A Literature Survey on IoT Botnet Detection Techniques

Umar Maikudi
Department of Computer Science
Federal University of Technology
Minna, Nigeria
maikudiumar509@gmail.com

Opeyemi Aderiike Abisoye
Department of Computer Science
Federal University of Technology
Minna, Nigeria
o.abisoye@futminna.edu.ng

Shefiu Olusegun Ganiyu
Department of Information and Media Technology
Federal University of Technology
Minna, Nigeria
shefiuganiyu@futminna.edu.ng

Sulaimon A. Bashir
Department of Computer Science
Federal University of Technology
Minna. Nigeria.
bashirsulaimon@futminna.edu.ng

***Abstract*— One of the significant security concerns in the Information Technology community is Botnet, which could be used by adversaries to launch different kinds of attacks from compromised IoT devices. Botnets were initially created for positive purposes, not until cybercriminals began to take advantage of their potentials and started programming malicious software for malicious intent thereby, making detection and mitigation difficult. The rapid rise in the development of IoT products has made cyber-attack permutations unpredictable and availed cybercriminals of new techniques for security breaches of such products. Hence, the motivation for this research is premised on the incessant increase in the botnet attacks on IoT-based products. Thus, this paper offers a comprehensive literature overview of current IoT botnet detection techniques with a focus on revealing the strengths and weaknesses of the existing techniques in the research area. In line with this, some selected techniques were retrieved and analyzed in the summary table and a conclusion is drawn which exposed the need for more robust detection techniques to detect and prevent the emerging sophisticated botnet versions in the domain. Therefore, the findings from this review will benefits researchers who are engaged in detecting and preventing botnet attacks over IoT devices and network.**

Keywords— Botnet Detection, IoT Devices, C&C Channel, Botmaster, Detection Techniques.

I. INTRODUCTION

Internet of things (IoT) is a new paradigm that aims to integrate and connect anything at anytime, anyplace with anything and by anyone thus creating smart devices capable of collecting, storing, and sharing data without requiring human interaction [1][2]. The incessant increase in IoT devices is equally proportional to the vulnerabilities it imposed on such devices as botnets and/or malware attacks [3]. The poor security model of IoT devices can be exploited by the adversary to carry out malicious and illegal actions of high-level damages [4]. The emergence of the IoT paradigm is one of the most spectacular phenomena of the last decade. These technological advances in electronics and computer science have led to an exponential increase in the number of Internet-connected sensing and computing devices (also known as smart devices) that can provide services only limited by human imagination [2]. IoT security is an ongoing research topic that is attracting increasing attention in academic, industrial as well as governmental researches. Many organizations worldwide and multinational corporations are involved in the design and development of IoT-based systems [5]. However, IoT security vulnerability and potential attack vector identified in [6] have made it easy for botnets to covertly launch attacks.

The incessant increase of IoT-based products necessitates the interests of researchers in detecting and preventing botnet attacks in cyberspace day by day. Therefore, in this study, we present a comprehensive literature survey on IoT botnet detection techniques and this will benefits researchers who engaged in detecting and preventing botnet attacks.

The main purpose of this work is to provide a literature survey on most recent IoT botnet detection techniques and the contributions of this paper are as follows:

- Comprehensive presentation of IoT botnet detection techniques.
- Review of the most recent botnet detection techniques along with their strengths and weaknesses.
- Emphasis on the need for more robust botnet techniques that will be able to detect the emerging sophisticated variants of botnets.

A. Botnet

The term "Botnet" is derived from two words "RoBOT" and "NETwork". The botnet is traced to have originated from Internet Relay Chat (IRC), a text-based chat system that organizes communication in channels, and the concept of bots did not necessarily involve harmful behaviour. The main idea behind botnets was to control interactions in IRC rooms. They were able to interpret simple commands, provide administration support, offer simple games and other services to chat users and retrieve information about operating systems, login, email address among others [7]. A botnet according to [8], is a group of infected devices called bots interconnected over the internet that have been compromised through malware [9][10], the devices can be a personal computer, mobile devices [11] and even IoT devices [12] which are remotely accessed and controlled by the adversary (Botmaster) via command and control (C&C)

channel. The botnet is used in a wide range of malicious activities such as e-mail spamming, Phishing, social engineering, and even DDoS attack could be launched. The life cycle of a botnet is comprised of 5 stages which begin with the conception stage followed by the recruitment, the interaction stage, execution of malicious activities, and finally the upgrade and maintenance stage which will be illustrated in section C.

Botnets are considered the basis for several security threats in the world and command and control servers are the backbone of botnet communications, through which the bots report to the botmaster and then later sends attack orders to the bot army [13]. Botnets are also categorized according to their C&C protocols, like Internet Relay Chat (IRC), Hypertext Transmission Protocol (HTTP), Peer-to-peer (P2P) botnets, and Domain Name Systems (DNSs) method known as fast-flux is used by a botmaster to cover malicious botnets activities and increase the lifetime of malicious servers by quickly changing the IP address of the domain names over time. Botnets are often difficult to detect and may take a long time before it finally launches an attack.

B. Types of Botnet

According to [14] botnets are grouped into three (3) categories based on their communication channel and the server they were created on:

i. **Internet Relay Chat (IRC) botnets**: these are the earliest botnets, they work through IRC protocol, this protocol was initially designed for communication and dissemination of information amongst end-users. The cybercriminals took advantage of its inherent flexibility and scalability to exploit its vulnerabilities to carry out malicious transactions. Once a device is compromised, is by default connected to the IRC chat room which is remotely controlled and commanded by the botmaster. The botmaster remotely instructs the zombie device to go on with malicious activities via the chat room. The botmaster can either use private or public chat servers for communication. IRC botnets are based on centralized C&C architecture which makes them prone to one end failure. IRC botnets are easy to detect and blocking them is also easy due to their centralized architecture.

ii. **HTTP Botnets**: in an attempt to evade botnet detection by the botmaster, HTTP botnets emerged, the botmaster employed the use of HTTP protocol to create botnets that look legitimate HTTP traffic to shield bots' activities in normal network traffic thereby making detection difficult. HTTP botnets are also based on centralized C&C architecture with the same limitation of one end failure. The distinction between IRC and HTTP botnets is that HTTP botnets are difficult to detect but once detected can be blocked easily just like that of IRC.

iii. **Peer-to-Peer (P2P) Botnets**: these are the modern and more sophisticated botnets that are versatile and resistant to countermeasures. P2P botnets are based on decentralized C&C architecture. There is no existence of central command and control server, at any point in time, each bot can be either a client bot or a C&C server which makes detection difficult and it is void of one end failure. Most of the attacks

C. Life-cycle of a typical Botnet

Botnet often follows five stages to accomplish or execute instruction ordered by the botmaster through the C&C channel. The stages are shown in the following figure:

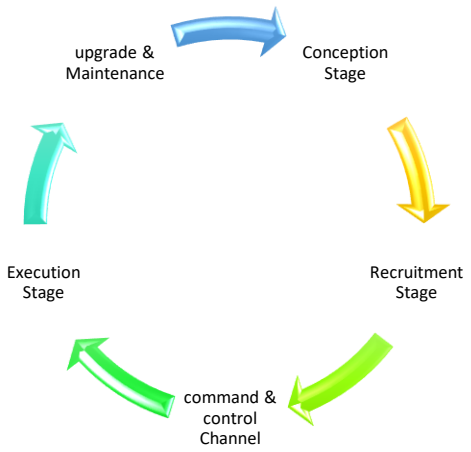

Figure 1: Life Cycle of a typical botnet

a) The Conception Stage

In this stage Botnets are the workhorses of the internet, they are connected computers performing series of tasks repeatedly to keep the website going and they are mostly used in connection with Internet Relay Chat, the botmaster examines a target subnet for vulnerabilities and uses different exploitation methods to infect the target's device. As soon as the botmaster is in control of your device, he will usually use your machine to carry out malicious activities.

b) The Recruitment Stage

In this, botnets are normally spread to infect other devices via malicious content injection on a visitation of unprotected websites. Botnets are capable of propagating themselves to recruit more devices into their army of bots.

c) The Interaction Stage

This stage involves both internal and external communications between the botmaster and the zombie army through the C&C channel. Communication must not be necessary with the bots within the bot army, even bot outside the army can be communicated to.

d) The Execution Stage

The execution stage, in this stage, the malicious activities are executed as instructed by the botmaster and this is for the botmaster to accomplish his set goals.

e) Upgrade and Maintenance Stage

In the upgrade and maintenance stage, the botnets report to the botmaster upon completion or execution of the instruction given and wait for further instructions.

D. Architecture and Communication Pattern

Based on the architectural model, botnets are divided into three, namely Centralized, Decentralized and Hybrid botnet architecture models. In Centralized architecture, the botnet structure is set up like the basic network with one main server alias the C&C server controlling the transmission of information from each client (bot), the botmaster uses a program to establish a C&C channel through which he relays instruction to each client device [15]. Bots are created using a single C&C Server and are communicated via a single C&C channel that connects all of them. In this communication pattern, the bandwidth of the central point needs to be very high because the botmaster sends and receives messages from all other bots through a single C&C channel thereby making the botnets network traffic so conspicuous to detect, and once detected, it can be blocked easily. The centralized architecture mainly used IRC and HTTP-based protocols. The IRC works on internet text messages in real-time. Botmasters use IRC bots because of their simplicity and flexibility in architecture. IRC botnets traffic is so conspicuous which limits its use. While the HTTP botnet traffic can be shielded thereby making the traffic inconspicuous within the normal traffic. In HTTP based protocol, botnet traffic is hidden thereby making it difficult to detect.

In decentralized Architecture, the vulnerability of detecting and blocking the C&C channel is been curtailed, because the botnet is extremely versatile and resistant to countermeasures [16], a large number of bots can be created in just one botnet. In this architecture, it is extremely tough to detect the C&C channel because it employed the use of peer-to-peer (P2P) protocol through which all bots are connected to. The protocol primarily focuses on shielding the C&C channel and the botmaster uses diverse bots when new instruction is issued. The advantage of using a P2P protocol is that detection of a particular bot does not translate to the detection of the whole botnet network. And in Hybrid architecture, the centralized and decentralized are combined, where a botmaster uses a centralized architecture because of its simplicity and flexibility and later upgrades a decentralized, making the botnet traffic extremely difficult to detect by hiding it using encryption methods [17].

II. RELATED STUDIES

We present, in this section, a comprehensive overview of some of the recent literature on IoT botnet detection techniques

[18] proposed a novel network-based anomaly detection model called N-BaIoT which extracted the behavior snapshot of the network and uses deep autoencoder to detect anomalous network traffic from compromised IoT devices. The proposed detection model was empirically evaluated using nine commercial IoT devices that were infected in a lab with the globally known IoT-based botnets (Mirai and Bashlite). Their evaluation result demonstrated the ability to accurately and instantly detect attacks as they are being launched from the compromised IoT devices that were part of the botnet. And the method shows some level of superiority in term of TPR and FPR when juxtaposed to Local Outlier Factor (LOT), One-Class SVM, and Isolation Forest

[19] proposed an IoT botnet detection via power consumption modeling. The Convolutional Neural Network (CNN)-based deep learning model for detection of botnets was based on power consumption that consists of a data processing module as well as an 8-layer CNN model. Before applying the CNN model, the authors segmented and normalized the collected power consumption data to the model to achieve higher accuracy. The 8-layer CNN classifies the processed data into four classes, including a botnet class which is the primary target. The performance of the model was measured by running self-evaluation, cross-device evaluation, leave-one-device out and leave one botnet out tests on three common types of IoT devices which are security Cameras, Router, and Voice Assistants Devices. Classification accuracy of 96.5% was achieved on the dataset for self-test, accuracy performance of cross-evaluation was about 90% and leave-one-out test accuracy for detection of botnet introduces higher than 90% accuracy. One of the limitations of this model is, it only learns the signatures of the well-known IoT botnets, and the detection of malicious behavior is done via power consumption data.

[20] proposed a hybrid botnet detection (HANABOT) based on host and network analysis. The model addressed the problem of botnet detection based on the network's flows records and activities in the host. The authors claimed that the model (HANABot) is a general technique capable of detecting new botnets in the early phase. The model was implemented in both the host and the network sides and it was interested in IRC, HTTP, P2P, and DNS botnet communications traffic using IP fluxing. The algorithm was proposed to process and extract features to distinguish between botnet from the benign behavior in the network. The solution of the model was evaluated employing a collection of real datasets (malicious and benign). The experiment in this study showed a high level of accuracy and low level of False Positive Rate (FPR) and it was compared with the result of some existing approaches with a focus on some specific features and performance and the HANABot outperformed some of the presented techniques in terms of accuracy in detecting botnets flow records within the network traces. One of the limitations of the study is that the accuracy largely depends on certain features of the datasets used.

A study by [21] proposed a DNS-rule-based schema for botnet detection (DNS-BD). The approach can improve the accuracy of DNS traffic-based detection of botnets that are based on DNS query and response behaviors. The technique aimed at detecting any abnormal DNS query and response behaviors by applying the proposed DNS query and response rules. The result of the technique in this study showed an accuracy of 99.35% in terms of botnet detection and a low False Positive Rate of 0.25%, also a comparison of the proposed method with the well-known DNS-based approaches evaluates the effectiveness of the proposed technique. This approach is effective only on DNS-based traffic flows.

A study by [22] argued that anomaly-based botnets detection approaches are more effective than signature-based detection techniques because recent variants of

botnets are equipped with sophisticated code update and evasion techniques. On this note, they proposed a botnets detection model based on machine learning algorithms that use Domain Name Service (DNS) query data and evaluated its effectiveness using popular machine learning techniques (K-Nearest Neighbour (KNN), Random Forest (RF), and Naïve Bayesian theorem) and RF produced the best overall detection accuracy of over 90%. High computing resources are one of the limitations of the model in this study.

A study by [15] proposed an HTTP Botnet Detection in IoT Devices using Network Traffic Analysis. The model in this study is a novel approach based on behavioral analysis of the botnets to detect IoT malware, the approach detected the presence of malware using supervised machine learning algorithms taking the discovered features as input. The model was implemented and compared with other various machine learning techniques and the result show that neural network outperformed all other methods in malware detection in IoT devices.

Also, another study by [23] proposed a method for botnets detection in the Internet of Things (IoT). The method is applicable for the detection of botnets that are propagated via brute-force attacks using the TELNET and/or SSH protocol. The detection of this model is done at the propagation stage. The method is based on a model of logistic regression which allows estimation of a probability that a device initiating a connection is running a bot. one of the limitations of the method is that it doesn't detect an unknown botnet.

A study by [24] suggested a visualized botnet detection system based on deep learning for the IoT networks of smart cities. The botnet detection system proposed in this study is based on a two-level learning framework for semantically discriminating botnet and normal behavior at the application layer of the domain name system (DNS) services. In the first level of the framework, the similarity measures of DNS queries are estimated using Siamese networks based on a predefined threshold for selecting the most frequent DNS information across ethernet connections. In the second level of the framework, a domain generation algorithm (DGA) based on deep learning architecture is suggested for classifying normal and abnormal domain names. The framework is highly scalable on a commodity hardware server due to its potential design for analyzing DNS data. The proposed framework was evaluated using two datasets and was compared with recent deep learning models. Various visualization methods were also employed to understand the characteristics of the dataset and to visualize the embedding features. The experimental result revealed substantial improvement in terms of F1-core, speed of the detection, and false alarm rate. However, the model in this study is computationally expensive and slow during the training stage.

In [25] an efficient reinforcement learning-based botnet detection approach was developed. In this study, a sophisticated traffic reduction mechanism was proposed, integrated with reinforcement learning techniques. The researchers focused on the passive monitoring of network traffic and the frequent communication between bots and their C&C servers during propagation. The proposed detection approach in this study comprises four phases, namely: network traffic capture and packet reduction, feature extraction, malicious activity detection, and bot behaviour detection using reinforcement learning. The authors evaluated the proposed approach in this study using real-world network traffic and achieved a detection rate of 98.3% and a relatively low false positive rate of 0.012%. however, their approach requires high computing resources.

[26] introduced a network traffic analysis-based IoT botnet detection using honeynet data applying classification techniques. The honeynet was used in this work to provide activity logs of the intrusion attempts as well as the network traffic dump in the form of packet capture, the network traffic is used in this work, for extracting the flow of the traffic. This research focused on botnet detection using the network flow by using machine learning techniques to distinguish the pattern exhibited by botnet in a network and by finding the feature which has significant influence for filtering traffic belonging to a botnet. The system implementation was carried out in Python and performance was compared with other machine learning algorithms.

Another research work by [27]**.** proposed a botnet detection in software-defined networks by deep learning techniques. The botnet detection method proposed in this study is based on deep learning techniques tested on a new SDN-specific dataset and a classification accuracy of 97% was achieved. The algorithm was implemented on two state-of-the-arts frameworks, that is Keras and TensorFlow. High computing resources could be one of the limitations of this research.

Also, research by [28] proposed an adaptive multi-layer botnet detection technique using a machine learning classifier. The method in this work presents a framework based on a decision tree that effectively detects P2P botnets. The authors applied a decision tree algorithm for feature selection to extract the most relevant features. At the first layer of the model, all non-P2P packets were filtered to reduce the amount of network traffic through well-known ports, Domain Name System (DNS) query, and flow counting. The second layer further characterized the captured network traffic into non-P2P and P2P. at the third layer of the proposed model, the authors reduced the features which may marginally affect the classification. At the final layer, the detection of P2P was done using a decision tree classifier by extracting network communication features. The experimental evaluation of the proposed model revealed an average accuracy of 98.7%.

[29] proposed botnet detection using graph-based feature clustering. The author applied Self-Organization Map to establish the cluster on nodes in the network based on the features. The model is capable of isolating the bot in small clusters while containing most normal nodes in the big clusters. A filtering procedure is also developed to further enhance the algorithm efficiency by removing inactive nodes from bot detection. The author verified the methodology using real-world CTU-13 and ISCX botnet dataset and benchmarked against classification-based detection methods and the method shows efficiency in bot detection despite their varying behaviors.

A study by [30] developed an effective botnet detection through neural networks on convolutional features. The

machine learning-based botnet detection system shown to be effective in identify P2P botnet. The approach extracts a convolutional version of flow-based effective features and trains a classification model by using a feed-forward artificial neural network. The experimental result shows that the accuracy of detection using the convolutional features is better than the ones using the traditional features. It can achieve 94.7% of detection accuracy and 2.25% of False Positive Rate on known P2P botnet datasets. However, the system in this approach provides additional confidence testing for enhancing the performance of botnet detection. It further classifies the network traffic of insufficient confidence in the neural network. The experiment shows that this stage can increase the detection accuracy up to 98.6% and decrease False Positive to as low as 0.5%.

Another study by [31] came up with an effective conversation-based botnet detection method. The research is an improvement over the progress of packet processing technologies such as New Application Programming Interface (NAPI) and zero-copy. The study proposes an efficient quasi-real-time intrusion detection system. The method detects botnet using a supervised machine learning approach under the high-speed network environment. This research came up with a detection framework using PF_RING for sniffing and processing network traces to extract flow features dynamically, the research uses the Random Forest model to extract promising conversation features and finally analyze the performance of different classification algorithms. The experimental result showed that the conversation-based detection approach can identify botnet with higher accuracy with a lower false positive rate than the flow-based approach.

[32] proposed a holistic model for HTTP botnet detection based on DNS traffic analysis. This research work presents a new detection framework that involves three detection model which can run independently or in tandem. The first detector profiles the individual application based on their interaction. The second decoder tracks the regularity in the timing of the bot DNS queries and uses this as the basis for detection. The third decoder analyses the characteristics of the domain names involved in the DNS and identifies the algorithmically generated and fast-flux domains which are staples of a typical HTTP botnet. The authors investigated each of the detectors using several machines learning classifiers and experimentally evaluated using public datasets and datasets collected in their testbed yielded very encouraging performing results.

[33] introduced an approach for the detection of IoT-botnet attacks using fuzzy rule interpolation (FRI). The FRI reasoning methods added a benefit to enhance the robustness of fuzzy systems and effectively reduce the system's complexity. These benefits help the Intrusion Detection Systems (IDS) to generate more realistic and comprehensive alerts. The proposed approach was applied to an open-source BoT-IoT dataset from the cyber range Lab of the center of UNSW Canberra Cyber. The approach was tested, evaluated and it obtained a detection rate of 95.4%. Moreover, it effectively smoothened the boundary between normal and IoT-Botnet traffics because of its fuzzy-nature, as well as, it had the ability to generate the required IDS alert in case of the deficiencies of the knowledge-based representation. Some of the weaknesses of this approach are, detection is completely dependent on human knowledge and expertise and cannot recognize machine learning or neural networks.

Another study by [33] proposed an IoT botnet detection using machine learning techniques. In this research, various machine learning techniques were proposed to effectively identify the presence of IoT botnet. The detection models predict the IoT botnet based on the network traffic information and the proposed model uses feature selection to achieve a faster detection rate with less false positive. The random forest classifier model outperformed the other machine learning models and deep learning model with an accuracy of 94.47% with lesser detection time. One of the major weakness of this approach is that it is used only on small network.

In [34] classification of domain generation algorithm (DGA) botnet detection techniques based on DNS traffic and parallel detection techniques for DGA botnet was presented. The proposed technique in the research uses genetic algorithm (GA) and parallel detection technique for DGA botnet detection. The GA considers the dynamicity of the DGA botnet; hence, it reduces the rate of false positive and also eliminates the need for human intervention. The parallel detection in the proposed work helps in reducing time complexity. The proposed approach gives the classification of DGA botnet detection techniques based on domain name system (DNS) traffic. Computational complexity and high implementation cost are some of the weaknesses of this method.

[34] developed a detection and confronting flash attacks from IoT botnets. This research proposed and implemented an adaptive filter that curtails DDoS attacks from a variety of compromised IoT bots. The major botnets used in the research are Mirai, Bashlite and cryptojacking. Experimental showed that detection of IoT botnet can be achieved with an accuracy rate of 99.69% and detection of cryptojacking with a misclassification rate of 1.5%. the performance analysis and overall results showed that the adaptive filter is tested using Amazon public cloud platform, and the results show that the adaptive filter can significantly reduce illegitimate botnet requests from variants such as FBOT, ARIS, EXIENDO and APEP and can reduce the instances processing time by 19%, connection time by 34% and the waiting time by 18%. This approach involved applying various mathematical and computational algorithms.

III. METHODOLOGY

This study aims to provide a survey on the most recent botnet detection techniques proposed by various researchers and to achieve this, we formulated research questions which are: 1) What are the strengths and limitations of the current techniques for detecting botnets in IoT devices? 2) Which of the botnet detection techniques is proposed most frequently in current studies? Based on these research questions we formulated three research objectives. The first objective is to review the most recent botnet detection techniques. The second objective is to identify the strengths and limitations of the recent techniques for botnet detection and the third objective is to discover the most effective and commonly used techniques

in IoT botnet detection. A total of 38 recent publications on IoT botnet detection techniques that includes journal articles and conferences papers published in English language were considered in the literature search. Also, eight 8 duplicate papers were excluded, while 20 relevant publications were selected based on their recency in line with the objectives of the study. Current methods for botnets detections are investigated from the reviewed literature and their strengths and limitations were identified. The second and third objectives were achieved in Table 1 for identifying the strengths and limitations as well as the most effective and commonly used technique respectively.

A. Methods

Here, we discuss the methods that are used in detecting IoT botnet. Researchers have articulated numerous botnet detection techniques with different approaches. Broadly, botnet detection techniques are classified in two [14][35].

1. IoT Botnet Detection Techniques

Researchers have articulated numerous botnet detection techniques with different approaches. Broadly, botnet detection techniques are classified in two [14][35],

a) Host-based Botnet Detection Techniques

A host-based botnet detection technique is also known as client-based botnet detection or stand-alone detection system. Host-based detection techniques encompass all processes involved in detecting, identifying, and preventing bots and other malicious flows on the host device [36][14], these methods are ancient ways of determining whether the host device is compromised by way of incessantly checking the network connection, process files and registries underneath controlled situation the host-based detection works, but work by [18] considers host-based botnet detection less realistic for detecting compromised IoT devices due to some reasons they discovered. However, bot malicious software running on the compromised devices easily detect these kinds of detection methods, in an attempt to evade the bot's malicious activity on the host devices, the botmaster employed different anti-detection techniques such as rootkits-enable, code obfuscation, and the likes, thereby making botnet detection hard to security professionals [14].

b) Network-based Detection Techniques

Network-based detection is a more preferred technique compare to host-based. Network-based techniques involve the analysis of network traffic flow, network behaviour as a result of bots running on the network. The resistance techniques employed by the attackers' such as encryption, fast-flux, and domain flux to make the bots more resilient and resistant to detection methods produce further traits that be so conspicuous via the network traffic flow analysis. Network-based botnet detection techniques can be further divided into two: 1) Signature-based detection techniques and 2) Anomaly-based detection techniques [37][38].

2. Signature-based Detection Techniques

The signature-based techniques alias Intrusion detection systems is a process where a unique identifier is established about a known botnet so that it can be identified and prevented in the future. These techniques are effective on predefined botnet features or characteristics, and one of the major drawbacks of signature-based detection techniques is its failure to detect a zero-day attack (i.e. attack with no corresponding signature in the repository) [38].

3. Anomaly-based Detection Techniques

Anomaly-based detection techniques seek to detect or identify bot by classifying the anomalies in the network traffic flow including network latency, traffic on unusual ports, which are an indication of the presence of bots over the network. These techniques are effective in detecting zero-day attacks and they have a high rate of FPR and difficulty in selecting the best features during training in the case of machine learning techniques.

4. Machine Learning Techniques

Machine learning (ML) techniques have also pave way for themselves into botnet detection approaches because of their usefulness and robustness in the area among others. Machine learning, been a subset of Artificial Intelligence (AI), where machines will make to mimic human beings in virtually all aspects of human endeavour through machine learning. it is used to train a system to learn how to detect and classify whether or not a network traffic flow belongs to a malware bot or benign. Supervised and unsupervised ML are the most used types of machine learning in botnet detection techniques.

a) *Supervised Machine Learning Methods*

In supervised machine learning methods, there exists sets of inputs vectors X and corresponding output vectors Y (target) and an algorithm is used to learn the mapping function Y = f(X). The goal for supervised ML is to estimate the mapping function such that when new input data is supplied to the algorithm, it can predict the output for that data based on the experience it acquired in the previous training. Support Vector Machine (SVM), Bayesian Classifier, Artificial Neural Network (ANN), and Decision Tree Classifier are some of the used supervised ML techniques among others.

c) Unsupervised Machine Learning

In unsupervised machine learning methods, there exists only input vector X with no corresponding target vector. The goal for unsupervised learning is for the system to evaluate data in terms of traits and uses the traits to form a cluster of items that are similar to one another.

5. Reinforcement Learning

In reinforcement learning according to [39] is an approach to machine learning that trains algorithms using a system of reward and penalty. A reinforcement learning algorithm, or agent, learns by interacting with its environment. The agent receives rewards for performing correctly and penalties for performing incorrectly. The agent learns without intervention from a human by maximizing its reward and minimizing its penalty.

IV. RESULTS AND DISCUSSION

Having achieved the first objective in section II, a summary of the reviewed IoT botnet detection techniques is presented in this section from the reviewed literatures. Table I presents a tabular form of the summary and the detailed summary comprises of publication year, reference

number, detection technique/method, strength, and limitation respectively.

TABLE 1: SUMMARY OF IOT BOTNET DETECTION TECHNIQUES

Pub. Year	Ref, No.	Detection Technique/Method	Strengths	Limitation
2020	Almutairi *et al*. [20]	Hybrid (Host and Network-Based) Detection - HANABoT	A high level of accuracy of 99% was achieved and a low FPR of 0.01 was achieved	Time of detection is not stated and requires high computing resources
2018	Meidan *et al*. [3]	Autoencoder (Network-based detection)	Achieved high TPR	Only botnet attack over the network can be detected and efficiency is only on the trained data
2020	Alazab *et al*. [24]	Domain Generation Algorithm (DNS-based)	The experimental result revealed substantial improvement in terms of F1-core, speed of the detection, and false alarm rate	Slow during training stage and computationally expensive
2018	Hoang & Nguyen [22]	Machine Learning Techniques using DNS Query Data	Detection Accuracy of 90% was achieved	The effect of DN features on the detection accuracy is not analyzed and the dataset used is relatively small
2019	Al-qerem & Choo [25]	Reinforcement Learning Technique	A detection rate of 98.3% and FPR of 0.012% were achieved	Computationally expensive
2018	Prokofiev *et al*. [40]	TELNET and/or SSH Protocol	Botnet propagated through brute-force were detected	Does not detect an unknown botnet
2019	Alieyan *et al*. [41]	DNS-rule Based Schema	Accuracy of 99.35 and FPT of 0.25 was achieved	Effective only on DNS-based traffic flow was considered
2020	Jung *et al*. [19]	Convolutional Neural Network (CNN)-based Deep Learning Technique	96.5% Classification accuracy was achieved	Only learns the signatures of the well-known IoT botnets
2019	Khan et al [28]	Multi-layer Traffic Classification Method with Decision Tree Classifier	Average accuracy of 98.7%	Computationally expensive
2018	Chen et al [30]	Neural Networks on Convolutional Features	Detection accuracy up to 98.6% and False Positive to as low as 0.5% was achieved.	It requires high computing resources
2017	Chen et al [31]	Supervised Machine Learning Technique	High accuracy and low FPR as against flow-based approach was achieved	Computationally expensive
2017	Chowdhury et. al. [29]	Graph-based Feature Clustering	Can efficiently detect the bots despite their varying behaviors	Computationally expensive
2020	Jagannath S. [42]	Machine Learning Technique	Detection rate of 94.47% with lesser detection time	Approach is used in small network
2020	Al-Kasassbeh et al [33]	Fuzzy Rule Interpolation	95.4% of detection accuracy was achieved	Detection is completely dependent on human knowledge and expertise
2019	Banerjee & Samantaray [26]	Supervised Machine Learning Classification Techniques	Best and consistent classification was achieved with Random Forest classifier	Computationally expensive and there no measurement of performance metrics
2021	Mathew, & Pauline [43]	Genetic Algorithm	Reduces FPR and time complexity	Computationally expensive and high implementation cost
2019	Kumar & Bhama [44]	Adaptive Filter	99.69% accuracy and 1.5 FPR achieved	Involves applying various mathematical and computational algorithm
2018	McDermott *et al*. [45]	BLSTM-RNN	Better progressive model when compared with LSTM-RNN, generated a labelled dataset for other researchers	Less transparent and computationally expensive
2017	Alenazi et al. [46]	DNS Traffic Analysis	99.3% detection accuracy and 0.2% FPR were achieved	Requires High computing resources and training time
2020	Nguyen [47]	Graph-based Method	Accuracy of 98.7% was achieved	Efficiency of the depends on scenario

As revealed in table I, it is evident that, due to the sophisticated nature of the emerging botnets, host-based detection techniques work well only on the host devices and do not detect unknown botnet and also, have little or no ability to detect botnet over the network. While Network-based detection techniques work effectively only on known botnet signatures stored in the memory over the network. Machine learning techniques are mostly employed in detecting botnet attacks for machine learning approaches have proven effectiveness in terms of accuracy and TPR only that machine learning techniques are computationally expensive and complex in implementation. All techniques used in detecting IoT botnet attacks as surveyed in this study have one drawback or the other. However, Machine learning techniques demonstrated efficiency and effectiveness in detecting IoT botnet over the network.

V. CONCLUSION

As observed in the literature, there are several effective and efficient types of research available in the field of botnet detection and despite the milestone achieved so far in this research domain, none of the techniques has achieved 100% accuracy. The effectiveness and efficiency of each technique reviewed in the study depend on the kind of botnet it was meant to detect. As adversaries keep devising numerous means for evading the existing detection techniques by bringing more sophisticated versions of botnet threats, more researches are required to be in control of these botnet threats. It has been also noted that there is an exponential increase in the number and use of IoT devices which in turn can lead to more botnet attacks in such devices. Therefore, the need for more robust IoT botnet detection techniques cannot be overemphasized. Finally, this study has presented weaknesses of the research area as shown in table 1. for further research, researchers can further develop more robust botnet detection techniques that can detect and prevent the emerging sophisticated botnet attack.

REFERENCES

[1] T. Y. Chung, I. Mashal, O. Alsaryrah, V. Huy, W. H. Kuo, and D. P. Agrawal, "Social web of things: A survey," *Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS*, pp. 570–575, 2013, doi: 10.1109/ICPADS.2013.102.

[2] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, pp. 586–602, 2017, doi: 10.1109/TETC.2016.2606384.

[3] Y. Meidan *et al.*, "N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.

[4] B. Alothman, "Robust Botnet Detection Techniques for Mobile and Network Environments," no. April, 2019.

[5] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet : The Internet of Things Architecture , Possible Applications and Key Challenges," 2012, doi: 10.1109/FIT.2012.53.

[6] R. Alhajri, R. Zagrouba, and F. Al-Haidari, "Survey for Anomaly Detection of IoT Botnets Using Machine Learning Auto-Encoders," *Int. J. Appl. Eng. Res.*, vol. 14, no. 10, pp. 2417–2421, 2019, [Online]. Available: http://www.ripublication.com.

[7] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," *Comput. Networks*, vol. 57, no. 2, pp. 378–403, 2013, doi: 10.1016/j.comnet.2012.07.021.

[8] S. Amina, R. Vera, T. Dargahi, and A. Dehghantanha, "A Bibliometric Analysis of Botnet Detection Techniques."

[9] "BoTShark: A Deep Learning Approach for Botnet Traffic Detection | SpringerLink." https://link.springer.com/chapter/10.1007/978-3-319-73951-9_7 (accessed Aug. 27, 2020).

[10] M. Hopkins and A. Dehghantanha, "Exploit Kits : The production line of the Cybercrime Economy ?," pp. 23–27, 2015.

[11] M. Damshenas, A. Dehghantanha, K. R. Choo, M. Damshenas, A. Dehghantanha, and K. R. Choo, "M0Droid : An Android Behavioral-Based Malware Detection Model M0Droid : An Android Behavioral-Based Malware Detection Model," vol. 6548, no. December, 2015, doi: 10.1080/15536548.2015.1073510.

[12] K. Kwang and R. Choo, "Detecting crypto - ransomware in IoT networks based on energy consumption footprint," *J. Ambient Intell. Humaniz. Comput.*, vol. 0, no. 0, p. 0, 2017, doi: 10.1007/s12652-017-0558-5.

[13] A. Al-nawasrah and S. Arabia, *A Survey of Fast Flux Botnet Detection With Fast Flux Cloud Computing*, vol. 10, no. 3. 2020.

[14] "Botnet Detection : Analysis of Various Techniques Sangita Baruah a," pp. 461–467, 2018.

[15] Abikoye Oluwakemi Christiana, Abubakar Abdullahi, Ahmed Haruna Dokoro, Akande Noah Oluwatobi (2020), Kayode Anthonia Aderonke, A Novel Technique to Prevent SQL-Injection and Cross-Site Scripting Attacks using Knuth-Morris-Pratt String Matching Algorithm, EURASIP Journal on Information Security, Vol. 14, Pp. 1-14. https://doi.org/10.1186/s13635-020-00113-y

[16] R. Vogt, J. Aycock, and M. Jacobson, "Army of botnets," *Netw. Distrib. Syst. Secur. Symp.*, pp. 111–123, 2007.

[17] S. Gaonkar, N. F. Dessai, S. Aswale, J. Costa, P. Shetgaonkar, and A. Borkar, "A Survey on Botnet Detection Techniques," pp. 1–6, 2020, doi: 10.1109/ic-ETITE47903.2020.Id-70.

[18] Y. Meidan *et al.*, "N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.

[19] W. Jung, H. Zhao, M. Sun, and G. Zhou, "IoT botnet detection via power consumption modeling," *Smart Heal.*, vol. 15, 2020, doi: 10.1016/j.smhl.2019.100103.

[20] S. Almutairi, S. Mahfoudh, S. Almutairi, and J. S. Alowibdi, "Hybrid Botnet Detection Based on Host and Network Analysis," *J. Comput. Networks Commun.*, vol. 2020, 2020, doi: 10.1155/2020/9024726.

[21] K. Alieyan, A. Almomani, M. Anbar, M. Alauthman, R. Abdullah, and B. B. Gupta, "DNS rule-based schema to botnet detection," *Enterp. Inf. Syst.*, pp. 1–20, Jul. 2019, doi: 10.1080/17517575.2019.1644673.

[22] Akande N. O., Abikoye C. O., Adebiyi M. O., Kayode A. A., Adegun A. A., Ogundokun R. O. (2019) Electronic Medical Information Encryption Using Modified Blowfish Algorithm. Lecture Notes in Computer Science, Vol. 11623, Pp. 166-179, https://doi.org/10.1007/978-3-030-24308-1_14.

[23] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, "A method to detect Internet of Things botnets," *Proc. 2018 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2018*, vol. 2018-Janua, pp. 105–108, 2018, doi: 10.1109/EIConRus.2018.8317041.

[24] M. Alazab, S. Member, and Q. Pham, "A Visualized Botnet Detection System based Deep Learning for the Internet of Things Networks of Smart Cities," vol. 9994, no. c, pp. 1–22, 2020, doi: 10.1109/TIA.2020.2971952.

[25] A. Al-qerem and K. R. Choo, "An Efficient Reinforcement Learning-Based Botnet," *J. Netw. Comput. Appl.*, p. 102479, 2019, doi: 10.1016/j.jnca.2019.102479.

[26] M. Banerjee and S. D. Samantaray, "Network Traffic Analysis Based IoT Botnet Detection Using Honeynet Data Applying Classification Techniques," *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 8, pp. 61–66, 2019, Accessed: Feb. 02, 2021. [Online]. Available: https://www.academia.edu/download/60722942/10_Paper_31071924_IJCSIS_Camera_Ready_pp61-6620190927-28005-18ji4kw.pdf.

[27] I. Letteri, G. Della Penna, and G. De Gasperis, "Botnet detection in software defined networks by deep learning techniques," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11161 LNCS, pp. 49–62, 2018, doi: 10.1007/978-3-030-01689-0_4.

[28] Akande O.N., Abikoye O.C., Kayode A.A., Aro O.T., Ogundokun O.R. (2020) A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_36.

[29] S. Chowdhury *et al.*, "Botnet detection using graph-based feature clustering," *J. Big Data*, vol. 4, no. 1, Dec. 2017, doi: 10.1186/s40537-017-0074-7.

[30] Abikoye Oluwakemi Christiana, Benjamin Aruwa Gyunka, Akande Noah Oluwatobi (2020), "Optimizing Android Malware Detection Via Ensemble Learning", International Journal of Interactive Mobile Technologies (iJIM), Vol. 14, No. 9, pp. 61-78. https://doi.org/10.3991/ijim.v14i09.11548 [31] R. Chen, W. Niu, X. Zhang, Z. Zhuo, and F. Lv, "An Effective Conversation-Based Botnet Detection Method," *Math. Probl. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/4934082.

[32] B. Alothman, "Robust Botnet Detection Techniques for Mobile and Network Environments," 2019. Accessed: Feb. 02, 2021.

[Online]. Available: https://dora.dmu.ac.uk/handle/2086/18144.

[33] F. Systems and I. O. S. Press, "rre cte d Au tho r P roo f Un co cte d Au tho r P roo f rre Un co," pp. 1–11, 2020, doi: 10.3233/JIFS-191432.

[34] S. E. Mathew and A. Pauline, "Classification of dga botnet detection techniques based on dns traffic and parallel detection technique for dga botnet," in *Advances in Intelligent Systems and Computing*, 2021, vol. 1167, pp. 297–304, doi: 10.1007/978-981-15-5285-4_29.

[35] Z. Chen, X. Yu, C. Zhang, J. Zhang, and C. Lin, "Fast Botnet Detection From Streaming Logs Using Online Lanczos Method," pp. 1408–1417, 2017.

[36] S. Kumar, "Botnet Detection Techniques and Research Challenges," *ieeexplore.ieee.org*, doi: 10.1109/ICRAECC43874.2019.8995028.

[37] S. Kumar, "Botnet Detection Techniques and Research Challenges."

[38] Oladipupo, Esau Taiwo, Abikoye Oluwakemi Christianah, Akande Noah Oluwatobi, Kayode Anthonia Aderonke, Adeniyi Jide Kehinde (2020), "Comparative Study of Two Divide and Conquer Sorting Algorithms: Quicksort and Mergesort", Procedia Computer Science, 171, pp 2532–2540. https://doi.org/10.1016/j.procs.2020.04.274.

[39] "What is Reinforcement Learning (RL)? - Definition from Techopedia." https://www.techopedia.com/definition/32055/reinforcement-learning-rl (accessed Mar. 07, 2021).

[40] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, "A method to detect Internet of Things botnets," in *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*, Mar. 2018, vol. 2018-January, pp. 105–108, doi: 10.1109/EIConRus.2018.8317041.

[41] K. Alieyan, A. Almomani, M. Anbar, R. Abdullah, and B. B. Gupta, "DNS rule-based schema to botnet detection," *Enterp. Inf. Syst.*, vol. 00, no. 00, pp. 1–20, 2019, doi: 10.1080/17517575.2019.1644673.

[42] S. Jagannath, "IoT Botnet Detection using Machine Learning Techniques Cybersecurity Suhas Jagannath School of Computing National College of Ireland Supervisor : Mr Vikas Sahni."

[43] Abikoye Oluwakemi Christiana, Haruna Ahmad Dokoro, Abdullahi Abubakar Akande Noah Oluwatobi, Asani Emmanuel Oluwatobi (2019), "Modified Advanced Encryption Standard Algorithm for Information Security", Symmetry, Vol. 11, No. 12, Pp. 1-17. https://doi.org/10.3390/sym11121484

[44] C. U. O. Kumar and P. R. K. Sathia, "Detecting and confronting flash attacks from IoT botnets," *J. Supercomput.*, no. 0123456789, 2019, doi: 10.1007/s11227-019-03005-2.

[45] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, pp. 1–8, 2018, doi: 10.1109/IJCNN.2018.8489489.

[46] A. Alenazi, I. Traore, and K. Ganame, "Holistic Model for HTTP Botnet Detection Based on DNS Traf fi c Analysis," vol. 3, pp. 1–18, 2017, doi: 10.1007/978-3-319-69155-8.

[47] H. T. Nguyen, Q. D. Ngo, and V. H. Le, "A novel graph-based approach for IoT botnet detection," *Int. J. Inf. Secur.*, vol. 19, no. 5, pp. 567–577, 2020, doi: 10.1007/s10207-019-00475-6.