Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.9854899

A REVIEW ON IOT DDoS TECHNIQUES

Owais Farooq
Research Scholar, Department of Computer Science and Engineering, Glocal School of Technology, Glocal University, UP, 247121, India, owaisuzair61@gmail.com

Dr. Mohammad Mazhar Iqbal
Associate Professor, Department of Computer Science and Engineering, Glocal School of Technology, Glocal University, UP, 247121, India

ABSTRACT

Internet of things (IoT) is become the most important part of the human life in a short span of time. Humans are having their surroundings with lots of IoT devices like sensors, actuators, sensing devices, and many more. The major criteria of IoT devices are to provide connectivity to the device, human, or things which do not have any processing element. However, security is one of the main challenges in IoT due to its always connected feature. The DDoSs are kind of malware which creates its team of compromised devices and make it large by affecting other devices also. There are several attacks which may affect the devices like DDoS, click fraud, phishing, and ransomware. This paper covers several components of IoT DDoS and with its detection techniques. It also covers several open challenges and future work in the field of detection of IoT DDoS.

Keywords- IoT, IoT DDoSs, Detection Techniques for IoT DDoS, Components, Future Challenges.

1. Introduction

The IoT plays a significant role in today's modern world, where everything is linked through the internet. The majority of people are drawn to this creative solution because it allows them to enjoy their lives despite their hectic schedules. Consider how an air-conditioner will be able to track their contents and place orders with the user if anyone wants cooler or hot environment with just hand gesture or any voice assistance from bed. Similar to those used by Google Assistant, Apple Siri, and Amazon Alexa. This kind of ease can be possible due to distinguish smart devices like the Alexa, smart gadgets, sensors, and Amazon echoes, etc. [1]. Kevin Ashton proposed the Internet of Things idea in 1999. The IoT is described as the connected objects which are identifiable using the RFID technology. IoT is characterized in a variety of ways by numerous researchers, including [2]:

1.1 Origin of IoT

As displayed in Figure 1, the Internet of Things has developed after some time thusly. In the pre-web time, otherwise called the "H2H" or "Human-to- Human" time, individuals had fixed or portable communication. With the exception of the way that SMS administrations were a significant method of correspondence. After the joining of savvy organizations, the web was conceived, and the "www" or "internet" time further developed correspondence, information, and amusement, in addition to other things. Besides, savvy IT stages and administrations were added to "www," coming about in the "web 2.0" period, which totally changes everything into computerized change, including e- usefulness, web based business, etc.

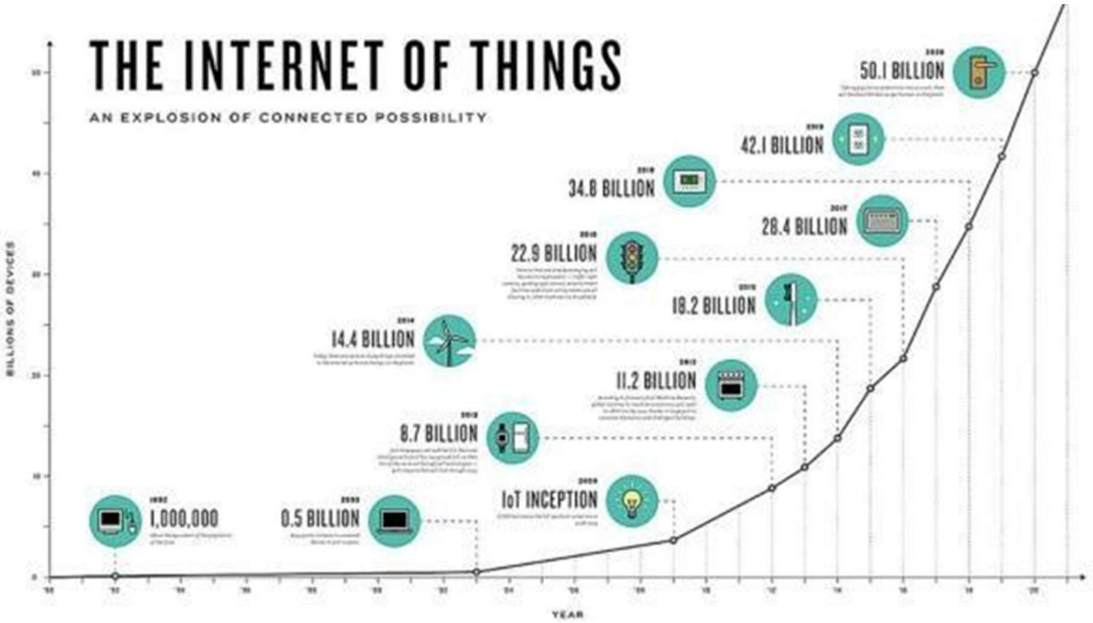

Fig. 1: Evolution of IoT

The next age is known to be the “social media” era, which includes mobile phones and apps such as Skype, Facebook, and YouTube. Furthermore, the humans are live in the “M2M” age, that can be possible by using IoT, as well as smart devices, artifacts, and data. The machine can identify, track, and control items with smart devices, and IoT also allows for automation, actuation, and payment.

2. IoT DDoS and its Components

IoT unit threats are a critical issue since they are difficult to fix and overcome. The attackers have a simple way of affecting these. After 2008, the existence of IoT DDoS was recognized. Nonetheless, it was not until 2016 that the magnitude of the threat they posed was recognized [1]. In general, DDoS characterize the network of infected end-hosts (also known as bots), and the network can be managed with the help of human being which called botmaster. DDoS use techniques similar to those used by other malware engineering, etc. [4], such smart gadgets create a C&C architecture among themselves so that malicious activities can be carried out. As a result, the bots provide the following services to Botmaster [3]:

- A connectivity of the network
- A bot which affects the network connectivity
- A DDoS with full of compromised devices.
- The recovery and monitoring of network from the bots.

2.1 IoT DDoS Components

There are several components in an IoT DDoS, those are listed below:

i) **C&C Server:** The DDoS's centralized server, which acts as a controller and transmits and receives data to affect the network. It usually follows a client- server architecture with peer-to-peer networking.

classes to recruit vulnerable models like applications,

ii) **Peer-to-Peer (P2P) DDoS:** To guarantee extra social- protection from takedowns, a decentralized bot network known as the P2P DDoS is utilized. While P2P-DDoSs can have a C&C server, they can likewise run without one and are coordinated randomly to conceal the DDoS and its objective. Despite the fact that P2P DDoSs are more uncertain, the botmaster can't screen and execute control conveyance as soon as possible.

iii) **Botmaster:** The botmaster, otherwise called the bot herder or DDoS regulator, is accountable for the DDoS's activity. The remote botmaster sends orders to explicit DDoSs and C&C servers, which control the DDoS. To forestall the botmaster's authorization and recognizable proof, the botmaster's area and name are kept stowed away.

iv) **IoT Bot:** The gadget is characterized as a DDoS network gadget associated with the Internet. The majority of the PC framework is utilized as a bot, yet a cell phone can likewise be utilized as a DDoS part with the approach of the innovation. DDoS get functional guidelines either from similar organization bots or straightforwardly from the botmaster or from a C&C server.

v) **Affected Device:** It is an elective name for zombie or bot. For controlling the bot an outer individual or a PC is utilized; a bot is hence called 'zombie' and a DDoS is alluded to as a "zombie armed force."

vi) **DDoS Attack:** By appropriating bot malware to contaminate PCs and extra frameworks, the botmaster gets a DDoS. He could likewise rent an extra criminal to a current DDoS. A recently gathered bot or "zombies" is accounted for to the DDoS C&C. C&C controlled these bots and potential casualties address records, email formats and malware documents are conveyed as per C&C rules. These bots are currently constrained by C&C. Numerous potential casualties get email messages from botmaster's organization from the tainted bots.

3. IoT DDoS Detection Mechanisms

IoT DDoS detection and monitoring are typically a major topic of research in recent years as a consequence of an increase in malicious activity. Due to malicious activity, the DDoS issue has been analyzed until recently by little proper research. As discussed below, researchers have therefore suggested different bot detection methods. There are several ways to detect the IoT DDoS like Intrusion Detection System [12], Honeypots, Filtering, Honeynets [13, 15], and Encryption. In this section, a taxonomy of detection mechanism is covered which is explained in Figure 3.

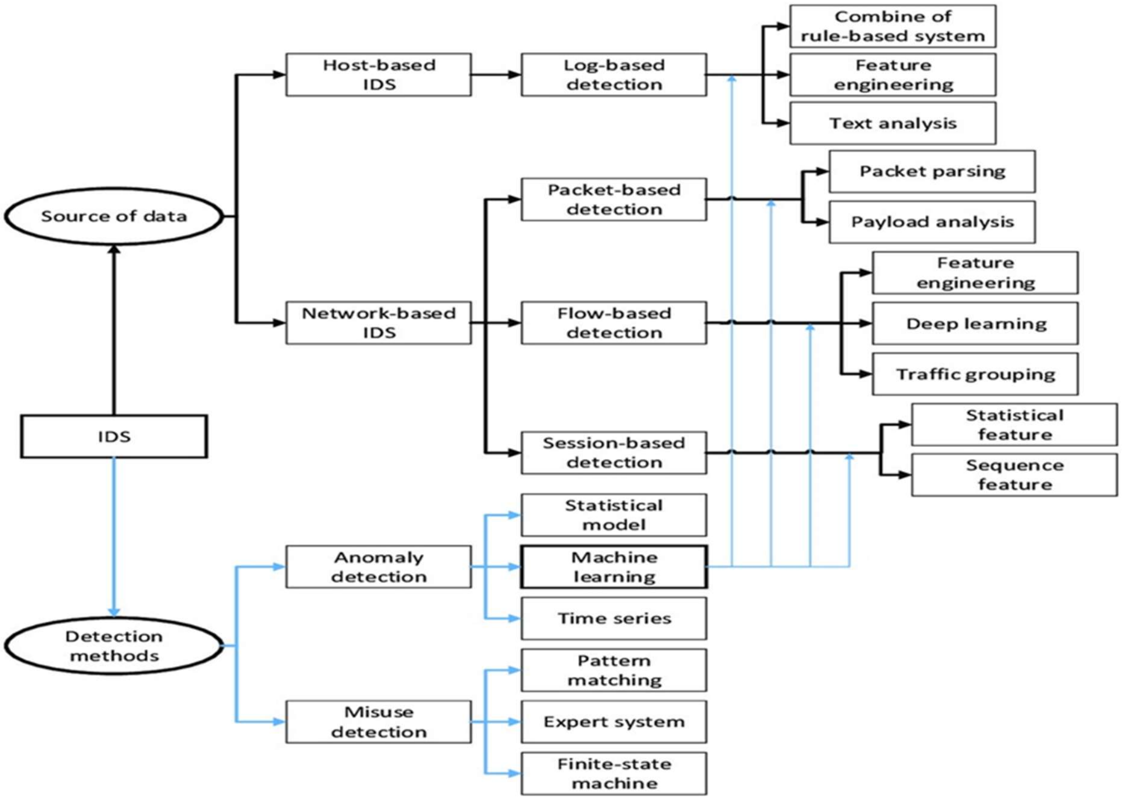

Fig. 3: A Taxonomy of IoT DDoS Detection Mechanism [5]

i) Honeynet: Honeypot and Honeywell collaborate to create a method based on Honeynet [8]. Honeypot is a computer system that helps to attract an intruder to target a specific computer system in terms of protection. This lovely lady should function as a terminal host. The honeynet's traffic is monitored, recorded, managed, and updated, for example, by snort [7], which can be hacked in a short period of time and is much more vulnerable to malicious attacks. The computer systems that are used as Honeypots have no value in terms of output. Most communications between other systems and the honeypot are distrustful or suspicious based on this theory, and should be investigated. A honeypot web server, for example, may be placed in a specific location on your network. Since this server is a honeypot with no useful tasks, any interaction with it is considered an unwanted entry or a malicious operation. A similar Honeynet was developed [6], allowing Honeywell's portion to analyze and capture all payloads on site traffic for accessing DDoS- related information such as the corresponding port number of the C&C server's DNS/IP address, and authentic data required for the C&C channel to register, as well as isolating the Honeypots from other honeypots.

ii) IDS: IDSs are utilized to caution the overseeing site when framework arrangements are abused, framework assets are checked for noxious conduct, or different infringement happen. These IDS may take the form of a hardware device or a software program. An IDS detection function [17, 20, and 21] has signatures for a number of well-known DDoSs, which is a big plus. The key drawbacks of such strategies, however, are as follows: the primary security which is based on the filtering of the content communicated in the network. Then a misuse-based IDS technique is used for the known attacks as the primary phase of the detection. If the detection is not done by the misuse-based detection mechanism, it can be done anomaly-based detection for new enabled DDoSs [20]. These detection methods are further divided into three categories: misuse, anomaly, and DNS IDSs [18].

a) Misuse-based IDS: This method is sufficient for trapping bots using the available information as well as the current bot's signature. Researchers compiled a library of specific DDoS feature names and instructions that could be used and summarized in the IDSs proposed by different researchers to define DDoSs. The IDS may raise an alarm and take further action against the DDoS if it finds corresponding search phrases while analyzing the payload's content, but this approach is limited to identifying only known DDoSs. Snort [11], for example, is a popular open-source intrusion detection system that searches for matches against a predefined set of signatures and guidelines while monitoring network traffic for signs of intrusion.

b) Anomaly-based IDS: This approach looks for unusual or abnormal device behavior to detect danger, malicious risk. In this context, "abnormal" behavior generally refers to bot detection as a deviation from "normal" action as described by some guidelines. To classify DDoS customers and reveal DDoS servers, Sigh and Binkley [9] proposed a successful TCP-based anomaly detection system with IRC tokenization and IRC message statistics. In this anomaly-based approach, an IRC parsing portion is first implemented, which collects TCP packet information and decides the IRC channel. Furthermore, the scanning operations are carried out on a broad sampled data set that is linked to IRC channel traffic [10]. Finally, the IRC routes with strong testing matter will be stamped as DDoS stations that are reachable. Akiyama et al. [16] suggest a three-metrics-based calculation that aids in the detection of irregular DDoS behaviors. All of the bots were thought to have identical coordination, responses, and relationships since they were all part of the same DDoS. Gu et al. [14] suggested BotHunter, a DDoS detection method. Using a user- defined bot infection life cycle model, this detection system runs a correlation algorithm to help identify the bot infection process.

c) DNS-based IDS: To analyze DNS traffic, this detection method combines data mining and behavior-based approaches. Consider the reasons DNS queries are used in many DDoS phases, such as C&C server updates, malicious attack initiation, and the rallying mechanism after infection, which is an advantage of the strategy.

iii) ANN based DoS Detection: An Artificial Neural Network (ANN) [22] is a data-processing viewpoint that is influenced by the way natural tangible frameworks, such as the brain, measure data. The clever generation of information dealing with structure is an important aspect of this perspective. It is made up of an infinite number of highly interconnected dealing with sections (neurons) that work together to solve unambiguous problems. Through a learning cycle, an ANN is sorted out for a given application, such as plan confirmation or data request. Acclimatation to the synaptic linkages that occur between the neurons are part of learning in regular structures. This is also significant for ANNs. With their incredible ability to extract meaning from jumbled or ambiguous data, brain connections can be utilised to eliminate plans and distinguish designs that are too unpredictable to be detected by humans or other computer techniques. In the grouping of knowledge it has been given to examine, a pre-arranged brain association can be regarded a "subject matter expert." ANN is used in [23] to denote a relationship formed during an assault. In this execution, data from an association testing stage is sent into a three-layer feed forward brain association, which can output 1 when there is an attack and 0 when there isn't. In fact, [22] has offered a strategy for regulating the redesign of ANN's farthest reaches of acknowledgment. They suggested using fleecy clustering as a pre-treatment for ANN preparedness. In all of the above methods, ANN is set up using standard and attack traffic data, and ANN determines if an attack is present or not.

iv) Packet Filtering DoS Detection

Parcel sifting must precisely catch bundles streaming on the internetwork where different gadgets are associated by numerous switches. Along these lines, in the organization bundle catch step, the initial step of this paper, a parcel is caught utilizing WireShark, an open-source bundle investigation program, and a separating interaction is performed to choose bundle information with noxious qualities. In bundle sifting, a record executed in a virtual climate utilizes WireShark to break down parcels that are expected to be sent through the organization. WireShark is adaptable in recognizing malignant bundles by compacting how much log information connected with the organization via consequently showing nitty gritty data inside the parcel information sent and got by the executable document, as well as catching just the particular bundles required through the separating capacity. In the element sifting step, initial, a standard for choosing parcels that perform noxious activities from a tremendous measure of informational collections is expected in light of the succession of organization bundles essentially found in pernicious codes and the recurrence of purpose. To begin with, highlights that show major pernicious practices are chosen by the request and recurrence of calls of organization parcels by different malevolent codes found through past examinations, and these are created as marks. The produced mark is a list that can determine whether a malignant code exists, as well as whether a comparable mark exists in another executable document in the informational index. If the mark through the examination activity makes a similar bundle call request and recurrence, it's possible that the comparative information is used to carry out an organization-related vengeful movement.

Zhou [24] examined the recognition of discrepancies for information security and confirmation as per network bundle development and internetwork, but it is applied to DTE (Data Terminal Equipment), so it is fundamentally subject to the host. Huda [25] proposed a malicious code identification model based on a deep conviction network method to protect the current control framework network connected to IoT devices from digital threats. API calls were extracted as items from the informational index to break down and get a handle on the attributes of the harmful code. A malicious code detection model was also built, which learns the extracted API calls and uses a profound conviction network technique to determine if there is a malicious code, although the precision isn't high due to limited data collection.

HaddaPajouh [26] suggested a strategy for detecting malicious codes by eliminating OPcodes and learning them in an LSTM model to protect IoT devices used in various IoT enterprises from malicious codes. As informational collections, 281 pernicious codes and 270 non-vindictive data were used to build a noxious code finding model. To obtain proficiency with the OPcode isolated as a malignant code trait, a model was developed by varying the number of layers in the LSTM model. Another nefarious code has been discovered.

4. Open Challenges and Discussion

The typical DDoS consists of smart IoT devices accessed remotely using the Internet and configured to send data to other computers on the Internet. Mechanical sensors, cars, industrial and home equipment, cardiac implant displays, and a variety of other devices with IP addresses and the ability to relay data over a network are all part of the Internet of Things. These are referred to as things in the sense of the Internet of Things. In general, DDoSs characterize the network of infected end-hosts (also known as bots), and these networks are actually managed by a human being known as the Botmaster. DDoSs use techniques similar to those used by other malware organizations to recruit vulnerable models. DDoSs have become a worldwide phenomenon, and the botmaster is responsible for keeping track of a large number of vulnerable hosts in domains all over the world. The study of DDoSs, as well as the identification of a DDoS, raises a slew of problems. The following are the key problems with DDoS detection on a large scale:

Assessing the impacted DDoS period is one of the main elements in determining the DDoS's severity. Pre-existing detection techniques are usually inaccurate in calculating DDoS measurements, and the figures generated are only useful for a limited range of DDoS sizes.

Due to clear conflicts over laws regulating the operation of secure IT services as well as some data protection laws, the applicability of assured detection and mitigation techniques is restricted [19]. Since complete datasets are not readily available to the researcher group, researchers have a difficult time comparing their findings to previously published benchmarks. Real traces are difficult to come by, and scientists need content to evaluate the functionality of their methods on small data trace sets, which is a difficult task due to heterogeneity (differences in hardware, software, architectural design, etc.) On the network, many datasets aren't well-known. Another terrifying threat in this area is the DDoS phenomenon, as well as its detection, which is caused by the increasing expansion of Internet use and computing capabilities (e.g., GPRS, 3G, and Wi-Fi) for mobile devices such as hand-held devices and smartphones. Furthermore, DDoS detection mechanisms are limited by a variety of factors, including I tracking other mobile devices (ii) SMS messages (iv) GPS data (v) a crowded phone service
(vi) limited bandwidth (vii) limited battery power. When a hacker uses a DDoS of hundreds or thousands of objects, each with its own unique IP address, it's nearly impossible to stop the attack or even differentiate legitimate owners from a slew of imposters. DDoSs aren't a novel idea in today's world. Hackers have been using DDoSs to gain access to unsecured products (usually computer systems) in order to launch DDoS attacks since at least the year 2000. On the other side, the Internet of Things exacerbates the problem. There was a plethora of low-cost Internet-connected gadgets on the market, including webcams, baby monitors, thermostats, and, of course, yoga mats and fry pans, all of which had their own IP address. Even if their devices have limited or no built-in protection, subscribers sometimes forget the

simple step of creating a password for them. As a result, online hackers trying to build and use a DDoS would find them easy targets.

Dyn, a vital Internet infrastructure provider, was taken down in 2016 by a DDoS comprising 100,000 unsecured Internet of Things computers. As a result, several high-profile and high-traffic websites were forced to take a break from the Internet. This DDoS was created using the Mirai malware, which automates the co-opting of these unsecured computers and is freely available. To put it another way, it wasn't a genius programmer who came up with fresh and inventive technology, but rather someone who repurposed old code. DDoSs can be used in a number of ways by hackers, including DDoS attacks. They can be used for click fraud, spam filter evasion, password guessing speed, and anything else that requires a large network of computers to work together. They can be used to commit click fraud. Criminal organizations can rent DDoS time for any mission they want, which is a well-kept secret. The ideal solution would be for all IoT devices to run safe apps, but this is unlikely to happen. Most IoT devices aren't designed to be safe, and there's no way to increase security. Millions of devices have already been manufactured, sold, and used. DDoSs are also likely to become a bigger problem in the future, as the use and manufacture of IoT devices is projected to increase dramatically in the coming years. Furthermore, the protection measures in place to thwart attackers can be easily overwritten, outdated, or ineffective.

5. Conclusion

Following the first DDoS workshop in 2007, various researchers proposed various DDoS detection techniques, and some systems were introduced with real bot detection methods based on some of these techniques. DDoS identification is one of the most difficult problems to solve. As a result, this paper described a comprehensive survey of DDoS detection methods. Furthermore, DDoS detection methods are divided into two categories: honeynets and intrusion detection systems (IDS), with other detection techniques in each category being discussed.

Future directions expect the advent of new IoT technologies, and it is clear that the IoT will be unable to provide the same services in terms of addressability, scalability, concurrency, interoperability, and versatility if technology progresses at a similar pace in the coming years. DDoSs may become more prevalent in such networks as a result of such issues, posing a risk to users. As a result, some techniques to aid in the resolution of these issues will be needed.

References

[1] Engrish, Kishore. "Turning internet of things (not) into the internet of vulnerabilities (Nov): It DDoSs." arXiv preprint arXiv: 1702.03681 (2017).

[2] Ray, Partha Pratim. "A survey on the Internet of Things architectures." Journal of King Saud University-Computer and Information Sciences 30.3 (2018): 291-319.

[3] P. Wang, S. Sparks, and C. C. Zou, “An advanced hybrid peer-to-peer DDoS,” in Proc. In Workshop on Hot Topics in Understanding DDoSs, 2010.

[4] Chao Li, Wei Jiang, Xin Zou,” DDoS: Survey and Case Study,” 4th International Conference on Innovative Computing, Information and Control, 2009.

[5] Karim, Ahmad, et al. "DDoS detection techniques: review, future trends, and issues." Journal of Zhejiang University SCIENCE C 15.11 (2014): 943-983.

[6] Hossein Rouhani Zeidanloo, Azizah Bt Manaf, Payam Vahdani, Farzaneh Tabatabaei, Mazdak Zamani," DDoS Detection Based on Traffic Monitoring" IEEE transaction,2010.

[7] G. Schaffer, "Worms and Viruses and DDoSs, Oh My: Rational Responses to Emerging Internet Threats", IEEE Security & Privacy, 2006.

[8] Xiaonan Zang, Athichart Tangpong, George Kesidis, and David J. Miller, CSE Dept Technical Report on "DDoS Detection through Fine Flow Classification" Report No. CSE11001, Jan. 31, 2011.

[9] J. Binkley and S. Singh, "An algorithm for anomaly-based DDoS detection" In Proceedings of USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI), pages 43– 48, 2006.

[10] D. Dagon, G. Gu, C.P. Lee, W. Lee, "A Taxonomy of DDoS Structures," in Proc. 23rd Annual Computer Security Applications Conference (ACSAC 2007), 2007, pp. 325-339.

[11] M. Roesch, "Snort-lightweight intrusion detection for networks," In Proceedings of the 13th USENIX conference on System administration, pages 229–238. Seattle, Washington, 1999.

[12] Liu, L., Chen, S., Yan, G., et al., 2008. BotTracer: execution-based bot-like malware detection. In: Information Security. Springer Berlin Heidelberg, p.97-113. [doi:10. 1007/978-3-540- 85886-7_7].

[13] Stinson, E., Mitchell, J.C., 2007. Characterizing bots' remote control behavior In: Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, p.89-108. [doi:10.1007/978-3-540-73614-1_6].

[14] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: Detecting malware infection through ids-driven dialog correlation" In Proceedings of the 16th USENIX Security Symposium, pages 167–182, 2007.

[15] Provos, N., 2004. A virtual honeypot framework. USENIX Security Symp.

[16] M. Akiyama, T. Kawamoto, M. Shimamura, T. Yokoyama, Y. Kadobayashi, and S.Yamaguchi, "A proposal of metrics for DDoS detection based on its cooperative behavior," In Applications and the Internet Workshops, 2007. SAINT Workshops in 2007. International Symposium on, pages 82–82, 2007.

[17] Wurzinger, P., Bilge, L., Holz, T., et al., 2009. Automatically generating models for DDoS detection. Computer Security ESORICS, p.232- 249.

[18] Stalmans, E., Irwin, B., 2011. A framework for DNS based detection and mitigation of malware infections on a network. IEEE Information Security South Africa, p.1-8.

[19] Plohmann, D., Gerhard-Padilla, E., Leder, F., 2011. DDoSs: Detection, Measurement, Disinfection & Defence. The European Network and Information Security Agency (ENISA).

[20] Kugisaki, Y., Kasahara, Y., Hori, Y., et al., 2007. Bot detection based on traffic analysis. IEEE Int. Conf. on Intelligent Pervasive Computing, p.303- 306.

[21] Goebel, J., Holz, T., 2007. Rishi: identify contaminated bot hosts by IRC nickname evaluation. Proc. 1st Conf. on 1st Workshop on Hot Topics in Understanding DDoSs, p.1-12.

[22] G. Wang, J. Hao, J. Ma, and L. Huang, "A new approach to intrusion detection using artificial neural networks and fuzzy clustering," Expert Systems with Applications, vol. 37, pp. 6225V6232, 2010.

[23] S. Seufert and D. O’Brien, “Machine learning for automatic defense against distributed denial of service attacks,” Proceedings of IEEE International Conference on Communications, ICC’07, pp. 1217-1222, June 24-28, 2007.

[24] Alireza S, Rahil H. A state-of-the-art survey of malware detection approaches using data mining techniques. 2018. p. 1-22.

[25] Donghao Z, Zheng Y, Yulong F, Zhen Y. A survey on network data collection. Journal of Network and Computer Applications. 2018. p. 9-23.

[26] Shamsul H, Suruz M, John Y, Sultan A, Hmood AD, Robin D. A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks suing deep belief network. 2018. p. 23-31.