IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

Survey on Internet of Things Botnet Detection Methodologies: A Report

B. P. Sreeja

Department of Information Technology, Karpagam College of Engineering, Coimbatore, India

E-mail: sreejabp@gmail.com

Abstract

Recently, Internet of Things (IoT) botnets have emerged as a serious security risk. IoT-related systematic and thorough research on botnet detection techniques' relevance are few. Therefore, this report seek to compile a comprehensive overview of experimental research related to the detection of IoT botnets and then evaluate it. Moreover, it builds a foundation of information about IoT botnet detection techniques. In this work, the gaps in research are studied and recommendations are made for future studies.

Keywords: Internet of Things, botnet detection, network protocols, network security, clustering

1. Introduction

A botnet is a group of computers that a hacker may manage from a distance. The botmaster and the bot slave are the two key players in a botnet, which are referred collectively as a botnet. As a botmaster's slave, the enslaved individual performs as instructed by the master. In order to carry out assaults, the botnet instructs the bot clients to follow the commands of their master and become slaves to the botmaster. Anti-malware software are unable to identify botnet assaults since they take place so quietly. Peer-to-peer networks have become a difficult target for botnet operations since it is difficult to locate the command center. Although botnet command and control operations are difficult to decipher, patterns in data may be found to create a comprehensive picture of how data flows across a network, and this can lead to the discovery of the botmaster behind the attacks [1-5].

To launch a DDoS assault, the botmaster uses powerful computers and servers to execute a malware software that gives instructions to the machines underneath it that are referred as handlers. Clients are attacked and enslaved by these handlers. Detection of a botnet's harmful behavior may be done in a number of ways. However, malware detection

DOI: https://doi.org/10.36548/jsws.2022.3.005
Received: 02.08.2022, received in revised form: 20.08.2022, accepted: 05.09.2022, published: 15.09.2022

software has a tough time detecting these assaults, as seen by the following facts. Botnet simulation data on virtual computers is often used to analyze network traffic and choose optimal communication pathways. The TCP and UDP protocols are used to transfer data across computer networks [6- 9].

Personal and corporate information is increasingly being exchanged over the Internet, which links billions of computers, tablets, and smartphones across the world. Its weaknesses are exploited by black hat hackers to carry out attacks. While these cyber thieves first set out to achieve notoriety, they've now switched their focus to financial gain [10]. Bot and network are the root terms of the phrase "botnet". When a device is infected with malicious code, it becomes part of a network of infected devices known as a "net" that is under the control of a single attacker or group of attackers. There are occasions when the term "zombie army" is used to refer to both the bot and the botnet. Malware is distributed automatically and without the user's knowledge via bots and zombies, both of which have similar meanings. Rather than focusing on a single person, business, or industry, botnet malware usually scans the Internet for weak points. As many linked devices as possible are used to create a botnet in order to do automatic activities that the devices' owners aren't even aware of.

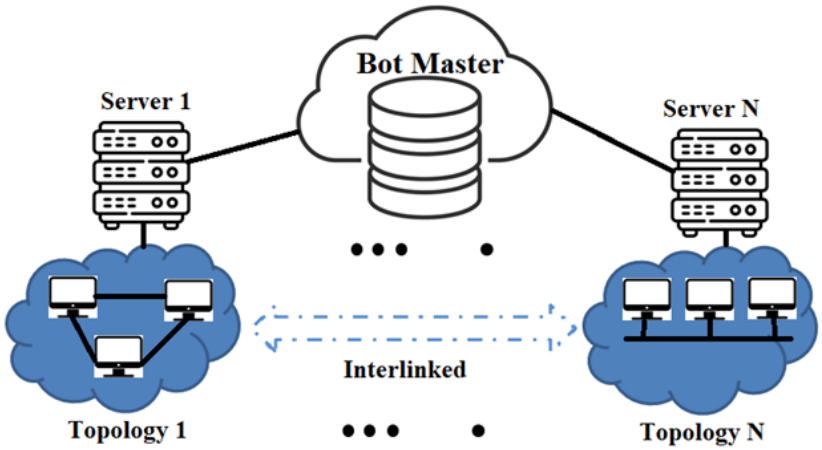

Figure 1. Standard Botnet Structure

Attacks on the Internet represent a huge concern since botnets are able to control millions of Internet-connected devices simultaneously. Botmasters use a variety of communication protocols to reach the botnet's command and control site. An crucial Internet service known as "Domain Name System" (DNS) is one of the most used protocols for communicating over the Internet. Domain Generation Algorithms (DGA) and fast-flux approaches are used by botmasters to avoid static blocklists and reverse engineering while maintaining their flexibility. As a result of this unusual DNS traffic generated by a botnet's

DNS connection, the existence of DNS-based botnets in the network may be determined. Even though DNS traffic analysis has been recommended as a technique to detect botnets, the issue persists and is difficult to fix for a number of reasons, including not taking into consideration the crucial characteristics and rules that assist in finding DNS-based botnets.

According to Klaus Schwab, the fourth industrial revolution was built on the great accomplishments of the third revolution, including the Internet, tremendous processing power, the ability to store information, and the endless potential for knowledge [11, 12]. Internet of Things (IoT) intends to link millions of smart items and devices in a seamless manner, using enormous volumes of data from heterogeneous IoT devices to sense, process, and analyze the data.

There are a wide range of applications for detecting botnets, from cyber security and banking to healthcare and law enforcement. Most conventional rule-based and flow-based detection approaches may not be able to identify bot activities quickly and effectively as botnets get more complex and deadly every day. As a result, developing a reliable and quick botnet detection solution is crucial.

The Internet of Things (IoT) has gotten out of hand, and cybercriminals are now taking advantage of this by targeting IoT devices for assault. As a result, mitigating the dangers of IoT device security has never been more important than it is now. Among the most serious and pervasive threats to IoT devices are botnet assaults, which are becoming more common. Lack of memory and compute power in immobile IoT devices make them vulnerable to attack.

1.1 Motivation of this research

Defending and responding to IoT botnet attacks is a top priority for organizations using the Internet of Things (IoT). The identification of IoT botnets and the overall security of the IoT ecosystem might benefit from a variety of methodologies and technologies. There is, however, a paucity of in-depth investigations on IoT botnet detection systems and a lack of systematization for such solutions in recent literature. As a result, the study is still in its infancy and has a great deal of promise.

2. Literature Survey

IoT anomaly detection using machine learning was studied by Al-Hajri et al. [13]. Auto-encoder methods for detection were examined by the researchers, and they proposed

future research topics that might help machine learning algorithms in this field. The study's closest collaborators, Ali et al. [14], summarized their findings. For IoT botnet avoidance, they conducted a study on IoT user demographics, then divided the available methods into two broad categories: preventative and remedial.

According to S. Dange et al. [15], machine learning techniques were used to investigate a variety of probable IoT assaults and determine the relative importance of each attack type for botnets. IoT botnet forensics and deep learning techniques were evaluated by N. Koroniotis et al. [16] and explored the difficulties and the existing solutions for both deep learning and IoT botnet forensics mechanisms. Autoencoder techniques in IoT botnet detection were also examined by R. Al-Hajri et al. [13], who performed a study as well as indicated prospective machine learning explorations in this field. Similarly, J. Sengupta et al., [17] conducted research on industrial IoT and blockchain assaults and security problems. They concentrated on blockchain-based solutions for IoT botnet detection since they thought it was a promising technology.

DNS-based botnets were identified using the following technique. Complex methodologies were used to identify features utilizing Principal Component Analysis (PCA) in the Gunner System approach [18]. Botnet detection relied on unusual DNS replies and querying activity, and data preparation improved the accuracy of the findings obtained. DNS characteristics were selected using IGR-based feature ranking. Information Gain Ratio (IGR), PCA, and chi-squared approaches were used to quantify the success of the feature detection process. The efficacy of each feature was given a score, which was used to calculate the information gain ratio. With this strategy, the amount of important attributes may be minimized while preserving accuracy. It was discovered by monitoring DNS activity on the Internet's backbone. When the botnet has been modified to include more strategies for evading system security, this sort of study will be very difficult. In peer-to-peer botnets, this is a common occurrence.

In paper [14] by Ali et al., the demographics of IoT botnet assaults were studied. In addition, several studies only looked at one form of IoT botnet malware without analyzing the appropriate detection techniques.

Taking all of this into account, it is clear that the stages of botnet creation were broken up in various ways in each research. Four sorts of assaults or harmful activities may be deduced from this examination and analysis: IoT botnets, DoS/DDoS, scanning attacks and IoT malware analysis.

3. IoT Botnets during the COVID-19 Pandemic

In January 2020, the WHO's Emergency Committee declared a global health emergency due to an increase in the number of new coronavirus cases being reported across numerous nations. The usage of the Internet has expanded as a result of this widespread epidemic of COVID-19 and its consequences. Because of this, all organizations, whether public and private, became digital and started to rely on the Internet and computer networks to share business data.

There was also an urgent need to take use of current technology because of changes in consumer behavior, new working methods, and constraints on traveling. This is why IoT is regarded one of the most promising new technologies in the battle against coronavirus epidemics. The patchy network of Internet-connected things is what makes up the Internet of Things (IoT). IoT is becoming more popular as COVID-19 expands. Many more gadgets are now able to connect to the Internet thanks to IoT. Despite this, most of the gadgets lack in many kinds of security [19, 20].

3.1 Botnets Detection on Internet of Things

The IoT has had a huge impact on our lives as a result of the digital revolution. IoT's rise, on the other hand, has led to a number of serious cybersecurity vulnerabilities. Detecting and mitigating attacks on IoT networks have lately attracted the attention of both the academic community and the private sector. Security measures such as intrusion detection and threat intelligence are often used by enterprises to identify and stop IoT botnets. Zero-day IoT botnets with no known signatures can't be detected by these approaches, which may be moderately successful. It is for this reason that research on IoT botnet detection systems is being conducted in both academia and industry. In most cases, the goal is to track out the source of an attack and limit the amount of traffic. Botnet architectures in IoT systems may be studied to improve security measures for spotting known and new botnets. It discusses more about how IoT botnets work, which means we're becoming better at stopping them [21]. Figure 2 shows the future IoT botnet detection which has two stages.

3.2 Data description

In the last several years, academics have been more interested in big data. When it comes to research that aims to design novel systems capable of processing enormous volumes of data throughout knowledge discovery's input, analysis and output phases have offered a complete evaluation of investigations. New data mining and analysis approaches are what

researchers have found most relevant. In contrast, the procedures used before and after the study have gotten less attention. The dimensionality of huge datasets may be reduced using evolutionary methods like accelerated particle swarm optimization [22].

3.3 IoT Botnets' basic components

Finding innovative and efficient techniques to locate and deal with Internet botnets is essential to limit their impact. It is also important to understand how these bots function in order to oppose them, keep cyberspace clean, and therefore contribute to the Internet's overall security. A number of fraudsters replicated and tweaked Mirai's source code to produce IoT malware that attempted to construct IoT botnets and compete to control the largest possible number of IoT devices [23]. IoT malware tends to follow a similar pattern of operation since it's a commonplace. These basic components are shown in figure 1.

3.4 Botnet detection using graph-based approaches

Anomalies may be detected using a variety of graph-based characteristics. Research in this area may be broken down into two basic categories: identifying abnormalities in static and in dynamic graphs. Simple charts and attributed graphs are subcategories of the static graphs. For the most part, the scholars have concentrated on examining the node networks that represent social ties. Both social interaction graphs and social correlation graphs have been addressed by the authors, and the suggested approach has been applied to a real-world case study. Researchers use clustering as a common strategy for detecting botnets using flow-based characteristics.

3.5 Flow-based detection strategies for botnets.

As IP traffic enters or departs an interface, NetFlow is able to capture it. High-speed data networks, such as botnets, may be detected using NetFlow-based (flow-based) characteristics. An example of a flow-based feature is a collection of packets that share a similar set of properties. If the packet properties of each box routed across the network are examined, it is possible to identify distinct flows. As the package's "fingerprint", these traits may be used to detect whether the container is unique or shares features with others [24, 25, and 16]. As a result, a number of academics have looked at the possibility of identifying network abnormalities using these properties. As a consequence, the literature on botnet detection based on net traffic is extensive, and several researchers have made substantial contributions to it.

3.6 Security Intelligence

Many people are concerned about the quality of data that is gathered and how it is used and stored, as well as the ethics of doing so. When COVID-19 patients have sensors attached to their bodies, the data sent from the sensors should be accurate, should reach its intended destination, should not be forged, should not be intercepted during transmission, and should be stored in an IoT computer's memory sicne it should not be accessible to all. Concerns have also been raised concerning how to prevent command and control channels from destroying the data they acquire.

IoT networks are scalable, but IoT devices have limited resources. As a result, traditional cryptographic algorithms are out of the question when it comes to securing the Internet of Things. Energy-efficient and less computationally intensive solutions to IoT network security should be implemented, rather than complicated algorithms that encrypt and authenticate IoT devices at every step along the way.

3.7 Self-organizing Map

As a type of unsupervised systems based on competitive learning, Self-Organizing Maps (SOMs) fight for activation amongst themselves. Adaptively and topologically organized, a SOM's principal objective is to discretize input data of any dimension into a one- or two-dimensional discrete map.

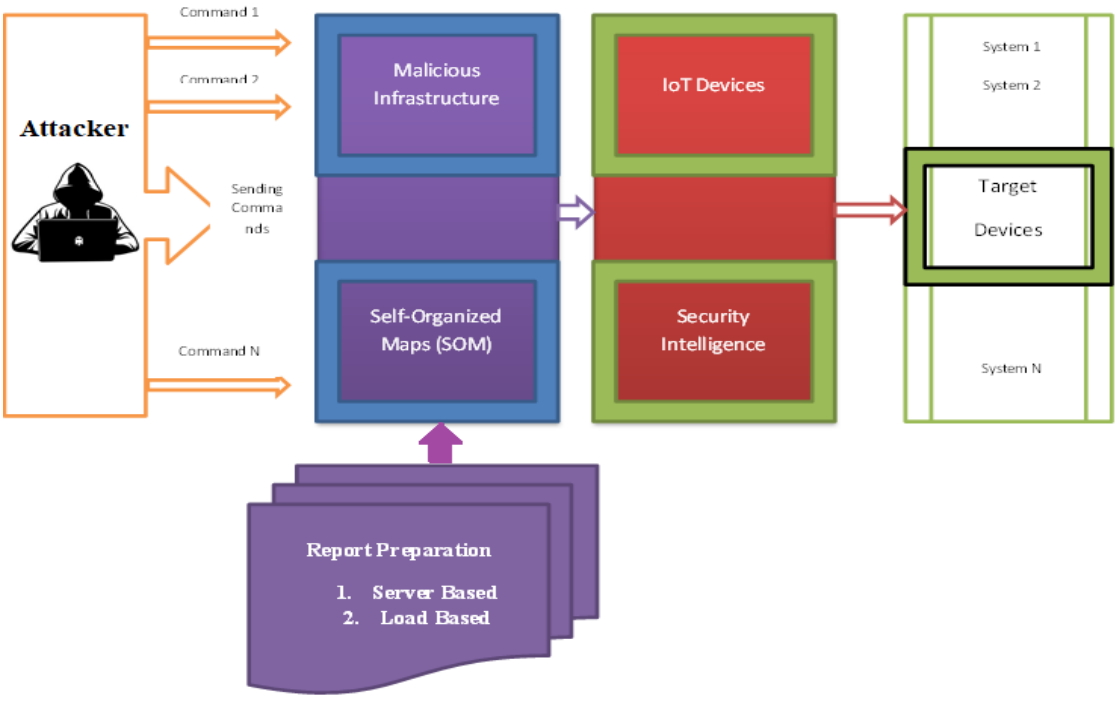

Figure 2. Future IoT botnet detection in two stages

4. Research Gap and Problem Finding

Botnets are notoriously difficult to track down due to their multi-platform functionality and ability to blend in with their surroundings. Since their footprints are typically disguised in diverse information spread at several levels, such as personal hosts and regional network backbones, and saved in different forms, this makes it difficult to track them down in the first place. Multisource reports also include material that is redundant in some way. There must be a sense of cooperation and intelligence in the acquisition of data. Accuracy, simplicity and consistency are all required in a cohesive approach.

Processing data is the next step in the process of gathering and storing information. In addition, the collection should be constantly adjusted in accordance with the real strategy of the scene. The current botnet detection system design has certain issues that need to be addressed such as, it is not appropriate for large-scale network settings, the feature extraction approach is not flexible, the design is a single process that cannot be merged, and it is not possible to include many processes into a single system.

Botnet activity can be swiftly detected and prevented, but many systems lack good information exchange and collaboration; their only means of coordination is a single-point mechanism, and thus are incapable of responding fast to botnet activities. It is essential that the detection system framework be scalable, distributed, and extensible. Detection and other security systems should be able to cooperate with it.

5. Conclusion

The presence of a botnet is a serious security risk, and it is difficult to find out about it. Therefore, a variety of botnet detection and monitoring solutions have been examined. Botnet detection is often carried out by means of an intrusion detection system. This study thoroughly analyzes the most current tools and approaches for detecting IoT botnets. The majority of the articles have discussed how to find a botnet in its latter stages of development. In addition, depending on the categorization approach, artificial intelligence-based solutions are common in research. Another option is to develop a more complex and comprehensive system that, for example, has several detection levels for each stage of the botnet. Other technologies including software-defined networks, edge computing, blockchain, fog computing, and network function virtualization might also be used in conjunction with machine learning classifiers in the same circumstance.

References

[1] Alazzam, H.; Alsmady, A.; Al Shorman, A. Supervised detection of IoT botnet attacks. In Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems, Dubai, United Arab Emirates, 2–5 December 2019; p. 42.

[2] Salim, M.M.; Park, J.H. Deep Learning based IoT re-authentication for botnet detection and prevention. In Advanced Multimedia and Ubiquitous Engineering; Springer: Singapore, 2019; p. 239.

[3] Shire, R.; Shiaeles, S.; Bendiab, K.; Ghita, B.; Kolokotronis, N. Malware squid: A novel IOT malware traffic analysis framework using convolutional neural network and binary visualisation. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems; Springer: Cham, Switzerland, 2019; Volume 11660, pp. 65–76.

[4] Habib, M.; Aljarah, I.; Faris, H.; Mirjalili, S. Multi-objective Particle Swarm Optimization for Botnet Detection in Internet of Things. In Algorithms for Intelligent Systems; Springer Science and Business Media LLC.: Singapore, 2019; pp. 203–229.

[5] Jung, W.; Zhao, H.; Sun, M.; Zhou, G. IoT botnet detection via power consumption modeling. Smart Health 2020, 15, 100103.

[6] S. Garg, M. Guizani, S. Guo, and C. Verikoukis, "Guest editorial special section on AI-driven developments in 5G-envisioned industrial automation: big data perspective," IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1291–1295, 2020.

[7] X. Wang, Q. Yang, and X. Jin, "Periodic communication detection algorithm of botnet based on quantum computing," Journal of Quantum Electronics, vol. 33, no. 2, pp. 182–187, 2016.

[8] M. Albanese, S. Jajodia, and S. Venkatesan, "Defending from stealthy botnets using moving target defenses," IEEE Security & Privacy, vol. 16, no. 1, pp. 92–97, 2018.

[9] Z. Zha, A. Wang, Y. Guo, D. Montgomery, and S. Chen, "BotSifter: an SDN-based online bot detection framework in data centers," in Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), pp. 142–150, Washington DC, DC, USA, November 2019.

[10] X. Cheng, Research and Implementation of Botnet Detection Method under Software Defined Network, Wuhan University, Wuhan, China, 2017.

[11] G. Sagirlar, B. Carminati, and E. Ferrari, "Autobotcatcher: blockchain-based p2p botnet detection for the internet of things," in Proceedings of the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 1–8, Philadelphia, PA, USA, July 2018.

[12] W. She, Q. Liu, Z. Tian, J. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," IEEE Access, vol. 7, pp. 38947–38956, 2019.

[13] Alhajri, R.; Zagrouba, R.; Al-Haidari, F. Survey for anomaly detection of IoT botnets using machine learning auto-encoders. Int. J. Appl. Eng. Res. 2019, 14, 2417.

[14] Ali, I.; Ahmed AI, A.; Almogren, A.; Raza, M.A.; Shah, S.A.; Khan, A.; Gani, A. Systematic literature review on IoT-based botnet attack. IEEE Access 2020, 8, 212220–212232.

[15] Dange, S.; Chatterjee, M. IoT Botnet: The Largest Threat to the IoT Network. In Advances in Intelligent Systems and Computing; Springer: Singapore, 2019; pp. 137–157.

[16] Koroniotis, N.; Moustafa, N.; Sitnikova, E. Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions. IEEE Access 2019, 7, 61764–61785.

[17] Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481.

[18] Keele, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering; Technical Report, Version 2.3; EBSE: Hajdúszoboszló, Hungary, 2007.

[19] G. Spathoulas, N. Giachoudis, G.-P. Damiris, and G. *eodoridis, "Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets," Future Internet, vol. 11, p. 226, 2019.

[20] Popoola, S.; Adebisi, B.; Ande, R.; Hammoudeh, M.; Anoh, K.; Atayero, A. SMOTE-DRNN: A Deep Learning Algorithm forBotnet Detection in the Internet-of-Things Networks. Sensors 2021, 21, 2985.

[21] Popoola, S.I.; Adebisi, B.; Hammoudeh, M.; Gacanin, H.; Gui, G. Stacked recurrent neural network for botnet detection in smart homes. Comput. Electr. Eng. 2021, 92, 107039.

[22] Vishwakarma, R.; Jain, A.K. A Honeypot with machine learning based detection framework for defending iot based botnet DDoS attacks. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1019–1024.

[23] Tzagkarakis, C.; Petroulakis, N.; Ioannidis, S. Botnet attack detection at the IoT edge based on sparse representation. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6.

[24] Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier. In Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30 September 2018; pp. 118–122.

[25] Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-baiot—network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. 2018, 17, 12–22.

Author's biography

B. P. Sreeja is currently working in the Department of Information Technology, Karpagam College of Engineering, Coimbatore India. Her area of research includes wireless sensor networks and cryptography.