalls linked to a network have interfaces connected to both the local and the internet network. If firewalls apply the ingress filtering to the internet interface so that packets having source address of the internal network can be dropped, then it prevents the attacker from covering-up the attack as a host within the same network. Egress Filtering is applied to the packets of the internal interface of the network that are leaving the network. In egress filtering, the firewall will drop all the packets that have origin or source address that does not fit in the LAN. Ingress/ Egress filtering mechanism prevents IP Spoofing, however, DDoS attacks, when triggered with real IP addresses cannot be prevented by this filtering technique. Liu et al. proposed the StopIt prevention method against DDoS attacks [2]. It is a hybrid filter-based prevention scheme use to deal with the limits of IP spoofing. It enables each destination to set up a network filter which tends to block attack traffic that it may receive. To overcome the problem of filtering attack packets based on the IP addresses history, Kim et al. [2] presented a filtering technique that is based on statistics. A score is given to every network packet on the basis of particular traffic features. The suggested system works in a way that a data packet is indicated as an un-malicious packet if the difference between calculated score and threshold of automatically calculated score is quite less, else packet is declared as an attack packet. Packet filtering filters out malicious packets accurately but they require wider deployment geographically so that it can be more efficient but due to the exposed and decentralization of Internet, their implementation is quite difficult.

Fig. 4: Ingress/Egress Prevention Scheme [14]

In [2], author presented a proactive, collaborative and distributed real-time filtering technique called ScoreForCore against DDoS attacks at application layer. When there is no attack the presented scheme goals are to calculate score of every connection. When the attack occurs, every incoming connection's score is matched with prior score of the connection. This method can recognize already identified attacks with 100 percent precision and it is capable of detecting unknown attacks with 80% detection precision.

2.2.2 Weight-fair Throttling Mechanism:

Saifullah presented a technique called weight-fair throttling mechanism to prevent a web server at upstream router from DDoS attack [17]. 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.

2.2.3 Secure Overlay Service

Secure Overlay Service (SOS) is another preventive technique against DDoS attacks. By using this overlay service, a secret node communicates with another random node in a manner that the secret node's identity cannot be checked, but previously authorized sources can know and access it

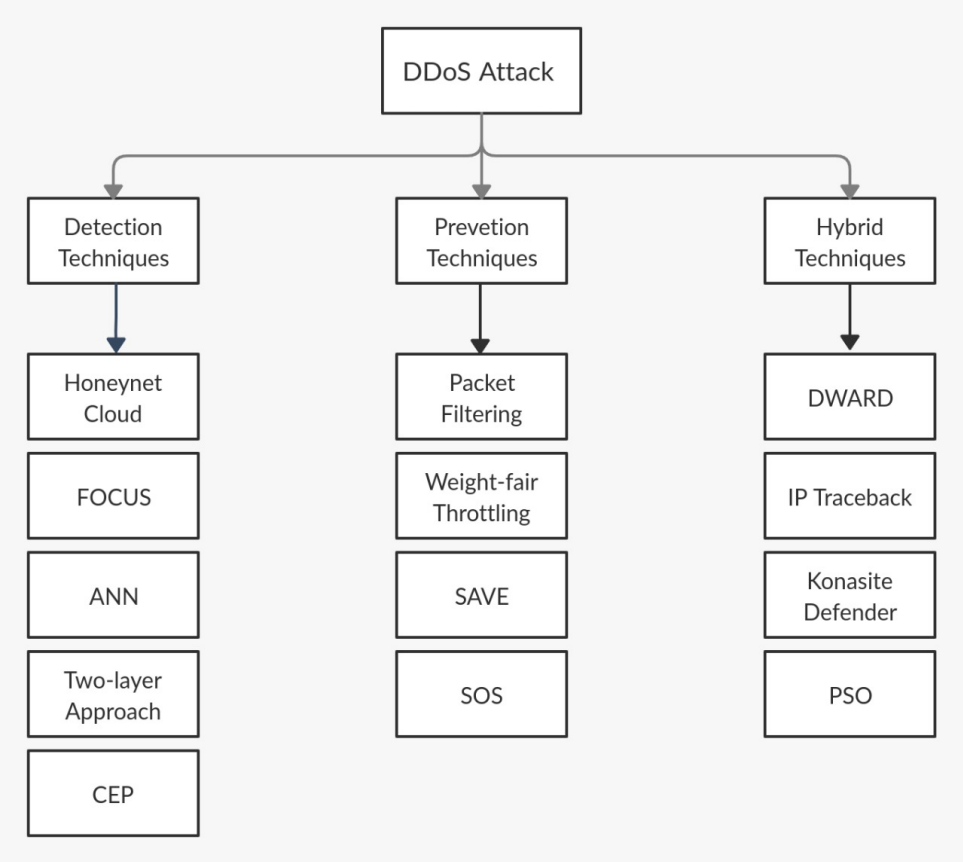

Fig. 3: Taxonomy of Detection and Prevention Techniques Against DDoS attacks in IoT

[17]. This process entails two independent authentications. In first, successful authentication allows transferring the traffic to some servlet that is referred as secret, and in second, the servlet again authenticates and pass only valid traffic to the edge routers of network. SOS works fine when predefined source nodes communicate. Its disadvantages include: It has limited scope and it doesn't work for web servers particularly and new routing protocol should be introduced if any other security issue rises. Secure Overlay Service has narrow scope as it does not comply with web servers.

2.2.4 SAVE

Li et al. has proposed a defense mechanism called SAVE [18]. In this mechanism, messages are sent by the source location to all destinations with valid IP addresses in a periodic manner. This method allows routers to recognize accurate routes rapidly, and also IP address ranges. Router already know the expected ranges of IP addresses, routers take valid addresses from routing tables and then on the basis of that information, routers block the packets with addresses that are not in pre-defined IP address range. The proposed model is proactive as it stops packets with invalid addresses. It appropriately filters improperly addressed packets but valid packets can also be dropped during the transient period as it isn't effective against intelligent IP spoofing.

2.3 Hybrid Techniques:

The techniques that are capable to perform both detective and preventive measures against DDoS attacks are called hybrid techniques. The basic workflow of hybrid techniques is as follows: Firstly, DDoS attack detection is done at victim's end. Secondly, prevention and mitigation is done at attacker's end [19]. Hence, in such a way,hybrid techniques appear to be more defensive against DDoS attacks in IoT.

2.3.1 D-WARD

"Distributed Network Attack Recognition and Defense" (D-WARD) is a well-known prevention technique deployed at source-end [20]. To detect malicious packets, it uses filtering and rate limit method. It is mounted on the exit router of last network as an inline system. The main components include observation which collects the statistics, traffic-policing and rate-limiting. D-WARD is useful in controlling TCP, UDP and ICMP flooding packets. It effectively detects suspicious traffic using communication patterns but there is no post attack analysis.

2.3.2 IP Traceback Technique: Proactive Approach

In the recommended technique of [11] detecting spoofed IPs differentiates the reliable TCP packets from the routine traffic reaching the DDoS shelter. The total amount of TTL hops and source's OS signature can be detected from the TCP packets, and in the reference table of bandwidth of each network, this information is used. When the attack happens, the attacking traffic can be detected by equating information

about TTL hops and OS signature and by conducting a statistical analysis to classify whether it is malicious or not. If so, the DDoS shelter blocks the related IP traffic.

2.3.3 Kona Site Defender Technology:

Kona Site Defender technology from Akamai is developed by IBM experts as a multifaceted defensive mechanism against DDoS attacks [21]. It serves as an online proxy based technique that allows network traffic through ports 443 (HTTPS) and 80 (HTTP), thus filtering the traffic targeted at application layer. By the collaborative efforts of IBM and Akamai, robust solutions are proposed to prevent DDoS attacks. For instance, in distributed website hosting, all the requests from legitimate users are redirected to Akamai server, then the request's load is redirected to various geographically distributed web-servers that host copies of the requested web pages.

2.3.4 PSO based DDoS Detection system:

Kesavamoorthy et al. [22] presented a swarm intelligence based DDoS detection and prevention using multi agent computational system with some agents interacting with each other. Four agents used in this paper are coordination, detection, monitoring and recovery agent. Whereas, particle swarm optimization (PSO) is a population oriented search algorithm. The population is known as swarm and individuals are called particles. The inherent idea is to find the optimum solution through information sharing and cooperation among particles in the swarm.

When the cloud service is started, the agents will be in active mode. Until any event occurs, all agents will remain in the live mode. In their proposed system, the coordination agent is said to be the global optimum whereas on the basis of default PSO rules, the Local Optimum is elected by each agent group on the basis of movements of agents within network. The monitoring agent generally monitors the irregular behavior from the client end. In active mode, it triggers the detection agent to examine the specific behavior of client to check whether the traffic is attack based or normal. The digital signature algorithm (DSA) curtails the possibility of DDoS attacks within the agent communication. The coordination agent then triggers the decision making agent. Before decision process starts, the decision making agent checks if any update in the local optimum has occurred within agent groups. If any update has occurred, local optimum is updated first and then information from detection agent is aggregated. Its advantages include: Attack detection and recovery time is minimum along with improved security features for cloud based platform. Its disadvantage is: Communication between agents sometimes is weakly vulnerable to attacks. By using a hybrid method that combines the co-variance matrices and entropy using the inputs collected from coordination agent, the decision making agent verify the DDoS attacks. Once the attack is confirmed by decision making agent, the recovery process begins. Decision making agent then triggers the recovery agent and the recovery agent then turns to active mode so that it can run the resource recovery agent to recover the particular IP address of that assigned resource.

After recovery process, the log recovery agent that keeps record of source IP address of the attacker's host address, TTL, port number, etc. is triggered. Finally, the coordination agent (COA) automatically refreshes its knowledge, based previous attack history, every time a new DDoS attacks is launched.

3 COMPARATIVE ANALYSIS

The techniques discussed in literature review are compared against certain parameters of evaluation so that we can find the optimal technique for detection and prevention against DDoS attacks in IoT. The comparison table clearly shows the level of accuracy with which DDoS attack can be handled by all discussed techniques. It also makes clear that whether a certain technique is capable of performing post attack analysis or not. Post attack analysis actually tells whether the technique efficiently renders its services to detect and prevent an IoT system from further attacks that could occur within small time of previous DDoS attack.

4 JUSTIFICATION

On the basis of comparative analysis, it is imperative that technique which simultaneously offers detection and prevention against DDoS appears to be an optimal technique due to certain factors. Hence, Particle Swarm Optimization (PSO) based DDoS attack detection mechanism using multi-agent system tends to be a reliable technique for securing cloud services in IoT as it provides the optimal performance and better security along with least attack detection and recovery time. Moreover, CEP based DDoS attack detection technique works well by ensuring precision and indicating its usefulness in the real time attack detection on IoT.

FOCUS is another DDoS attack detection technique that consumes less network bandwidth. Furthermore, a two-layer method for DDoS attack filtering and detection filters mixed low-rate high-rate successfully. Learning Automata is an intelligent technique that prevents DDoS attacks with almost 99 percent accuracy by taking into account packet sampling concept. The working node treats the legitimate requests and malicious requests uniquely whereas the attacker node isn't served after the first serving cycle. Thus, in further turns, only legitimate requests are considered. Furthermore, it monitors attacker nodes' information to issue a DDoS alert to neighboring nodes so they can also drop malicious incoming traffic.

Furthermore, D-WARD detects DDoS attacks with high accuracy and precision [18]. As its source-end deployment type, so it tends to control attack source. By constant monitoring of bidirectional traffic movements between the networks, D-WARD detects an attack and performs the periodic deviation analysis to identify normal traffic flow patterns. Furthermore, D-WARD gives a good detection rate along with significantly dropping the DDoS attack traffic. It makes use of an already defined model for usual patterns of traffic and tends to detect abnormalities in the two-way communication. Moreover, D-WARD also notices the network traffic for either attack validation or refutation. If attack is confirmed, D-WARD tends to control the attack rate. Conversely, if it is refuted, then increased traffic rate is gradually allowed. D-WARD does not perform post attack analysis to mitigate further attacks in near future. Moreover, Kona site being highly intelligent software by Akamai

TABLE 1: Comparative Analysis.

Techniques	A	OH	R	DL	RT	DR	P	D	RC	DT
Honeynet Cloud [11]	H	L	M	M	L	M	N	Y	N	-
FOCUS [12]	H	L	H	L	L	H	N	Y	N	Victim-End
ANN [13]	H	L	H	L	H	L	N	Y	NA	-
Two-Layer Approach [14]	M	H	M	M	M	M/L	N	Y	N	-
CEP [15]	H	L	M	L	H	H	N	Y	NA	-
Packet Filtering [2]	H	M	M	M	L	L	Y	N	NA	Source-End
Weight Fair Throttling [17]	H	L	L	L	L	H	Y	N	Y	Intermediate
SAVE [18]	M	L	M	L	H	M	Y	N	N	Source-End
SOS [17]	L	H	L	M	L	M	Y	N	Y	Source-End
D-WARD [20]	H	L	H	L	M	M	Y	Y	N	Source-End
IP Traceback [11]	L	L	L	M	L	H	Y	Y	Y	Victim-End
Konasite Defender [21]	H	L	L	L	L	H	Y	Y	Y	Intermediate
PSO [22]	H	H	H	M	L	H	Y	Y	Y	-

A- Accuracy	DL- Delay	P- Prevention	OH- Overhead
RT- Responce time	D- Dectection	P- Reliability	DR- Detection Rate
RC- Recall	DT- Deployment Type	H- High	L- Low
M- Moderate			

works very well as many high profile companies including Microsoft are using it to mitigate and detect the effect of DDoS attack.

Moreover, ANN based Intrusion Detection System uses supervised learning algorithms, along with neural networks. The ANN model detected attack against a simulated IoT network demonstrating with over 99.4 percent accuracy. Packet filtering is a DDoS attack prevention technique being used for years, it also works fine when it comes to prevent network from DDoS attack but give medium-level reliability. FOCUS applies fog computing based approach so that DDoS attacks can be detected by adopting a two-level security approach by making use of VPN. However, post attack analysis isn't done by it.

5 RECOMMENDATIONS

Hence, on the basis of techniques discussed, Swarm intelligence based technique that uses multi-agent system provides least time for DDoS attack detection time and recovery from attack is also done with almost 98 percent accuracy. It also tends to offer better security and optimum performance IoT environment. Simultaneously, ANN based IDS model detects DDoS attack by using different low cost ML algorithms and checks network traffic patterns to analyze attack packets to provide almost 99.4 perccent accuracy. So, we recommend Particle Swarm Optimization based DDoS attack defense mechanism and ANN based IDS as they seem to be more promising in terms of detection and then providing security to the network.

6 CONCLUSION AND FUTURE WORK

The major influx of IoT devices has specifically broadened the chance of vulnerability of infamous DDoS attacks. DDoS attacks are factual to occur and there exist many techniques to detect and prevent networks from DDoS attacks. Various techniques for DDoS attack detection system and prevention mechanism have been proposed to check how detection and prevention is done in networks against these attacks and comparative analysis is done to determine the optimal technique that provides better tradeoff between security and network performance during and after attack. Hence, it is learnt that various techniques make use of filtering and rate-limiting techniques to detect and prevent DDoS attacks with higher reliability. Regarding future work, we will be exploring latest artificial intelligence and machine learning based detection and prevention techniques in IoT domain. Furthermore, we will assess various other performance evaluation parameters that need to be balanced against each other precisely and appropriately for better security in IoT.

REFERENCES

[1] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[2] H. Zare, M. Azadi, and P. Olsen, "Techniques for detecting and preventing denial of service attacks (a systematic review approach)," in *Information Technology-New Generations*. Springer, 2018, pp. 151–157.

[3] T. Shah and S. Venkatesan, "A method to secure iot devices against botnet attacks," in *International Conference on Internet of Things*. Springer, 2019, pp. 28–42.

[4] Y. Lee, W. Lee, G. Shin, and K. Kim, "Assessing the impact of dos attacks on iot gateway," in *Advanced Multimedia and Ubiquitous Engineering*. Springer, 2017, pp. 252–257.

[5] M. Shabbir, M. A. Khan, U. S. Khan, and N. A. Saqib, "Detection and prevention of distributed denial of service attacks in vanets," in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2016, pp. 970–974.

[6] M. Shabbir, M. A. Khan, U. S. Khan, and N. A. Saqib, "Detection and prevention of distributed denial of service attacks in vanets," in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec 2016, pp. 970–974.

[7] L. R. Brasilino and M. Swany, "Mitigating ddos flooding attacks against iot using custom hardware modules," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, 2019, pp. 58–64.

[8] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating dos attacks targeted on iot networks," in *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*. IEEE, 2017, pp. 1–4.

[9] R. Abbas, I. Ibrahim, M. Masoudi, and J. Pacione, "Iot network security based on machine learning techniques for ddos threats mitigations," 2019.

[10] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, "Protecting iots from mirai botnet attacks using blockchains," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2019, pp. 1–6.

[11] A. Gupta and B. Gupta, "Honeynettrap: Framework to detect and mitigate ddos attacks using heterogeneous honeynet," in *2017 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2017, pp. 1906–1911.

[12] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, and Z. Ye, "Focus: A fog computing-based security system for the internet of things," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2018, pp. 1–5.

[13] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat analysis of iot networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2016, pp. 1–6.

[14] S. Toklu and M. Şimşek, "Two-layer approach for mixed high-rate and low-rate distributed denial of service (ddos) attack detection and filtering," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7923–7931, 2018.

[15] A. M. da Silva Cardoso, R. F. Lopes, A. S. Teles, and F. B. V. Magalhães, "Real-time ddos detection based on complex event processing for iot," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2018, pp. 273–274.

[16] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, p. 1550147717741463, 2017.

[17] M. Wisthoff, "Ddos countermeasures," in *Information Technology-New Generations*. Springer, 2018, pp. 915–919.

[18] K. Kalkan, G. Gür, and F. Alagöz, "Filtering-based defense mechanisms against ddos attacks: A survey," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2761–2773, 2016.

[19] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, "Towards iot-ddos prevention using edge computing," in {*USENIX*} *Workshop on Hot Topics in Edge Computing (HotEdge 18)*, 2018.

[20] C. Zhang and R. Green, "Communication security in internet of thing: preventive measure and avoid ddos attack over iot network," in *Proceedings of the 18th Symposium on Communications & Networking*. Society for Computer Simulation International, 2015, pp. 8–15.

[21] P. Kamboj, M. C. Trivedi, V. K. Yadav, and V. K. Singh, "Detection techniques of ddos attacks: A survey," in *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)*. IEEE, 2017, pp. 675–679.

[22] R. Kesavamoorthy and K. R. Soundar, "Swarm intelligence based autonomous ddos attack detection and defense using multi agent system," *Cluster Computing*, vol. 22, no. 4, pp. 9469–9476, 2019.