Constructing IoT Botnet Detection Model Based on Degree Centrality and Path Analysis

Wan Nur Fatihah Wan Mohd Zaki [1], Raihana Syahirah Abdullah [1,*], Warusia Yassin [1], Siti Rahayu Selamat [1], Muhammad Safwan Rosli [1], and Syazwani Yahya [2]

[1] Information Security Forensics and Computer Networking (INSFORNET), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal Melaka, Malaysia
[2] Faculty of Computing and Engineering, Quest International University, 31250 Ipoh, Perak, Malaysia
Email: wantehawanzaki95@gmail.com (W.N.F.W.M.Z.); raihana.syahirah@utem.edu.my (R.S.A.); s.m.warusia@utem.edu.my (W.Y.); sitirahayu@utem.edu.my(S.R.S.); safwan.rosli92@gmail.com (M.S.R.); syazwani.yahya@qiu.edu (S.Y.)
*Corresponding author

***Abstract*—Internet of Things (IoT) Botnet is a network of connected devices, generally smart devices with software and intelligent sensors, networked over the internet to send and receive data from other intelligent devices infected with IoT Botnet malware. It is very challenging to detect IoT Botnet activity since the targeted devices are IoT devices. IoT Botnet attack patterns have not yet been disclosed. Current IoT Botnet detection is still unable to identify attack patterns, and failing to recognise key IoT Botnet behaviours has led to a loss of ability to meet detection criteria. The purpose of this research study is to identify IoT Botnet behaviour, propose an IoT Botnet attack pattern based on its behaviour, build an IoT Botnet detection model, and validate the selection of the IoT Botnet detection model using the IoT Botnet attack criteria. In addition, an IoT Botnet attack pattern is being developed by combining the IoT Botnet life cycle and IoT Botnet behaviour via IoT Botnet activities. A graph analytics-based IoT Botnet detection model has been created in order to detect IoT Botnet attack activities. The earlier detection of IoT Botnet has been visualised by IoT Botnet attack patterns using degree centrality and path analysis. The outcome demonstrated that the proposed IoT Botnets model met the detection criteria.**

***Keywords*—Internet of Things (IoT) Botnet, attack pattern, graph analytics, degree centrality, path analysis**

I. Introduction

During the worldwide breakout of the COVID-19 pandemic, reliance on technologies such as the Internet of Things (IoT), Blockchain, Artificial Intelligence (AI), Cloud Computing, and Big Data Analytics has elevated. IoT plays a significant role in mitigating the risk of coronavirus transmission by providing platforms that facilitate WHO compliance [1]. The IoT refers to internet-connected devices, including software and smart sensors. IoT can transmit and receive data from other devices such as smartphones, smart lamps, smart homes, smart toys, smart door locks, baby monitors and IP cameras [2]. According to the research of Wegner [3], expenditure on IoT hardware increased by 5.4% in 2020, while expenditure on IoT infrastructure/cloud services increased by 34.7% during the same period. Consequently, the COVID-19 pandemic has significantly impacted various areas of the IoT sector. Moreover, IoT infrastructure services are expanding, indicating IoT's widespread use during the COVID-19 pandemic. Industry 4.0 is a set of technologies that facilitate the modernisation of industry. The third annual study by Deloitte Global focused on Industry 4.0 technologies, which may be the immediate objectives of customer experience officers and have the most significant impact on various businesses [4]. Fig. 1 depicts the potential impact of static technology on industry 4.0, particularly the Internet of Things. The Internet of Things ranks highest among AI, cloud infrastructure, and big data/analytics. It demonstrates that IoT is rapidly expanding. In addition, IoT provides essential tools for automating data collection and generating insights through sensors, networks, and analytics. IoT is the essential digital stack component for the industrial sector.

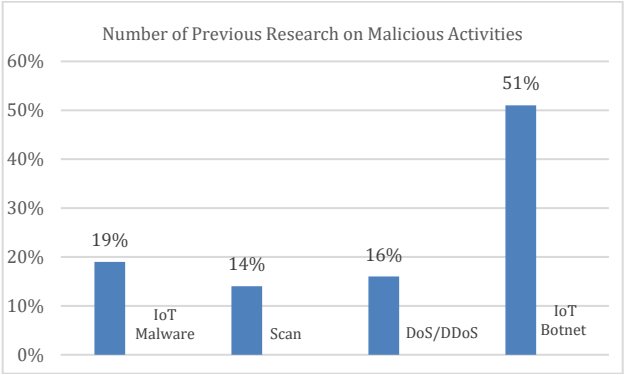

Fig. 1. Number of previous studies on malicious activities.

The growing interest in the Internet of Things indicates that IoT development will increase throughout the year. Typically, IoT devices are interconnection devices that can

Manuscript received April 12, 2023; revised June 16, 2023; accepted September 13, 2023; published March 8, 2024.

interact online. The researchers have taken the development and improvement of IoT intelligence devices seriously in response to IoT device security concerns. Thus, these interconnected devices are vulnerable to a novel attack that may exploit security flaws. For instance, IoT-based attacks are more challenging to eliminate as the number of attacks on various devices increases rapidly [5]. On the other hand, IoT devices are still in their infancy, with the majority of IoT devices being unsafe, and this situation has remained uncertain over the past few years. Thus, attackers gradually exploited these vulnerabilities to compromise vulnerable devices [6]. In addition, increasing the number of inappropriate IoT devices would attract the attention of cybercriminals and generate massive cyberattacks. As a result, Botnets have become the most prevalent cyber-attack that infects many IoT devices. The botnet is an abbreviation for the robot and network. As claimed by Abdullah *et al.* [7], the Botnet has the ability to infiltrate any system of devices. It will transform from a group of hostile computers into a computer, an automated, a drone, and a zombie. In contrast, the minimum number of Botnet infections is approximately 3.5 million, which could cause significant harm to the future of the Internet of Things applications [8]. Therefore, researchers have numerous opportunities to investigate IoT Botnet infection in terms of available solutions for detection methods, detection sources, communication protocol, and IoT Botnet type. This available solution will make it easier for the community to acquire current information.

IoT Botnet is the subject of the most extensive prior research on IoT malware, scans, and DoS/DDoS. IoT Botnets are 32% distinct from IoT Malware, as demonstrated in Fig. 1. This study focused on IoT Botnet because the increasing number of IoT devices makes it difficult to identify and evaluate the spread of malware in IoT activity. In addition, the existing IoT Botnet detection technique was flow-based, allowing malware to be automatically detected using machine learning and deep learning techniques [9].

IoT has enormous potential for expansion despite numerous identified problems [10, 11]. Therefore, IoT is not entirely secure, as most previous research required the development of proper detection techniques for the new IoT Botnet attack behaviours [12]. It has been discovered that numerous detection techniques for IoT Botnets rely on the analysis of flow packet traffic, deep packet inspection, and statistical features. Further, Chowdhury *et al*. [13] mentioned that the detection techniques capture the features of IoT Botnet attacks that are unique to specific links. The IoT Botnet is not fully understood because of the rapid development of technology. Earlier studies have encountered constraints in effectively addressing the identification of IoT Botnets. To have a greater understanding of IoT Botnets, it is essential to identify new IoT Botnet behaviours and characteristics and select the appropriate IoT Botnet detection techniques. Thus, this leads to the primary objective of this study, which is to construct an IoT Botnet Detection Model Based on Degree Centrality and Path Analysis.

II. Literature Review

IoT Botnets are typically malware that infects IoT devices under the control of a botmaster. The IoT Botnet detection model can detect bots and provide information regarding C&C communication. These detection models focus on the bot's characteristics that the botmaster commands. In addition, the detection model can track the actual bot's network traffic. The detection model is a conceptual framework that provides support and direction for detecting IoT Botnets. Typically, the detection model is the system that indicates the type of programmes and how they are interrelated.

A. Related Works

Due to the growing interest in the IoT, its development is anticipated to accelerate throughout the year [14]. According to IoT-connected device statistics, the number of IoT-connected devices will continue to increase through 2025, presenting enormous growth potential, despite the recognition of numerous obstacles. In contrast, rapid technological development has resulted in insufficient IoT knowledge. IoT devices may exploit many design flaws or vulnerabilities to commit identity theft, steal data, compromise networks, or even cause physical damage. Thus, the exponential increase of IoT device utilisation provides hackers with more opportunities to exploit them.

Moreover, according to the research of Lab [15], malware attacks on Internet of Things (IoT) devices increased substantially in 2018 compared to the previous year. IoT devices have become the new Botnet platform, and Botnet hackers exploit IoT devices [1]. Therefore, IoT devices are still insecure and may be responsible for several threats and viruses in recent years, particularly IoT Botnets.

Previous research by Patel and Upadhyay [16] focused more on recognising than revealing the motivations behind an attacker's activity pattern. Understanding typical usage patterns facilitate the detection and prevention of IoT Botnet attacks. As IoT Botnets are not entirely secure, additional research is required to develop efficient detection algorithms that account for the new characteristics of IoT Botnet attacks [17]. In addition, most investigators utilised platform functionality without addressing IoT Botnet detection attacks. As a result, hackers create increasingly sophisticated IoT Botnets and improperly conduct massive attacks on IoT devices. As IoT Botnet represents an emerging threat and high-profile security breaches, IoT Botnet activity attacks remain complex.

According to the research of Kamal *et al*. [1], modern IoT Botnet detection technology uses flow-based machine learning and deep learning for automatic detection. With the vast number of IoT devices producing voluminous amounts of data, it may be challenging to manage manually. Most IoT Botnet detection strategies rely on statistical flow/packet traffic characteristics or deep packet inspection. However, current graph-based IoT Botnet disclosure strategies have significant flaws. In addition to the overall field or subgraph topological structure, this

method captures the properties of each connection's IoT Botnet effect [13].

In addition, the graph theory associated with attack graphics can aid in identifying and preventing attacks before they have a negative impact on the business [18]. Therefore, any technique based on graph theory can demonstrate attack activity in IoT Botnet detection. The IoT Botnet Detection using a graph model is designed to close the gap in this study. To identify the IoT Botnet attack pattern, the behaviours of IoT Botnet attacks were analysed. The IoT Botnet attack pattern is then utilised as a starting point for developing the IoT Botnet Model using a graph analytic approach.

Overall, research references and case studies are helpful resources for developing the research. Fortunately, from the enthusiastic reading in the literature review, this research successfully identified the gap that requires further analysis to detect the IoT Botnet. Therefore, this research concentrates on constructing the IoT Botnet detection model based on degree centrality and path analysis.

B. IoT Botnet Detection Model Component Reviewed

The analysis of IoT Botnet detection model components was performed within six detection models. This model describes a similar component in the IoT Botnet detection model so that the activities of the detection model can be better understood. Moreover, this analysis is necessary to comprehend the involvement activities of each model to enhance the IoT Botnet detection model with an appropriate and pertinent model. As shown in Table I, the IoT Botnet detection model consists of four components: the dataset, behavior analysis, attack pattern, and detection.

TABLE I. GENERAL TERMINOLOGY COMPONENT IN IOT BOTNET DETECTION MODEL

No	Component	Description
1	Dataset	The samples of malware or binary files.
2	Behaviour Analysis	Analyses the behaviour of IoT Botnet dataset sample which are static, dynamic or hybrid.
3	Attack pattern	Visualize IoT Botnet attack activities in complete flow.
4	Detection	The process of revealing and discovering the IoT Botnet attack.

The terminology used to describe the component of the IoT Botnet detection models is displayed in Table I. A dataset represents malware and benign. It is also known as a binary sample, an ELF file, a malware and benign sample, a data bootstrap, a single malware binary, and input data. This dataset is a compilation of files containing both malware and benign samples. The malware sample's behaviors will then be analyzed and examined by the behavior analysis. This analysis of the dataset's behavior is essential to determining whether the dataset contains malware or is benign. In addition, the attack pattern will disclose the entire IoT Botnet attack flow. This attack pattern describes the behavior of an IoT Botnet attack. This attack pattern is essential for identifying potential weaknesses. Detection is the process of determining the presence of an IoT Botnet attack.

Based on Table II, the syntactic and behavioural analysis model in a study by Said *et al.* [19] focused on determining whether or not the dataset contained malware. This model investigates the dataset's behaviour using a syntactically trained classifier. However, this research was ineffective at detecting particular malware. This research only determined whether or not the dataset contained malware. Next, a study by Kamal *et al.* [1] on PSI-graph and convolutional Neural Network Classifier (CNN) model focused on combining the PSI graph with the CNN classifier. The dataset used was an ELF file. The PSI graph analyses the ELF file's behavior to determine whether or not it is malicious. In contrast, CNN is used to detect and analyses the PSI graph.

TABLE II. ANALYSIS OF IOT BOTNET DETECTION MODELS

Researchers/ Components	Dataset	Behaviour Analysis	Attack Pattern	Detection
Syntactic and behavioural analysis model [19]	✓	✓		✓
PSI-Graph and Convolutional Neural Network Classifier (CNN) Model [9]	✓	✓		✓
Behaviour-based Deep Learning Framework (BDLF) Model [20]	✓	✓		✓
BotChase Bot Detection System Model [21]	✓	✓		✓
Function Call Sequence Graph (FCSG) Model [22]	✓	✓		✓
IoT Malware Analysis Model [23]	✓	✓		✓

Moreover, a study by Yu and Siyi [20] on the Behavior-based Deep Learning Framework (BDLF) model focused on collecting the dataset from the IoTE and analyzing the dataset into CP. Then, the behavior analysis was applied to the analyzed dataset to construct the behavior graph. Within this model, SAE-based malware detection has been implemented. Moreover, in a study by Daya *et al.* [21], the BotChase bot detection system model focused on bot detection. The data bootstrap phase was the dataset phase. The behavior analysis then enters the BotChase model training phase. Ultimately, detection occurs during the inference phase.

The Function Call Sequence Graph (FCSG) model based on the study by Kawasoe *et al.* [22] divided their dataset into two sections, the first for the binary and the second for the malware. The defining characteristic of FCGS is behavior analysis in the form of graph matching. The extraction phase is then utilized for detection in this model. Finally, the IoT malware analysis model in research by Wu *et al.* [23] focused on a malware analysis detection model. The dataset is undergoing reverse engineering. In this model, the phase responsible for classifier training is the behavior analysis phase. In this model, the classifier training phase serves as the detection phase.

No research has constructed a model of attack patterns. IoT Botnet attack pattern construction is correlated with

IoT Botnet behavior. Infecting IoT activities with IoT Botnet behaviors will cause IoT Botnet life cycle stages to occur. This IoT Botnet attack pattern was designed to identify the source of malicious IoT Botnet activity. IoT Botnet attack patterns are used to verify IoT Botnets' existence and assess IoT vulnerabilities. In addition, the IoT Botnet attack patterns consist of step repetition necessary to simulate an IoT Botnet attack for earlier detection. Thus, this IoT Botnet attack pattern can be used as a reference and a solution for identifying the flow of IoT Botnet attacks. All previous detection models have flaws that requiring further models.

C. Graph Analytic

Graph analytics is a representation of data analysis research. As part of graph analytics, the analysis data will be transformed into a graph representation. Graph analytics is a graph structure consisting of data storage, retrieval, modelling, and performance. It uses graph theory, statistical, and database techniques to construct a graph [24]. Graph analytics are also referred to as graph algorithms. This graph compares the data node's strength to other data nodes. In addition, this graph displays the relationship between the data. Implementation of graph analytics can identify the optimal solution to a problem [25].

The two primary components of the graph representation are vertices and edges [26, 27]. Vertices can be referred to as nodes. Vertices constitute the object's representation. In contrast, edges are referred to as links or lines; they are the object's connection. Fig. 2 depicts the graph representation component; it demonstrates that edges connect vertices a and b.

Fig. 2. Components of graph representation.

Graph analytics also includes all methods, techniques, and tools described by Sangkaran *et al.* [28]. The graph visualises and codifies numerous network devices' relationships for comprehension. Network analysis is another name for graph analytics. This graph can be used in network analysis to determine the shortest path within a network. Consequently, this research will concentrate on graph analytics. It facilitates the organisation and research of IoT Botnet attack patterns. Graph analytics also helps represent complex data by depicting the relationship between IoT Botnet behaviours and the data [29].

The type of graph analytics that provides data for graph construction. The selection of graph type depends on the problems. Four types of graphs are centrality analysis, path analysis, community analysis, and connectivity analysis [6, 7].

1) Centrality analysis

Centrality analysis is the process of identifying the vertices of a graph. Depending on the problem, it is responsible for locating the characters of the vertices in a network. The centrality analysis includes six categories: degree centrality, eigenvector centrality, katz centrality, pagerank centrality, closeness centrality, and betweenness centrality [13]. The number of graph nodes connecting other vertices defines a graph's degree of centrality. The formulation of degree centrality is as follows: directed graph $G = (V, E)$, where V is a compilation of nodes/vertices, and E is a group of directed edges/arcs. Each edge consists of a pair of ordered vertices. For example, the directed edge (u, v) begins at u and finishes at v.

There are two degrees of centrality: in-degree and out-degree. In addition, the number of lines pointing to a vertex is its in-degree, while the number of lines pointing away from it is its out-degree. A vertices out-degree, denoted by $\deg+(v)$, is the total lines and edges that begin with those vertices [30]. A directed path is a specific direction digraph sequence of vertices with a directed line connecting each node into the line to its replacement in the series without any overlapping edges. As a result, $G = (V, E)$ is a directed graph with directed lines/edges [31].

$$\sum_v \in v\ deg+(v) = \sum_v \in deg\text{-}(v) = |E| \quad (1)$$

Next, eigenvector centrality is the graph's adjacency matrix. Katz centrality is a node measure of network centrality. It is the weight a pair of nodes is assigned. PageRank centrality is the ranking of each vertex that is proportional to in-degree and inversely proportional to out-degree. The measure of closeness and centrality is the mean distance between vertices.

In contrast, betweenness centrality is required to determine the shortest path along which vertices are connected Singh *et al.* [24]. The centrality analysis is essential for determining the characteristics of the graph's vertices. Consequently, the characteristics of vertices will be specific when analysing a problem within a graph.

2) Path analysis

Path analysis examines the distance and shape between various connected edges. It also identifies every connection between the vertices. Path analysis, for instance, can determine the shortest distance between vertices and edges. Path analysis identifies the connections between edges and vertices. Path analysis can also determine the IoT Botnet attack path between vertices.

3) Community analysis

Distance and density analysis are performed using community analysis. One vertex to another vertex that interacts with the group forms this analysis. This analysis is employed primarily in sociology and biology.

4) Connectivity analysis

Connectivity analysis is concerned with how vertices connect. This analysis can identify a weak network, such as the electrical grid. Additionally, it can be used to compare network connectivity.

Technically this research centred on graph-based analyses of the relationships between a set of nodes and links. A graph is a valuable tool for quantifying and simplifying IoT Botnet attack patterns. In addition, graphs facilitate the organisation and analysis of information

regarding IoT Botnet behaviour in a well-structured IoT Botnet attack pattern. It also aids effectively in data interpretation. Graphs are a statistically standard method for visually illustrating data relationships. The graphs present detailed data in a textless and space-saving manner. Both centrality analysis and path analysis graphs were utilised in this research. The centrality analysis was centred on indegree and out-degree centrality. Degree centrality determines the potential magnitude of the IoT Botnet attack. In addition, degree centrality depicts the most vigorous IoT Botnet attack through IoT Botnet behaviours. In contrast, path analysis requires knowledge of the graph's path. Therefore, the path of the graph can illustrate the IoT Botnet attack pattern.

Based on previous research, this research applied an IoT Botnet attack pattern to the IoT Botnet testbed environment based on the IoT Botnet life cycle and IoT Botnet behaviour. This research developed an IoT Botnet attack pattern to identify the origin of malicious IoT Botnet activities. This research validated the IoT Botnets and the vulnerability potential of IoT devices. This research focused heavily on Mirai as IoT Botnet malware; Mirai is designed to attack IoT devices, connect them to a network, and infect them. Typically, the Botnet is utilised for phishing and massive spam attacks. Nevertheless, due to the nature of IoT devices, the Mirai Botnet is ideally suited for launching DDoS attacks against servers and websites.

For the sake of ongoing scientific research, this research investigates potential improvements to previous detection models' limitations and drawbacks. Through the development of an IoT Botnet detection model, this research aimed to improve the previous detection. In addition, this research contributed to identifying IoT Botnet behaviour through the behaviours of locating, identifying, classifying, and detecting. Developing IoT Botnet attack patterns by analysing IoT botnet behaviour characteristics is the second contribution. The third contribution is the development of an IoT Botnet graph based on IoT Botnet attacks utilising graph degree centrality and representing path analysis. This research validated the IoT detection model based on IoT Botnet detection criteria.

III. Methodology

Fig. 3 depicts the environmental setup that this research adopted from Iot-23 dataset [32]. The setup was selected as this environment utilised a real network and actual IoT Botnet malware. Fig. 3 describes the IoT Botnet analysis environment for gathering the IoT Botnet dataset. It collects data from three IoT devices: Philips Hue smart lights, Somfy smart locks, and Amazon Echo. The switch acts as a router to transmit electronic data from IoT devices. DHCP and C&C servers were linked to a switch. An attacker known as a botmaster or cybercriminal controls a C&C server, issuing instructions to infiltrated computers and receiving data from the target network. This C&C server utilises cloud-based services, such as webmail and file-sharing. Use VirusTotal, Cuckoo Sandbox, and Wireshark to extract IoT Botnet behaviours. A controlled environment for experimenting with this IoT Botnets environment has been established. This research replicates the experiment's IoT-23 dataset design using real networks and IoT Botnet malware. The IoT-23 dataset was one of the newly published datasets in 2020 that provided a relatively large dataset with labelled traffic data and various Botnets. This dataset's malicious data was captured for 24 h.

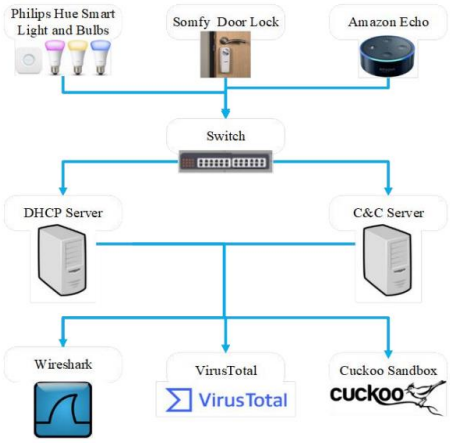

Fig. 3. Flowchart of IoT Botnet dataset collection.

These IoT devices are not simulations but real hardware. In addition, real IoT devices collect and evaluate actual network behaviour without bias or problems resulting from simulated traffic. Malicious and benign scenarios are executed in a network environment with a direct Internet connection. Mirai is a malicious scenario that results in the execution of particular IoT Botnet traffic. IoT Botnet maintains extensive records and rotates pcaps every 24 hours because each infection generates substantial traffic. However, the capture files expanded so quickly that they ceased in some cases before the 24 h mark. Consequently, the duration of various clips varies. Furthermore, the appropriate tools for exploring and researching were open sources that numerous researchers utilised for data collection and analysis.

IV. Analysis and Design

Fig. 4 depicts the IoT Botnet analysis methodology, which consists of four stages: dataset collection, IoT Botnet analysis environment, IoT Botnet behaviour analysis, and IoT Botnet attack pattern. The subsequent section discussed the specifics of the approach to analysis.

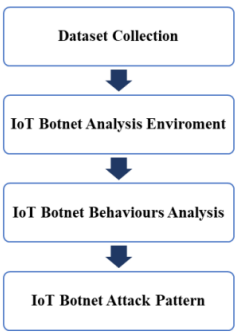

Fig. 4. Analysis approach.

A. Dataset Collection

The data collection flowchart is depicted in Fig. 5. The datasets used in this research were retrieved from Stratosphere Laboratory because they suit the research's purposed Garcia, Parmisano, and Erquiaga [32]. Nevertheless, for the purposes of this research, the datasets were uploaded to Virus Total to identify Mirai variants' existence by verifying the sample's checksum.

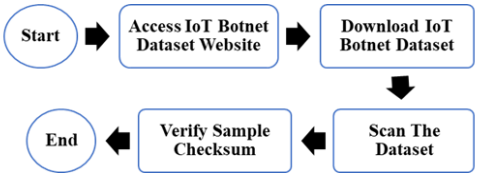

Fig. 5. Flowchart of dataset collection.

The IoT Botnet dataset has subsequently been uploaded to Virus Total. Virus Total is capable of scanning the IoT Botnet dataset by utilising static analysis. The static analysis examines the program's code before it is executed. The ability to then scan raw code prior to programme execution. For the security community, Virus Total can analyse files, IP addresses, and URLs to detect malware. In addition, the sample checksum is validated to ensure the IoT Botnet dataset is compatible with Mirai variants.

Table III displays the IoT Botnet dataset with MD5 checksums expressed in hexadecimal for each file. The dataset in Table III comprises IoT Botnet malware originating from actual IoT devices. So that it can evaluate real network behaviour without simulating traffic. This IoT Botnet dataset was captured continuously for 24 h. Unfortunately, some data generates uncontrollably massive amounts of data, causing the capture process to be terminated before 24 h.

TABLE III. IOT BOTNET DATASET [32]

No	Dataset	MD5	Variant
1	CTU-IoT-Malware-34	82062b666f09fc5c0fe4f68d1ea90916	Mirai
2	CTU-IoT-Malware-52	94d8c3ece239331b817456bcdbec6569	Mirai
3	CTU-IoT-Malware-43	6d2fa0dc9836cf1944a925c6aa77519d	Mirai
4	CTU-IoT-Malware-35	4686b69425706b336439ed9e1d74a511	Mirai
5	CTU-IoT-Malware-48	ddb4154628732f9a873b367fe9060f47	Mirai
6	CTU-IoT-Malware-44	4d182dbfaf4f03395f9fb3f056f7b3fa	Mirai

B. IoT Botnet Behaviours Analysis

Fig. 6 depicts the IoT Botnet behaviour analysis. It began by analysing each IoT Botnet dataset file individually. Two levels of analysis, Virus Total, Cuckoo Sandbox analysis and Wireshark analysis comprised the IoT Botnet behaviour analysis strategy. At this stage, the log analysis closely monitors each dataset. The existence of abnormal IoT Botnet behaviours was determined by identifying seven primary behaviours, as described in the following section.

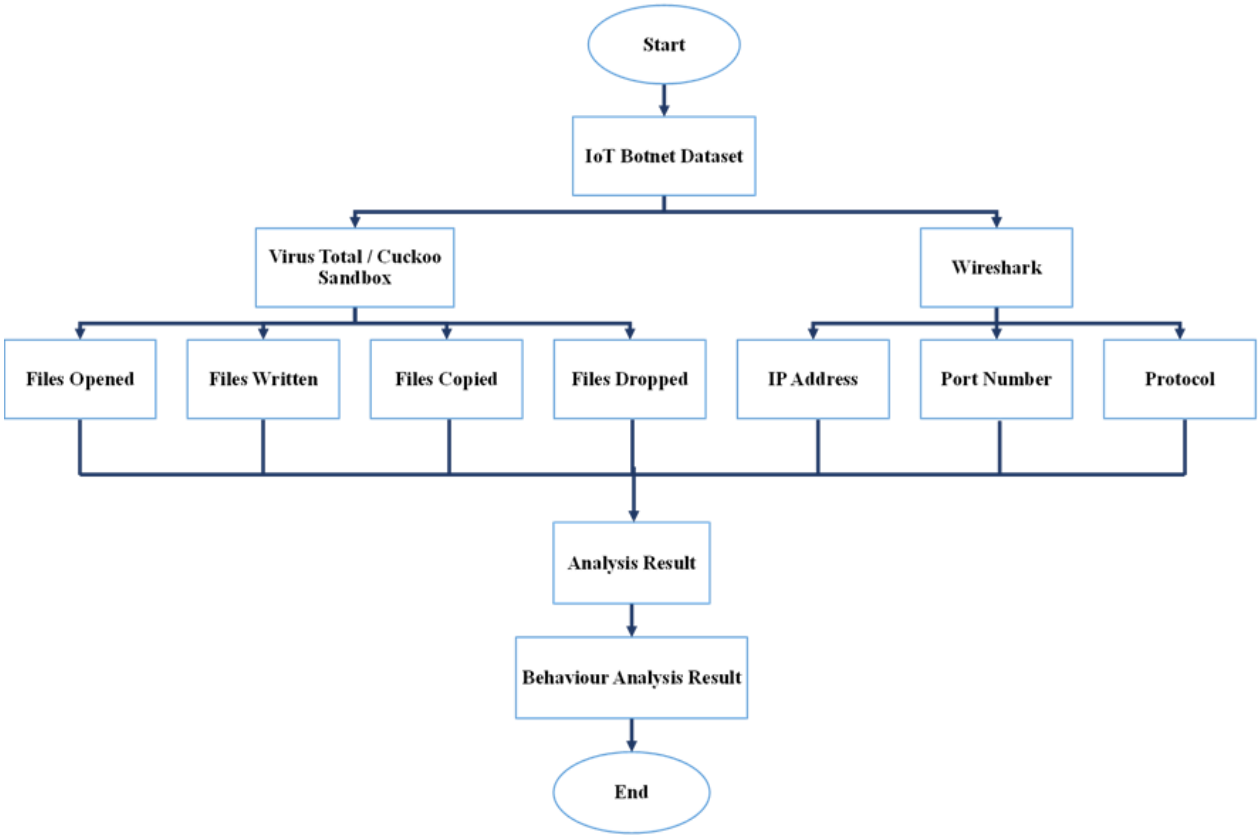

Fig. 6. IoT Botnet behaviour analysis.

1) File opened

The file opened is a modified and reviewed software file. The Opened File is the file location where IoT Botnet samples enter, and it creates an IRC channel for infected clients to join. The File Opened plugin is only accessible when an encrypted File Opened document is opened. It contains no spyware or malware, leaves nothing running on the computer, and does not modify the Windows registry or system files.

2) File written

The new file overwrites the existing one. This file was created to cause harm and conduct malicious activity. The File Written will write data to a CSV file. After writing to a file, the line-ending characters \r\n are appended. The message is either a string expression or a message number containing the file's text.

3) File copied

The copied file has the same content as the original file. This file generates a new file by copying the contents of the existing file to the target file. It can also copy a file from a local or shared folder to another file.

4) File dropper

The file dropper is intended to install malware. This malware is installed on the target system. The malware code within the file dropper is designed to evade virus scanners. The file dropper is capable of downloading malicious malware to the target file. A File dropper is a type of Trojan designed to install malware on the target file system.

5) IP address

The IP address is a protocol address for the Internet. A device's IP address is a sequence of numbers used to identify it on a network. This IP address is used for communication between two devices. This IP address can also generate spam, launch DDoS attacks, host a botnet, and contain malware in general.

6) Port number

The port number is the application's address. This port number is used for network communication. It identifies a computer's network application. The port number is associated with an IP address to communicate and identify the data transfer process. It allows one host to have multiple port numbers.

7) Protocol

The protocol enables devices to exchange data over the Internet with other devices. The majority of bots communicate with C&C via IRC or HTTP. IoT Botnet typically employs these two protocols. Meanwhile, TCP and UDP protocols were used for the same port number.

C. IoT Botnet Attack Pattern

IoT Botnet attack patterns are derived from a combination of IoT Botnet life cycle and IoT Botnet behaviour within an IoT Botnet environment. The IoT Botnet life cycle consists of four stages: scanning, attacking, infecting, maintaining, and updating. The IoT Botnet lifecycle is analysed in the IoT Botnet analysis [1, 33]. The findings of this analysis will play a significant role in developing an IoT Botnet model.

The IoT Botnet attack pattern construction is related to the IoT Botnet life cycle. Infecting IoT devices, IoT Botnet will go through IoT Botnet life cycle stages. The IoT Botnet attack pattern comprises four distinct phases. The initial stage is scanning. The scanning consists of two sections: initial infection and secondary infection. For the initial infection, the IoT Botnet initiates a network scan. It transmits SYN packets to unspecified IoT devices. It will connect to the device's IP address while the IoT Botnet waits for a response. Following this, the second infection will execute the script known as shell code. The shell code is stored in both binaries. This binary bot will be automatically downloaded to the target host. The IoT Botnet's downloaded files were extracted and analysed using Virus Total and Cuckoo Sandbox. As a result, the initial and second infections have detected the IoT Botnet behaviours of file opening, writing, copying, and deletion.

In addition, the second stage is offensive. In this stage, the IoT Botnet bot attempts to authenticate with IoT devices. When the login is successful, the bot connects to the C&C server to relay information to the botmaster and establish the connection. After that, the target host transforms into a bot and joins the botmaster's army. IP address and port are the IoT Botnet behaviours detected at this attack stage.

The third stage focuses on malicious C&C activities. The botmaster communicates with bots via the C&C channel. The bots receive commands and act accordingly. The bots will carry out malicious activities. The bot from the IoT Botnet downloads the executable file from the attack device. The file will then be deleted, and the device's temporary memory will be utilised. Through protocol, this infection stage can be detected as IoT Botnet behaviour. In addition, the fourth stage is maintenance and updating. This stage is responsible for keeping the bot's activity updated. Through the C&C channel, the botmaster has complete control over the bot and can compromise the IoT device. In order to circumvent detection techniques, the botmaster instructs bots to download updated binary. Then, the bots constantly change their C&C location to ensure their survival. However, IoT Botnets can be tracked and identified based on their port and protocol behaviour.

The attack pattern describes how an attack has been executed and is displayed. The IoT Botnet attack pattern is based on a combination of the IoT Botnet life cycle and IoT Botnet behaviour in an IoT Botnet environment. This IoT Botnet attack pattern was designed to identify the source of malicious IoT Botnet activity. This IoT Botnet attack pattern can be used to verify the existence of IoT Botnets and the vulnerability of IoT devices. In addition, the IoT Botnet attack pattern is used to simulate an IoT Botnet attack for security purposes. Consequently, this IoT Botnet attack pattern can be used as a guide and a remedy for identifying IoT Botnet attacks.

D. Proposed IoT Botnet Detection Model

The behaviours and patterns of the IoT Botnet were identified and elaborated on. The findings demonstrated the relationship between each attribute. This research proposed an IoT Botnet detection model capable of identifying the accuracy and completeness of an attack by

improving detection using degree centrality and path analysis based on its findings.

Fig. 7 depicts the IoT Botnet detection model proposed. Five components comprised the IoT Botnet detection model: dataset, identification attack pattern, degree centrality analysis, path analysis, and IoT Botnet detection. Furthermore, the IoT Botnet detection model began with the dataset collection. Then, IoT Botnet attack behaviours were identified to construct an IoT Botnet attack pattern. Continuing by selecting a graph model that applies degree centrality analysis and path analysis. Finally, the IoT Botnet was detected.

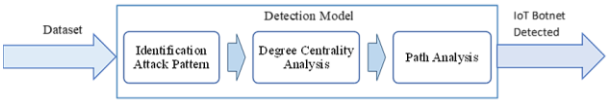

Fig. 7. Proposed IoT Botnet detection model.

V. Result and Discussion

The phase depicted in Fig. 8 consisted of two steps: constructing the IoT Botnet detection model and selecting graph analytics. The development of the model follows the IoT Botnet attack pattern. The graph containing this model construct is static. After the model is constructed based on the IoT Botnet attack pattern, degree centrality and path analysis are applied to the model graph selection. The model employs degree centrality to determine the path analysis between IoT Botnet attack patterns.

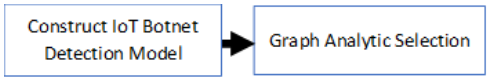

Fig. 8. Model development approach.

The CTU-IoT-Malware-34 dataset has been implemented in a graph-based format, allowing the graph to be analysed by executing the degree. Fig. 9 depicts the directed graph corresponding to CTU-IoT-Malware-34. A directed path in a digraph is a sequence of vertices and edges that point from each vertex to its successor in the line, with no edges repeated. A directed path is simple if none of its vertices is repeated. There are two degrees for a directed graph: in-degree and out-degree. The in-degree of vertices is the number of inward-pointing edges, whereas the out-degree is the number of outward-pointing edges.

Fig. 9 shows the IoT Botnet behavior in CTU-IoT-Malware-34 implemented into the graph. This graph shows the connection of the IoT Botnet attack based on its behavior. Table II show the details of the graph degree for CTU-IoT-Malware-34. The CTU-IoT-Malware-34 represents vertex 1. The file opened represents vertex 2. The desktop/file, en.UTF-8, en.utf8,en,en_US.UTF-8,en_US.utf8,en_US,locale.alias is the variable for the file. The UTF-8 is the variable character for the encoding method. In addition, UTF-8 is used for electronic communication. The locale. Alias is a database file used by the locale command. Table IV shows also the detailed vertex representing the graph's construct.

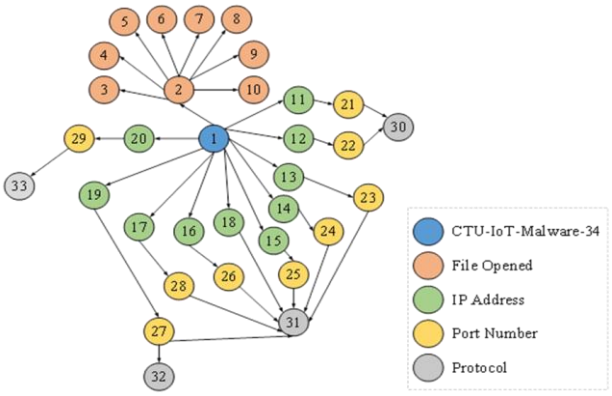

Fig. 9. Graph CTU-IoT-Malware-34.

TABLE IV. Graph Degree CTU-IoT-Malware-34

Variant name	Vertex, v	In-degree	Out-degree
CTU-IoT-Malware-34	1	0	11
File opened	2	1	8
Desktop/file	3	1	0
en.UTF-8	4	1	0
en.utf8	5	1	0
en	6	1	0
en_US.UTF-8	7	1	0
en_US.utf8	8	1	0
en_US	9	1	0
locale.alias	10	1	0
185.244.25.235	11	1	1
192.168.1.195	12	1	1
66.67.61.168	13	1	1
1.1.1.1	14	1	1
50.50.50.53	15	1	1
192.223.29.150	16	1	1
71.61.66.148	17	1	1
116.220.1.247	18	1	1
123.59.209.185	19	1	1
74.91.117.248	20	1	1
6667	21	1	1
48986	22	1	1
63798	23	1	1
1	24	1	1
53	25	1	1
62351	26	1	1
80	27	1	2
65279	28	1	1
5376	29	1	1
IRC	30	2	0
TCP	31	7	0
HTTP	32	1	0
UDP	33	1	0
Total	**33**	**39**	**39**

Based on Fig. 9 and Table IV, this graph has 39 edges and 33 vertices for the directed graph. The total in-degree is 39, $\sum \deg - v \in V\ (v) = 39$, the total of out-degree is 39, $\sum \deg + v \in V\ (v) = 39$. Then, the degree of graph theory model was constructed to detect IoT Botnet attacks. The graph of CTU-IoT-Malware-34 needs to be proven with some weighted degree calculation. $G = (V, E)$, the in-degree is $\deg -(v)$, and the out-degree is $\deg +(v)$.

The graph is a balanced directed graph for every vertex $v \in V$, $\deg +(v) = \deg -(v)$. Prove that, $\sum \deg +(v) = \sum \deg - v \in V\ v \in V\ (v) = |E|$. The sums of the in-degree, outdegree, and edges are 39. This proves that the graph for this dataset is valid based on this equation. Furthermore, the principal aggregate counts the number of active edges across all vertices approaching edges. Therefore, the two

totals are equivalent to the number of edges. Thus, this research analyses the IoT Botnet attack patterns using a degree centrality in the graph analytic approach.

Then, path analysis examines the distance and shape between various connected edges. It also purposely identifies every connection between the vertices. Path analysis, for instance, can determine the shortest distance between vertices and edges [24]. This section discussed the result of the path analysis implementation for the CTU-IoT-Malware-34 datasets.

The outcome of the path analysis is presented in Table V. The path for CTU-CTU-IoT-Malware-34 has the highest degree path with 39 paths. CTU-IoT-Malware-48 has the shortest path with its 18 paths. This path analysis helps to measure the potential relationship between the IoT Botnet attacks. Path analysis is also a statistical method for investigating the IoT Botnet attack pattern. CTU-IoT-Malware-34 has the longest path and most aggressive IoT Botnet attack compared to other datasets. Using degree centrality and path analysis to develop the graph, the IoT Botnet can be detected through the graph analytic approach. Degree of centrality and path analysis information used to detect IoT Botnet activities.

TABLE V. PATH ANALYSIS CTU-IOT-MALWARE-34

Dataset	IoT-Malware-34	IoT-Malware-35	IoT-Malware-48
Edges, E	39	27	18
Vertex, V	33	26	16
$\sum_{v \in V} \deg -(v)$	39	27	18
$\sum_{v \in V} \deg +(v)$	39	27	18

The research was time-consuming, particularly during the pandemic of COVID-19, especially in the data analysis process which is it needs more time. Continuous research significantly needs to improve the IoT Botnet attack detection model. Constant actions are required in detecting other behaviors to enhance the security level in current demand. Perhaps, analyzing and testing new behaviors using other network analyzer software that provides superior capabilities is essential. Besides that, the outstanding capabilities support more excellent analysis for large capture data packet files for advanced research. Apart from concentrating on the different behaviors, future research is encouraged to use another mechanism or algorithm to recognize the IoT Botnet attacks and IoT Botnet activities.

VI. CONCLUSION

This study examines the analytical methodology employed in the development of an IoT Botnet detection model utilizing degree centrality and path analysis. The fundamental concept underlying the construction of an IoT Botnet model entails the integration of the IoT Botnet life cycle, IoT Botnet behaviors, and IoT Botnet patterns. In addition, this research includes a discussion and analysis of centrality degree and path analysis. Using degree of centrality and path analysis, IoT Botnet activities were also demonstrated. The degree of centrality and path analysis can be used as measurement criteria to detect the strongest IoT Botnet attacks.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Wan Nur Fatihah Wan Mohd Zaki and Raihana Syahirah Abdullah conducted the research, analyzed the data, and wrote the paper. Warusia Yasin and Siti Rahayu Selamat verified the flow of research. Syazwani Yahya checked the grammatical errors in this paper. At last, all authors had approved the final version.

ACKNOWLEDGMENT

This publication has been supported by the Centre of Research and Innovation Management (CRIM), Universiti Teknikal Malaysia Melaka (UTeM). The authors would like to thank UTeM and INSFORNET research group members for their support.

REFERENCES

[1] M. Kamal, A. Aljohani, and E. Alanazi. (2020). IoT meets COVID-19: status, challenges, and opportunities. [Online]. Available: http://arxiv.org/abs/2007.12268

[2] W. M. Zaki, W. N. Fatihah, R. S. Abdullah, W. Yassin, M. Faizal, and M. S. Rosli, "Constructing IoT botnets attack pattern for host based and network based platform," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, no. 8, pp. 1–8, 2021.

[3] P. Wegner. (2021). Global IoT spending in 2021 to grow 24%, led by investments in IoT software, IOT analytics. [Online]. Available: https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/

[4] S. Goswami, A. M. Bagchi, A. Sain, and V. Tyagi. (2020). Internet of Things (IoT). [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-mediatelecommunications/in-tmt-IoT_Theriseoftheconnectedworld-28aug-noexp.pdf

[5] L. Z. Granville and C. B. Margi, "Improving IoT botnet investigation using an adaptive network layer," *Sensors*, pp. 1–16, 2019.

[6] N. Koroniotis *et al*., "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[7] R. S. Abdullah *et al*., "Recognizing P2P botnets characteristic through TCP distinctive behaviour," *International Journal of Computer Science and Information Security*, vol. 9, no. 12, pp. 12–16, 2011.

[8] M. Berhad, "National Internet of Things (IoT) strategic roadmap: A summary," *MIMOS Berhad*, vol. 2, 2018.

[9] H. T. Nguyen, Q. D. Ngo, and V. H. Le, "A novel graph-based approach for IoT botnet detection," *International Journal of Information Security*, vol. 19, no. 5, pp. 567–577, 2019.

[10] T. S. Gopal *et al*., "Mitigating mirai malware spreading in IoT environment," in *Proc. 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 2226–2230.

[11] Z. K. Zhang *et al*., "IoT security: Ongoing challenges and research opportunities," in *Proc. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014, pp. 2163–2871.

[12] M. Wazzan *et al*., "Internet of things botnet detection approaches: Analysis and recommendations for future research," *Applied Science*, vol. 11, 5713, 2021.
[13] S. Chowdhury *et al*., "Botnet detection using graph-based feature clustering," *Journal of Big Data*, vol. 4, no. 1, 2017.
[14] I. Gartner. (2018). Gartner identifies top 10 strategic IoT technologies and trends. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends
[15] K. Lab. (2018). New IoT-malware grew three-fold in H1 2018. [Online]. Available: https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-foldin-h1-2018
[16] K. Patel and H. Upadhyay, "A survey: Mitigation of DDoS attack on IoT environment," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 6, pp. 94–96, 2018.
[17] W. S. Hamza *et al*., "IoT botnet detection: Challenges and issues," *Test Engineering and Management*, pp. 15092–15097, 2020.
[18] K. R. Saoub, *Graph Theory: An Introduction to Proofs, Algorithms, and Applications*, CRC Press, 2021.
[19] N. B. Said, F. Biondi, V. Bontchev, *et al*., "Detection of Mirai by syntactic and behavioural analysis," in *Proc. 2018 IEEE 29th International Symposium on Software Reliability Engineering (ISSRE)*, Memphis, TN, USA, 2018, pp. 224–235. https://doi.org/10.1109/ISSRE.2018.00032
[20] D. Yu and Z. Siyi, "Malware detection based on deep learning of behavior graphs," *Neural Computing and Applications*, vol. 31, no. 2, pp. 461–472, 2019.
[21] A. A. Daya *et al*., "A graph-based machine learning approach for bot detection," arxiv preprint, arXiv:1902.08538, 2020.
[22] R. Kawasoe *et al*., "Investigating behavioral differences between IoT malware via function call sequence graphs," *ACM Computing Surveys*, vol. 4, no. 9, 2021.
[23] C. Wu *et al*., "IoT malware detection using function-call-graph embedding," in *Proc. 2021 18th International Conference on Privacy, Security and Trust (PST)*, 2021. https://doi.org/10.1109/PST52912.2021
[24] D. K. Singh, P. K. D. Pramanik, and P. Choudhury, "Big graph analytics: Techniques, tools, challenges, and applications," *Data Analytics*, 173, 2018.
[25] D. Victory. (2021). What is graph analytics and its top tools. [Online]. Available: https://analyticsindiamag.com/what-is-graph-analytics-its-top-tools/
[26] What Is the Internet of Things (IoT)? [Online]. Available: https://www.oracle.com/internet-of-things/what-is-iot/
[27] N. S. Abouzakhar, A. Jones, and O. Angelopoulou," Internet of things security: A review of risks and threats to healthcare sector," in *Proc. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017.
[28] T. Sangkaran, A. Abdullah, N. JhanJhi, and M. Supramaniam, "Survey on isomorphic graph algorithms for graph analytics," *International Journal of Computer Science and Network Security*, vol. 19, no. 1, pp. 85–92, 2019.
[29] K. D. Rangaswamy and M. Gurusamy, "Application of graph theory concepts in computer networks and its suitability for the resource provisioning issues in cloud computing—A review," vol. 172, 2018.
[30] L. Euler and S. Bridges, "Weighted degree, weighted in-degree, weighted outdegree authority score," *Hub Score*, vol. 101, no. 11, 2013.
[31] K. H. T. Da and T. Touili, "Malware detection based on graph classification," in *Proc. the International Conference on Information Systems Security and Privacy*, 2017, pp. 455–463.
[32] S. Garcia, A. Parmisano, and M. J. Erquiaga. IoT-23 dataset: A labeled dataset of malware and benign IoT traffic. [Online]. Available: https://www.stratosphereips.org/datasets-iot23
[33] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378–403, 2013.