IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 25, 2021, accepted November 22, 2021, date of publication November 25, 2021,
date of current version December 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3130714

Detecting Internet of Things Bots: A Comparative Study

BEN STEPHENS[1], (Student Member, IEEE), ARASH SHAGHAGHI[2], (Member, IEEE), ROBIN DOSS[1], (Senior Member, IEEE), AND SALIL S. KANHERE[3], (Senior Member, IEEE)

[1]Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, VIC 3220, Australia
[2]School of Accounting, Information Systems and Supply Chain, RMIT University, Melbourne, VIC 3000, Australia
[3]School of Computer Science and Engineering, The University of New South Wales, Sydney, NSW 2052, Australia

Corresponding author: Ben Stephens (bastep@deakin.edu.au)

ABSTRACT Since the Mirai botnet attacks in 2016 research into the Internet of Things (IoT) botnet malware has increased substantially. IoT botnet relevant threats continue to rise, impacting businesses and users. This paper aims to contribute to the problem space by compiling and synthesizing the relevant literature over the last five years to provide an overview of the most recent advances in IoT botnets, their detection and prevention, and laying down the future research directions required to better address this ever growing threat.

INDEX TERMS Internet of Things, botnet, IoT botnet detection, IoT botnet survey, malware.

I. INTRODUCTION

As computing has become more miniaturized over time, smaller devices could be attached to networks. This started as industrial control systems, in areas such as electricity generation and distribution, and water treatment and pumping, with physical devices such as pumps or relays being actuated remotely. As prices dropped in the 2010's, small devices started to appear in the homes of wealthy countries as convenience devices. This included programmable space heaters, lighting, and air conditioning devices. With the rise of smartphones and always-connected Internet services these devices, along with remote industrial and scientific instruments, are starting to become more ubiquitous. And so the Internet of Things (IoT) was born [1].

Malicious software existed almost since computers were first connected together. A botnet is a network of computing devices hijacked by malware that can be controlled remotely by an attacker, called a 'botmaster'. The botmaster will then send commands to the bot network instructing it to perform a number of different tasks, ranging from attacks such as distributed denial of service (DDoS), disseminating spam or simply ordering it to spread and infect more devices [2].

According to Spamhaus's 2019 Botnet Threat Report [3], which measures the number of botnet command and control servers (abbreviated as C&C or sometimes C2) over time, in 2019 the number of C&C servers detected was 17,602. This is a substantial growth compared with 7,314 C&Cs reported in 2014. The same report in the first quarter of 2021 indicates 24% increase in just a few months [4] (i.e., the last quarter of 2020). The growing number of botnets is therefore an increasing cyber security concern [5].

The Internet of Things (IoT) presents a unique set of security challenges, as devices are often unmonitored, remotely located, and have limited computing resources. Many IoT devices are based on low-power-consumption chips such as MIPS, ARM or Arduino [6]. Many use limited functionality chips that are purpose-made, such as sensors and actuators.

Hackers have found an opportunity in the heterogeneous IoT landscape with many manufacturers creating devices, where price and time-to-market are their primary objectives rather than security [7]. There are several open standards for IoT communication protocols including Zigbee, Constrained Application Protocol (CoAP), and Bluetooth Low Energy [8]. Many manufacturers, however, choose to use proprietary protocols instead, or may choose how to implement standards themselves.

Firmware updates may be unavailable or poorly controlled and communicated, and default credentials are often used, making IoT devices an attractive target for attackers.

A. METHODOLOGY

It was found that the 2016 Mirai malware was a driver for research in this area, and much of the research that was analyzed focuses on preventing a repeat of similar future attacks. Therefore papers from the last five years were collected to expose the current state of research on IoT botnets.

The associate editor coordinating the review of this manuscript and approving it for publication was Xianzhi Wang.

Search terms were used on Google Scholar and EBSCOhost database for ''IoT Botnet'' and ''Internet of Things Botnet''. The resulting list of approximately 1,200 conference and journal papers' titles were reviewed for relevance. Papers published at well-established and top-ranking publications including Q1 on SJR (SCImago Journal & Country Rank) or A/A* on CORE 2020 (Computing Research and Education) portals were selected, given the stringent peer review process and traditional impact in the field.[1] We initially selected 19 core papers that gave a range of IoT botnet detection methods which informed the formulation of our research questions:

1) What are the methods for identifying and classifying malware detection in IoT devices?
2) What IoT malware detection methodologies are better suited to detect IoT bots?

Drawing on the literature review guidelines given by Snyder [9] we reviewed each paper within the targeted five-year time frame, leading to our selection of around 50 of the most relevant papers. We read and summarized these papers to classify them, and then followed up the reference lists to 'snowball' more relevant literature, which was again categorized and summarized.

B. RELATED WORK

Several surveys on botnets have been conducted, as have several IoT security surveys, but only one could be found that specifically addresses the issue of botnets in IoT devices. Vu *et al.* [5] provided an extensive survey on botnets, focusing on the incentives for their creation, how they have evolved and current trends. Cozzi *et al.* [6] traced the evolution and code-sharing of IoT malware and provided valuable insight into the relationships between malware families. Costin & Zaddach analysed malware in IoT but did not look specifically at botnets in their 2018 BlackHat paper [10]. They conducted an earlier survey in 2014 [11] which is focused solely on security of embedded firmware. Meneghello *et al.* [8] provided a comprehensive survey of vulnerabilities in IoT devices. Rytel *et al.* [12] conducted another survey of vulnerabilities but focus on the data sources for vulnerability sharing.

Wazzan *et al.* [13] wrote the most similar paper to this, having conducted a literature review on botnets in IoT. However, the research questions, motivations, and scope are different and we find their survey complimentary to ours. Wazzan *et al.* primarily focus on the phases of infection detection with the majority of papers reviewed focusing on early-detection of IoT bots. Several high-quality and influential research publications from the past few years in IoT botnet (e.g., [10], [11], [14], [15] among others) are overlooked. Recent significant IoT botnet threats such as Hajime are only discussed in a few words, the paper has limited focus on mitigation and it does not establish future research directions systematically. Our contribution differs from [13] in that we compare detection and mitigation methods (e.g., network blocking, software patching) and establish a framework for future research in detecting and mitigating IoT bots. More important, we focus on different papers within the same problem space (i.e., IoT botnet instead of botnet broadly) in the form of a targeted literature review focusing on the more stringently reviewed research publications published at a higher quality conferences and journals.

[1] When looking at future research directions, this requirement was relaxed for a few papers to accommodate inclusion of promising early ideas.

C. CONTRIBUTIONS

To the best of our knowledge this paper is the first IoT botnet specific survey which compares detection methods and suggests a framework for future research. Our main contributions are:

- A detailed review of IoT botnet attack impacts to identify the problem space.
- A systematic review of recent IoT botnet detection and mitigation literature (2015-2020) inclusive of methodologies, contributions, and shortcomings.
- Review of the emerging IoT botnet threats as well as emerging research directions.
- Recommendations for future research directions, open research questions, and a framework for future research.

In Section II we explore the history of botnet malware and methods of infection for traditional PC malware versus embedded systems such as IoT devices. Section III details methods of botnet detection in IoT devices, which is split into two subsections. Section III-A looks at the research into Host-based detection and Section III-B explores Network-based detection. Network detection is further split into remote (over the network) detection and local detection via the router/gateway at the network edge. Section IV explores new research into emerging directions as well as emerging threats. In Section V we discuss a framework for future research and the open questions that have not been answered. In Section VI we provide our final thoughts and conclude the paper.

II. METHODS OF ATTACK

A. TRADITIONAL BOTNETS

The threat of botnets were first recognized in the 1990's, with early botnets such as Eggdrop, SDBot and Sub7 spreading through Trojan horses or email worms to infect hundreds of personal computers and their associated networks. These botnets were then used to send spam or conduct DDoS attacks against the botmaster's targets. Botnets of this era often used Internet Relay Chat (IRC) servers as a central point for the botmaster to control the bots [20].

As malware evolved so did botnets, with peer-to-peer (P2P) botnets being developed in the mid-2000's to avoid having the single point of failure of a central C&C server. The 2010's were the decade when botnets starting becoming monetized according to Cimpanu [21], first as 'DDoS for hire' then more recently, cryptocurrency-mining botnets. Sophos Labs [22] disagree with the dating, stating that the use of botnets for pharmacy spam from 2006 was the start of botnet monetization.

Crypto botnets are being used to 'mine' cryptocurrencies such as Bitcoin or Monero [23] to directly add to the botmaster's wallet. Crypto botnets have been observed since 2014 [24] running on embedded devices such as routers, security cameras and set-top boxes, however these are less effective than higher-powered computing devices. The most recent monetization method employed by botmasters is ransomware, whereby infected machine's files are encrypted and a ransom demand is displayed before the files are irretrievably removed.

Botnets impact in two ways; the device is no longer under the control of the legitimate owner, and is then used to generate malicious activity on the Internet. Bots will remain quiet and behave as normal until the malware is triggered, which complicates their detection and mitigation. Botnets are a problem for the Internet as a whole as they are used to send large amounts of spam from unwitting hosts and can also be used to create huge DDoS attacks. Some of the largest botnet attacks were comprised of IoT devices, as we will explore in the following section.

B. IoT ATTACKS

Traditional botnets are able to infect PCs which have high computing resources and the ability to run anti-malware programs. IoT devices, with lower resources, do not have the capacity to run anti-malware software which makes them more vulnerable to infection and less able to mitigate threats. Vulnerabilities that can turn IoT devices into bots include: 1) brute-force password guessing [25], 2) unsecured services [26], 3) leaked/reused passwords, 4) network stack vulnerabilities in unpatched firmware [10], and 5) physical access to the device.

There is no central database of IoT vulnerabilities, however Rytel, Felkner & Janiszewski [12] have explored the USA and China's National Vulnerability Databases (NVD and CNVD respectively) and other databases. From this, they extracted features they plan to use in a future IoT vulnerability reporting database.[2]

Mirai's variants are the most widely studied botnets, due to the scale of the attacks. The first reported attack, on the ''Krebs on Security'' blog (discussed below), hit 623Gbps using simple TCP port flooding, which knocked the website offline. This was followed by the attack on Dyn which was between 1-1.5Tbps [27] which disrupted domain name resolution for Dyn's customers, including Amazon, GitHub, Netflix and Twitter. This botnet was created by exploiting default passwords such as 'root/root' or 'admin/admin' [14] that were left on the devices when they were installed.

Antonakakis *et al.* [14] assembled an army of researchers in 2017 to analyze the Mirai botnet. Mirai peaked at 600,000 infected IoT devices in November 2016, one of the largest botnets at the time. When it was used to attack the Krebs on Security blog the botnet was smaller at around 120,000 hosts, but had grown to its peak by the time of the Dyn attack. It is suspected that attackers were attempting to bring down Sony's PlayStation network, whose name servers are hosted by Dyn. Other targets include Lonestar Cell, a Liberian telecommunications provider and OVH, a French cloud hosting provider. After Mirai's source code was publicly released, variants started appearing [14], attacking new targets using new tactics such as reflection attacks, where DDoS traffic is bounced off a third party.

Gu *et al.* [28] predicted in 2008 that a peer to peer (P2P) IoT botnet was coming, 8 years before the emergence of Hajime, the first IoT P2P botnet. Between 2016 and 2019 Hajime was examined in depth by Herwig *et al.* [17]. Hajime peaked at around 300,000 infected hosts, before returning to a steady state of about 90,000. Herwig *et al.* believe the worm was created to secure vulnerable devices, as no attacks have ever been observed from Hajime. However, other researchers such as [21] disagree, claiming the botnet may be used for proxying – masking malicious Internet traffic.

Bashlite (also called Gafgyt), the precursor to Mirai displayed similar characteristics, but was missing Mirai's encrypted traffic and had hard-coded IP addresses for its C&C servers [2]. Brickerbot is another significant botnet from 2017 that was used to create a 'permanent denial of service' attack by exploiting default credentials, then wiping vulnerable devices storage and network capabilities [18] turning them into 'bricks'. Costin and Zaddach [10] estimate that over 10 million devices could have been affected by this attack.

Persirai [19] was a 2017 Mirai variant that exploited an empty password bug in certain IP cameras that allowed it to gain user passwords in clear text [26]. Other vulnerabilities have been exploited and combined with the released Mirai code-base to create smaller botnets such as Reaper in 2017.

As the number of IoT devices continues to grow, botnets will become larger, and their attacks more devastating. It is therefore vital that ways are found to protect these devices from malware [27]. Table 1 gives an overview of the most significant IoT botnets to date. The data shows that 95% of botnet attacks are caused by default credentials being left on devices.

III. METHODS OF DETECTION

There are two main groupings of botnet detection methods; network-based and host-based. Network-based detection methods can be used with any networked device remotely. Host-based methods require the firmware from a device to be loaded onto a computer and studied either statically (not running) or dynamically (running).

An advantage noted by several researchers when comparing botnet-infected IoT devices with general purpose computing devices is that IoT devices are not multipurpose machines, so will usually only follow specific patterns of execution and network usage. This leads researchers to explore the two available methods of detection, host-based – discovering malware by examining the device firmware, or network-based where network traffic is analyzed.

[2]https://www.variot.eu

TABLE 1. IoT botnet families and impact.

Years Active	Family	Peak bots	Vulnerability Exploited	Affected Devices	Impact	Source Released
2012	Carna [16]	420,000	default credentials	routers, set-top boxes	research only	no
2016-	Bashlite	120,000	default credentials	IP cameras, DVRs	DDoS	yes
2016-	Mirai [14]	600,000	default credentials	IP cameras, routers	DDoS attacks	yes
2017-	Hajime [10], [17]	300,000	default credentials	multiple devices	minimal	no
2017	Brickerbot [10], [18]	10,000,000	default credentials	multiple devices	destroy devices	partial
2017	Persirai [10], [19]	120,000	authentication bug	IP cameras	DDoS	no

TABLE 2. Host-based detection approach.

Year	Paper	Purpose	Unique Features	Citations	Accuracy	Precision
2014	[11]	Large-scale survey	Embedded firmware	353	NA	NA
2018	[10]	Survey	IoT firmware	30	NA	NA
2016	[25]	Capture samples	IoT Honeypot	145	NA	NA
2014	[15]	Dynamic Analysis	Real hardware-emulated software hybrid	211	ND	ND
2018	[29]	Static Analysis	Image recognition AI algorithms	94	95%	93%
2018	[30]	Static Analysis	Strings graphed, trained neural network	25	92%	91%

A. HOST-BASED DETECTION

Table 2 summarizes the most recent literature focusing on host-based detection. It gives details of citations to measure impact of each paper, accuracy (correctly predicted observations) where reported for detection, and precision (correctly predicted positive observations), where reported.

Host-based detection describes the methodology for analysis of code on a device. It can be categorized into two distinct methods. First the static method, where binaries or source code are examined without executing the code. The second method is dynamic analysis, where a sandbox is created and monitored, and the code is executed to observe its effects.

Static analysis is slow, but more conservative, and in malware is much less likely to cause an unexpected consequence such as infection. Dynamic analysis is faster, however all paths of execution and variables cannot be guessed by the analyst so some functionality of the malware may be missed [31].

Costin *et al.* [11] provided a comprehensive survey of embedded systems firmware in 2014. They updated their research in 2018 [10] with a similar survey of malware, specifically on IoT devices. This section will add to their work with novel techniques that have been discussed since then.

Pa *et al.* [25] proposed and implemented an IoT honeypot, which presented itself to the Internet as varied unprotected IoT devices to capture malware. It emulated telnet services of various devices on the front end, with a back-end connected to a series of virtual environments emulating embedded CPU architectures. During its 81 days of operation, the honeypot had 79,935 download attempts by malware from 180,581 Internet hosts. The researchers manually downloaded 106 samples and analyzed them in their emulation system, identifying 5 families of IoT malware.

Su *et al.* [29] propose a technique where IoT firmware binaries (executable low-level software) were converted to gray-scale visual images, then passed through a shallow (2 layer) convoluted neural network algorithm. The neural network classified the image as malware or goodware. Basic firmware to image processing can be done on the IoT device, then the image can be passed to a cloud-based classifier. They do, however warn that this method may be vulnerable to binary obfuscation.

Nguyen *et al.* [30] outlined a method of static analysis of firmware source code or binary executables, searching for printable strings then fed those to a convoluted neural network. The neural network, which had been trained on known good and malware samples, put the strings into context and classified them as malware or goodware, whether they have been obfuscated or not. They did this by leveraging a control flow graph, which traverses paths of execution in the sample. As shown in table 2 they achieved 92% accuracy and 91% precision.

Zaddach *et al.* [15] described Avatar, a dynamic approach that relied on a hybrid of hardware to provide the input/output of the system, and software running on an external emulator to dynamically analyse (possibly malicious) firmware. They created an open-source framework based on QEMU[3] with debugging interfaces that could be used to analyze and change device execution. The authors provided three examples of Avatar in action: an analysis of a hard drive's on-board firmware, a vulnerability assessment of a Zigbee device, and manipulation of a mobile phone GSM network stack - proving the versatility of their platform.

B. NETWORK-BASED DETECTION

Several methods have been suggested, modeled and prototyped for network-based detection of IoT malware using network traffic. The advantage of these methods are that the device can stay in place, connected to the network and continue performing its function. Table 3 provides a summary of the most recent literature with a focus on network-based detection. Citations are included for impact on further research and accuracy (correctly predicted observations)

[3]https://www.qemu.org

TABLE 3. Network-based detection approach.

Year	Paper	Purpose	Unique features	Detect/ Mitigate	Citations	Acc.	Prec.
2020	[34]	Detection	Adhoc overlay networks, traffic monitoring	m	17	98%	98%
2017	[35]	Block at router	Whitelist/blacklist system	m	53	100%	100%
2018	[36]	Deep packet inspection	Recurrent neural network	d	73	92%	99%
2018	[37]	Anomaly detection	Autoencoders, detect attack stage	m	304	100%	99%
2017	[38]	Remote fingerprinting	Network fingerprinting, SDN compartments	m	327	NA	NA
2018	[39]	Reduced features	Unsupervised ML	d	24	92%	90%
2020	[40]	DNS detection	Deep learning for name generator	d	49	99%	85%
2018	[41]	P2P bot detection	Reduced feature set neural network	d	62	99%	99%

and precision (correctly predicted positive observations) are included where available.

Emerging research aimed to leverage recent network advances to enhance detection and mitigation of IoT bot threats. For instance Software Defined Networking (SDN) is a recent network paradigm that splits network operations into data and control planes, decoupling the functions from the hardware. It adds separate layers for policy definition, enforcement, and implementation, allowing the network to be reconfigured dynamically in real time using an ''intelligent orchestration and provisioning engine'' independently from the hardware used [32].

Similarly, Network Function Virtualization (NFV), use virtual machines to emulate hardware. This can be useful for adding network resources such as firewalls, domain name resolvers, virtual routing or traffic control on an as-needed basis [33]. This technology could be used in the future for mitigation of botnet malware.

1) LOCAL DETECTION

Habibi *et al.* [35] proposed a software solution called Heimdall that they implemented on a Linksys router. This solution is in two parts, a traffic manager which continuously validated traffic and a whitelist manager that managed allowed and blocked addresses. A profile of each device was built when they were connected to the network, and once patterns were established the system moved to an enforcement phase per device. DNS requests were mediated through the system, which checked validity of the DNS response to prevent DNS poisoning attacks. While the results in table 3 look significant, this is based on just a few test devices.

Miettinen *et al.* [38] proposed methods of detection and mitigation at the network edge on the gateway in conjunction with a web-based IoT security service provider. The gateway fingerprinted the connected IoT device, then sent the fingerprint to the service provider, who sent back a classification of *restricted, trusted* or *strict* which was applied by the gateway depending on whether vulnerabilities exist. They also provided a method for fingerprinting devices as they were inducted into the network.

Hafeez *et al.* [34] built on the work of Miettinen *et al.* [38]. They had the gateway classify devices in both cases, but where Miettinen *et al.* proposed a central service provider, Hafeez *et al.* proposed all the work be done by the network gateway. They created a prototype that could be run on a regular consumer-grade router with minimal impact (1.8% increased latency). It was a modular system with monitoring, detection and enforcement modules which used fuzzy C-means clustering, after feature extraction, to classify network traffic. They then used SDN to create adhoc network overlays to modify traffic flows.

Meidan *et al.* [37] ignored the infection stage of botnet malware entirely, under the assumption that some malware will get past any filters, and concentrated their network anomaly detection at the point when devices are given the attack order by the botmaster. They used autoencoders, a compressed neural network, training them on benign traffic. Once the autoencoder was trained for a particular device it could detect anomalous network behavior. They infected 9 commercial IoT devices with Mirai and Bashlite to test their detection method. Their results detected 100% of attacks in the samples and a false-positive rate of 0.007 in 174-386ms.

2) REMOTE DETECTION

Nõmm and Bhaşi [39] used Machine Learning (ML) to detect anomalies in IoT network traffic by only training benign data. Their system detected outlying data points and classified them as suspicious. Nõmm & Bhaşi performed multiple tests to determine the best ML algorithm for accuracy (low false-negative) and precision (low false-positive rate) when a system is trained on benign data and then exposed to combined normal and botnet data from Mirai and Bashlite botnets. They concluded that the most effective ML algorithms were five feature-point entropy for feature selection and isolation forests for unsupervised learning. These performed better than local outlier function, support vector machines, and Hopkins statistics for botnet traffic detection. The authors updated their work in [42] with an examination of a hybrid feature selection model.

McDermott *et al.* [36] used a deep learning method called Bidirectional Long Short Term Memory based Recurrent Neural Network (BLSTM-RNN). This method fed whole packet data into a neural network over long time periods to extract text features, then contextualized the data. The self-learning capabilities and knowledge of the past that the RNN provided allowed for the detection of botnet traffic even when there was a large time gap between attacks. This came at a processing cost but provided very high levels of accuracy, even where malware had mutated.

Vinayakumar *et al.* [40] explored converting domain names extracted from malware binaries into images then

using Siamese Neural Networks. They used this to analyze whether domain names had been computer-generated or were legitimate domains to detect domain generation algorithms (DGA). The same researchers have explored the use of deep learning in PC botnet detection in previous papers [43], [44].

Sriram *et al.* [45] built on the work of Vinayakumar *et al.* [40] by comparing multiple ML and Deep Neural Network (DNN) algorithms when applied to normal and botnet traffic to classify them. They explored which algorithms use the least time for training and detection and presented their results. They showed that the most promising techniques were Decision Tree (DT) for differentiating botnet vs. normal traffic, and that 4-hidden-layer DNN is effective in classifying which botnet is operating at real-time speeds. In this paper they also used a t-distributed stochastic neighbor embedding visualization, which separated the attack and normal traffic graphically. They suggested that this visualization could be run through a convoluted neural network to achieve differentiation using existing computer vision algorithms.

Alauthaman *et al.* [41] proposed a method targeted at detecting P2P botnet traffic by passively monitoring network traffic, extracting TCP headers and reducing the data to a feature set. This method did not require deep packet inspection and so was scalable. The remaining features were fed to a resilient back-propagation neural network using a classification and regression tree (CART) algorithm. Experimental results showed that the CART algorithm was faster and more effective than random forest (RFtree) and principle component analysis (PCA) neural network algorithms.

While machine learning and AI models are effective when trained on mixed botnet and normal traffic, they have a couple of drawbacks. They use more computing power than other methods, and for large volumes of traffic they may become a bottleneck unless appropriate resource planning is undertaken. They can also be tricked using adversarial machine learning techniques [46].

Local detection is useful when the scale of the IoT deployment is not large and the limited resources of a consumer router are able to scan and classify network traffic in real time. Remote detection suits larger networks such as an enterprise or campus as the remote resources are used on faster devices such as servers or high-end workstations. A combination of detection methods would be ideal for sensitive IoT devices such as industrial control systems.

IV. EMERGING DIRECTIONS

In this section we will explore future threats that have been theorized and emerging directions in botnet detection and mitigation. These are broken down to Emerging Threats and Emerging Detection Methods, which are further categorized by their themes of Trust and Patch Delivery. This is not a comprehensive list, but rather research that the authors believe have not had the attention they deserve and as such we highlight them here.

A. EMERGING THREATS

Soltan *et al.* [47] described a theoretical attack they call BlackIoT on a power grid by a group of malware infected high wattage IoT devices such as water heaters, air conditioners and space heaters. In this scenario the Supervisory Control and Data Acquisition (SCADA) devices of power distribution are not attacked directly, but instead large changes in power consumption are initiated by the botnet master controlling consumer high-wattage appliances in certain regions to overload or under-load the electricity grid and cause blackouts and potentially cascading failures in power transmission systems.

Kamenski *et al.* [48], [49] proposed a threat model for increasing the resilience of botnets by leveraging blockchain technology in place of traditional centralized C&C servers. This would make bots harder to take over for security teams as they would not be able to impersonate the botmaster. If a public blockchain such as bitcoin were used to store botnet data then the data would become part of the immutable blockchain and be distributed to all nodes. This also makes the C&C structure more resistant to government shutdown.

In February 2021, as this paper was being written, the attack predicted by Kamenski *et al.* has been observed by Saias [50]. The Skidmap cryptocurrency mining botnet, identified in 2019, was seen in 2021 attempting to download malware to Akami's honeypot with a bitcoin wallet address that contained encoded IP addresses for backup C&C servers. Nagy [51] also observed in June 2020 that the Glupteba botnet has also been using the Bitcoin blockchain since 2019 to update C&C servers.

Future IoT device threats must be classified by the technology layer that they attack [52]. Application-level attacks are the most common to date, but vulnerabilities in network stacks are a real threat as evidenced by Karliner [53], who described discovering thirteen vulnerabilities in the FreeRTOS operating system used in embedded devices.

Vulnerabilities in IoT devices may come from unexpected sources, such as attacks on cloud-based service providers or the headline-making work of Sugawara *et al.* [54] who used lasers to remotely control voice assistant software. This demonstrated that vulnerabilities can exist in surprising places such as sensors, network bridges, hardware or software and that security should be a high priority design consideration for device manufacturers.

B. EMERGING DETECTION METHODS

In this section we will examine new and experimental methods of detection and mitigation that fall outside of the host/network-based paradigm. Table 4 summarizes the emerging directions in detection and mitigation of IoT bots. Citations are listed for impact on future research.

Zheng *et al.* described IoTAegis [55], a model security platform that worked on a workstation within a large network to discover and secure devices, both Internet-facing and internal. It used active and passive network scanning to discover IoT devices, connected to, and identified them. It then checked for security vulnerabilities and could be used

TABLE 4. Emerging directions in detection & mitigation.

Year	Paper	Purpose	Unique features	Citations
2018	[55]	Device discovery	Network scanning, remote firmware/password update	3
2020	[56]	Botnet detection	IoT device power usage monitoring	4
2019	[57]	Honeypot	Honeypot as a service	6
2019	[58]	Architecture	Pluggable reusable modular device architecture	3
2020	[59]	Botnet detection	Hybrid network/host system	4
2020	[60]	Trust	Social features, PageRank algorithm	11
2016	[61]	Trust	Hardware-based hashing trust	7
2018	[62]	Trust	Zero-trust, Blockchain	15
2016	[7]	Patching	Chained signatures of firmware updates	47
2016	[63]	Patching	Lightweight mesh distributed updates	24

to change default passwords and update firmware remotely. It was successfully used on a university campus to update passwords and firmware of Hewlett-Packard printers as their test cases. Their scan of 2399 hosts discovered 1701 IoT devices, which were then analyzed. 66% of VoIP phones and 51% of IP printers were discovered to have default or no password, and 59% of printers were found to have out of date firmware.

Jung *et al.* [56] discussed a method for detecting botnet traffic by monitoring power consumption in IoT devices. They attached a power monitor to a simulated IoT device using Raspberry Pi, then measured changes in current when a device was working normally compared to when it was infected with malware. They found that botnets generate a detectable pattern of electricity usage.

Demeter *et al.* [57] described a production honeypot-as-a-service run by Kaspersky Labs. This aimed to record and analyze new malware targeting IoT devices to protect enterprise networks from intrusion attempts. Results from their monitoring show a marked increase in infection attempts from 2018 to 2019, with mostly Mirai-based attacks observed.

Authors in [58] introduced a PLuggable And Reusable (PLAR) architecture for firmware development aimed at giving IoT device manufacturers tools to create more secure devices. They suggested modularizing software components, with middleware that mediates between the components in the device, so modules can be swapped for tested and secure components depending on the manufacturer's needs.

While most traditional computing research separate their detection methods by the same host-based or network-based methods as the IoT literature, there is some early research into combining the two methods. Almutairi *et al.* [59] described an algorithm for host and network analysis to detect botnet activity at early stages of infection before communication with the C&C server. They used a combination of file state from the host being monitored and network traffic to determine anomalies through a common detection engine. This method is impractical in the current generation of IoT devices, however future generations may be able to include self-checking software which could be combined with network-based detection for more transparency of device configuration and software.

1) TRUST

Devices must communicate between themselves and back to controllers such as a service provider or home hub to be able to function. This has led researchers to examine the subject of trust between devices, and how trust can be established that a device has not been compromised.

Xia *et al.* [60] suggested using social features to establish trustworthiness between devices. They explained that a PageRank algorithm can be used to promote distribution of information (whether patches or data) from more trustworthy sources and reduce the impact of untrustworthy devices.

England *et al.* [61] described RIoT or Robust Internet of Things, a system for establishing hardware-based trust using simple hashing cryptography in IoT devices. An immutable bootloader was used to read a device secret during boot, which was never revealed to higher layers of software. Rather, a derived key was generated using a HMAC algorithm which could be used to establish trust with upper-layer software and external devices, such as for attestation of software being run.

Samaniego and Deters [62] suggested using a blockchain middleware to establish trust. They followed a zero-trust model where each device must validate their credentials and configuration each time they participate in a network before they can send a message on the network, ensuring transactions are legitimate. The IoT devices can store their configuration on a blockchain where it is immutable and updated only by consensus with other devices. They outline a two-level hierarchy of mining for identity-trust and transaction-trust.

2) PATCH DELIVERY

An effective method for defending against botnet infection is keeping IoT device firmware up to date, as manufacturers release patches from time to time to plug security bugs and improve functionality [63].

Choi *et al.* [7] proposed an ecosystem for securely updating device firmware. In their system, an IoT device will not run software that has not been properly signed. Signatures are chained, from the manufacturer to a central server on the Internet, then middleware running on a home gateway. Each device in the chain signed the firmware with its private key, and the device used public key cryptography to verify the signature of each step in the chain from the manufacturer to the device and would not run firmware that does not pass all tests. They proved their method mathematically.

Chandra *et al.* [63] proposed a method of pushing firmware updates to very low power or capacity devices via a lightweight mesh over-the-air protocol. They used a gateway device to download the firmware, then a hub to distribute it across the mesh network, with any devices at too great a distance from the hub being able to acquire the updated firmware from their end-device peers in the mesh. The authors did not provide details on use-cases, but this method could be used for diverse applications of wireless IoT devices such as sensor networks, distributed weather monitoring or even micro satellites.

IoT updates are primarily delivered through a client-server architecture. Evidently, this approach is not scalable given the exponential growth in device numbers. Furthermore, the existing mechanisms to ensure integrity of updates are challenging given the IoT devices' limited computing power (e.g., only lightweight cryptographic primitives can be implemented). Puggioni *et al.* [64] proposed CrowdPatching to address the aforementioned challenges in IoT update delivery. CrowdPatching is a blockchain-based decentralized protocol that allows device manufacturers to delegate the delivery of software updates to self-interested distributors in exchange for cryptocurrency. Compared with similar work proposed in [65], CrowdPatching allows the involvement of an unrestricted number of distributors, leveraging recent IoT deployment architectures, and rewards trustworthy distributors in the network.

V. FINDINGS

After reviewing the literature, the authors have formed the following conclusions:

- The vulnerability exploited to create most IoT botnets (around 95%) is use of default credentials. This could be replaced with a per-device unique password generation system to alleviate much of the botnet infection activity.
- Host-based detection is not feasible on the current generation of IoT devices and has limited application.

Artificial intelligence and machine learning models are a promising avenue of research into botnet detection and can be used in mitigation. Researchers contributing in this space, however, do not present side by side comparisons. Their results are often communicated in different ways and with their experimental methods not detailed enough to reproduce their results. This presents a problem when trying to decide which is the most effective or efficient algorithm for detecting botnet activity. Sharing of full experimental setup and methodology, as well as publishing of data sets such as network traffic capture, would help future researchers verify results and build upon the work of others. Authors in [66] recently have made an attempt to provide a comparison given the ongoing inconsistencies in results.

Malware analysis is, by nature, reactive to threats discovered in the wild or on honeypots. If device manufacturers could be convinced of the value of designing with security prioritized then their devices could be much less vulnerable. Provisions need to made for decommissioning IoT devices once they have served their purpose and patch management should be automated or very simple for a typical end-user to perform until the device reaches its end of life.

Over the course of this research we have discovered that while there are many researchers aiming to solve the problems facing IoT devices and detecting botnets in particular, the work is disparate and each researcher uses their own metrics to measure their success. We therefore propose a framework that will allow future researchers to compare and contrast results in an accurate and methodical way.

A. FRAMEWORK FOR FUTURE RESEARCH

We have devised a framework for future research in IoT botnet detection and mitigation. We have noticed that research in IoT botnet detection and mitigation is hardly repeatable and comparable, which has slowed down practical progress in this domain. The main goal we are pursuing with this framework is, therefore, to ensure that research in this critical domain does not suffer from such limitation. Generally, research in IoT botnets can be categorized into the matrix shown in table 5. This framework table can be used to assist researchers to move their research from the early exploration phase to an operational product that can perform detection and mitigation of botnets in IoT devices.

Examples of research papers in the exploration phase include [42], [60], [62], [63] and [64] which are early experiments that explore whether a concept is worth pursuing. Papers that are in the solution phase like [30], [36], [39] and [41] take their research a step further, comparing algorithms against malware to measure effectiveness. Finally, operational phase papers such as [34], [35], [38] and [55] provide more fully-fledged mitigation solutions to the IoT botnet problem, having built on previous research.

Future researchers are encouraged to use a standard set of characteristics for reporting results so that different methodologies can be compared. For machine learning models or other automated detection methods we suggest the following characteristics as a minimum: Number of samples, accuracy %, false positive %, time for training, time per 1000 training samples, time per 1000 test classifications. We also suggest researchers enumerate the hardware that they are running their simulations or experiments on.

B. OPEN QUESTIONS

In this section we list some open questions that we believe could prompt future research in IoT botnet domain:

- How can device manufacturers be brought on board to use standards-based best practice such as IEEE 2413-2019 [67] and ISO/IEC 30141 [68] when designing their devices? Could smart home hubs (e.g., Home Assistant[4]) be developed to include pluggable modules [58] for device reconfiguration on the fly?
- Could the IoTAegis network scanning method be used in conjunction with device fingerprinting such as that

[4]https://www.home-assistant.io

TABLE 5. Framework for future research.

Research Phase	Host	Network	Purpose
Exploration	H		Examine the problem space on local hardware
		N	Examine the problem space remotely
Solution	H		Local detection methods
		N	Remote detection methods
Operation	H		Local mitigation methods
		N	Remote mitigation methods

described by [69] to give an organization a centralized database of connected devices? Could this be combined with the work of Miettinen *et al.* [38] and Hafeez *et al.* [34] or Software Defined Networking layers described in [70] to provide whole network protection for IoT devices through white-listing and patching?

- How will developing 5G technologies and the large IPv6 address space be addressed when IoT devices are manufactured to run off a 5G SIM card with even less interface with the owner? Broadly, how do 5G advancements complicate or facilitate protection against IoT botnet? ([71])
- Whether developing revamped software architectures such as the pluggable and dynamic model presented by Maroof *et al.* [58] should be prioritised for the next generation of IoT devices?
- Whether traditional domain-based detection and filtering of bots can be effectively imported for IoT bot detection and mitigation (e.g., [72], [73])?
- How technological advancements through Fog and Edge computing can be used to develop more efficient IoT botnet detection and mitigation solutions? For instance, authors in [74] propose an edge-oriented detection/mitigation scheme against DDoS in IoT leveraging SDN and Fog capabilities.

Other research gaps identified, which need to be addressed by thorough research, include:

- Using Shamir Secret Sharing to create networks of trust between IoT devices.
- Production practices from industry (e.g., certifications) that can eliminate default credentials shared between devices.
- Decommissioning strategies for devices at the end of their life.

VI. CONCLUSION

Kaspersky's 2020 Security Bulletin [75] notes that Mirai variants continue to dominate the IoT malware space along with Nyadrop, which is used to download further Mirai variants.

Our research has shown that there are two methods for detecting botnets in IoT devices; host-based and network-based. Research can be categorized further into exploration, solution or operation depending on the stage of research and the researchers' goals. We reviewed the most recently emerging threats and solutions and report that there seems to be an agreement among researchers that network-based detection suits the heterogeneous, distributed, and sometimes remote nature of IoT devices. Innovative approaches for detection of IoT botnet such as monitoring power usage, hybrid approaches (i.e., local and remote detection), leveraging other technologies such as Blockchain and Software-Defined Networks seem to be early stage promising efforts that require further exploration. Specifically, we note that the real world efficacy of proposals will be dependent on deployment assumptions that recent efforts seem to be too idealistic about.

Future researchers in IoT botnet domain can plan their work based on the findings reported in this paper including the framework suggested to increase effectiveness and better positioning of their contribution.

REFERENCES

[1] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, and I. Fellow, "DDoS in the IoT," *Computer*, vol. 50, no. 7, pp. 80–84, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7971869/

[2] A. Marzano, D. Alexander, O. Fonseca, E. Fazzion, C. Hoepers,K. Steding-Jessen, M. H. P. C. Chaves, I. Cunha, D. Guedes, and W. Meira, "The evolution of bashlite and mirai IoT botnets," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2018, pp. 813–818.

[3] Spamhaus. (2019). *Botnet Threat Report 2019*. [Online]. Available: https://www.spamhaus.org/news/images/full-2019/spamhaus-botnet-threat-report-2019.pdf

[4] Spamhaus. (2021). *Botnet Threat Report 2021—Q1*. [Online]. Available: https://www.spamhaus.org/news/article/809/spamhaus-botnet-threat-update-q1-2021

[5] S. N. Thanh Vu, M. Stege, P. I. El-Habr, J. Bang, and N. Dragoni, "A survey on botnets: Incentives, evolution, detection and current trends," *Future Internet*, vol. 13, no. 8, p. 198, Jul. 2021.

[6] E. Cozzi, P.-A. Vervier, M. Dell'Amico, Y. Shen, L. Bilge, and D. Balzarotti, "The tangled genealogy of IoT malware," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2020, pp. 1–16.

[7] B.-C. Choi, S.-H. Lee, J.-C. Na, and J.-H. Lee, "Secure firmware validation and update for consumer devices in home networking," *IEEE Trans. Consum. Electron.*, vol. 62, no. 1, pp. 39–44, Feb. 2016.

[8] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[9] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, Nov. 2019.

[10] A. Costin and J. Zaddach, "IoT malware: Comprehensive survey, analysis framework and case studies," in *Proc. BlackHat*, Aug. 2018, pp. 1–9.

[11] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," in *Proc. 23rd USENIX Secur. Symp.*, 2014, pp. 95–110.

[12] M. Rytel, A. Felkner, and M. Janiszewski, "Towards a safer Internet of Things survey of IoT vulnerability data sources," *Sensors*, vol. 20, no. 21, pp. 1–26, 2020.

[13] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, and L. Cheng, "Internet of Things botnet detection approaches: Analysis and recommendations for future research," *Appl. Sci.*, vol. 11, no. 12, p. 5713, Jun. 2021.

[14] M. Antonakakis, T. April, M. Bailey, M. Bernhard, and A. Arbor, "Understanding the mirai botnet," in *Proc. 26th USENIX Secur. Symp.*, 2017, pp. 1093–1110.

[15] J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti, "AVATAR: A framework to support dynamic security analysis of embedded systems' firmwares," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2014, pp. 1–16.

[16] Anonymous. (2012). *Internet Census 2012*. [Online]. Available: http://census2012.sourceforge.net/paper.html
[17] S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, "Measurement and analysis of Hajime, a peer-to-peer IoT botnet," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–15.
[18] Radware. (2017). *BrickerBot Results in Permanent Denial-of-Service*. [Online]. Available: https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service
[19] T. Yeh, D. Chiu, and K. Lu. (2017). *Persirai: New IoT Botnet Targets IP Cameras*. [Online]. Available: https://www.trendmicro.com/en_us/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html
[20] S. Gibson. (2002). *The Strange Tale of the Stemming the Flood With Our ISP*. [Online]. Available: https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/grcdos.pdf
[21] C. Cimpanu. (2019). *A Decade of Malware: Top Botnets of the 2010*. ZDNet. [Online]. Available: https://www.zdnet.com/article/a-decade-of-malware-top-botnets-of-the-2010s/
[22] SophosLabs. (2021). *Sophos 2021 Threat Report*. [Online]. Available: https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
[23] R. Murimi, "Use of Botnets for mining cryptocurrencies," in *Botnets: Architectures, Countermeasures, Challenges*. Boca Raton, FL, USA: CRC Press, 2019, pp. 359–386.
[24] Anonymous. (2014). *Linux Worm Targets Internet-Enabled Home Appliances to Mine Cryptocurrencies*. [Online]. Available: https://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html
[25] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A novel honeypot for revealing current IoT threats," *J. Inf. Process.*, vol. 24, no. 3, pp. 522–533, 2016.
[26] P. Kim. (2017). *Multiple Vulnerabilities Found in Wireless IP Camera (P2P) WIFICAM Cameras and Vulnerabilities in Custom*. [Online]. Available: https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html
[27] P. Nicholson. (2020). *Five Most Famous DDoS Attacks and Then Some*. [Online]. Available: https://www.a10networks.com/blog/5-most-famous-ddos-attacks /
[28] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: Clustering analysis of network traffic for protocol and structure-independent botnet detection," in *Proc. 17th USENIX Secur. Symp.*, San Jose, CA, USA, 2008, pp. 139–154.
[29] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, and K. Sakurai, "Lightweight classification of IoT malware based on image recognition," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jul. 2018, pp. 664–669.
[30] H.-T. Nguyen, Q.-D. Ngo, and V.-H. Le, "IoT botnet detection approach based on PSI graph and DGCNN classifier," in *Proc. IEEE Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, Sep. 2018, pp. 118–122.
[31] M. D. Ernst, "Static and dynamic analysis: Synergy and duality," in *Proc. ICSE Workshop Dyn. Anal.*, 2003, pp. 24–27.
[32] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, "Software-defined network (SDN) data plane security: Issues, solutions, and future directions," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*. Cham, Switzerland: Springer, 2019, pp. 341–387.
[33] Y. Park, N. V. Kengalahalli, and S.-Y. Chang, "Distributed security network functions against botnet attacks in software-defined networks," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw.*, Nov. 2018, pp. 1–7.
[34] I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 45–59, Mar. 2020.
[35] J. Habibi, D. Midi, A. Mudgerikar, and E. Bertino, "Heimdall: Mitigating the internet of insecure things," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 968–978, Aug. 2017.
[36] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the Internet of Things using deep learning approaches," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2018, pp. 1–8.
[37] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici, "N-BaIoT: Network-based detection of IoT BotNet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018.
[38] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "IoT SENTINEL: Automated device-type identification for security enforcement in IoT," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 2177–2184.
[39] S. Nomm and H. Bahsi, "Unsupervised anomaly based botnet detection in IoT networks," in *Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2018, pp. 1048–1053.
[40] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, Jul. 2020.
[41] M. Alauthaman, N. Aslam, L. Zhang, R. Alasem, and M. A. Hossain, "A P2P botnet detection scheme based on decision tree and adaptive multilayer neural networks," *Neural Comput. Appl.*, vol. 29, no. 11, pp. 991–1004, 2018.
[42] A. Guerra-Manzanares, H. Bahsi, and S. Nomm, "Hybrid feature selection models for machine learning based botnet detection in IoT networks," in *Proc. Int. Conf. Cyberworlds (CW)*, Oct. 2019, pp. 324–327.
[43] R. Vinayakumar, P. Poornachandran, and K. P. Soman, *Scalable Framework for Cyber Threat Situational Awareness Based on Domain Name Systems Data Analysis*. Singapore: Springer, 2018, pp. 113–142.
[44] R. Vinayakumar, K. P. Soman, P. Poornachandran, M. Alazab, and A. Jolfaei, *DBD: Deep Learning DGA-Based Botnet Detection*. Cham, Switzerland: Springer, 2019, pp. 127–149.
[45] S. Sriram, R. Vinayakumar, M. Alazab, and S. Kp, "Network flow based IoT botnet attack detection using deep learning," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Jul. 2020, pp. 189–194.
[46] J. Su, D. Vargas, and K. Sakurai, "One pixel attack for fooling deep neural networks," *IEEE Trans. Evol. Comput.*, vol. 23, no. 5, pp. 828–841, Oct. 2019.
[47] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 15–32.
[48] D. Kamenski, A. Shaghaghi, M. Warren, and S. S. Kanhere, "Goraider: Managing cyber-resilient botnets through blockchain," in *Proc. 45th IEEE Conf. Local Comput. Netw. Demos*. Sydney, NSW, Australia, Nov. 2020, pp. 1–4. [Online]. Available: https://www.ieeelcn.org/lcn45demos/1570680086.pdf
[49] D. Kamenski, A. Shaghaghi, M. Warren, and S. S. Kanhere, "Attacking with Bitcoin: Using Bitcoin to build resilient botnet armies," in *Proc. 13th Int. Conf. Comput. Intell. Secur. Inf. Syst. (CISIS)*, Á. Herrero, C. Cambra, D. Urda, J. Sedano, H. Quintián, and E. Corchado, Eds. Cham, Switzerland: Springer, 2021, pp. 3–12.
[50] E. Saias. (2021). *Bitcoins, Blockchains, and Botnets—Akamai Security Intelligence and Threat Research Blog*. [Online]. Available: https://blogs.akamai.com/sitr/2021/02/bitcoins-blockchains-and-botnets.html
[51] L. Nagy. (2020). *Glupteba: Hidden Malware Delivery in Plain Sight*. [Online]. Available: https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final.pdf
[52] H. C. Folts, "Open systems interconnection reference model," in *The Cable and Telecommunications Professionals' Reference: PSTN, IP and Cellular Networks, and Mathematical Techniques*, vol. 1. Butterworth-Heinemann, 2012.
[53] O. Karliner. (2018). *FreeRTOS TCP/IP Stack Vulnerabilities*. [Online]. Available: https://blog.zimperium.com/freertos-tcpip-stack-vulnerabilities-details/
[54] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: Laser-based audio injection attacks on voice-controllable systems," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 2631–2648.
[55] Z. Zheng, A. Webb, A. L. N. Reddy, and R. Bettati, "IoTAegis: A scalable framework to secure the Internet of Things," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–9.
[56] W. Jung, H. Zhao, M. Sun, and G. Zhou, "IoT botnet detection via power consumption modeling," *Smart Health*, vol. 15, Mar. 2020, Art. no. 100103.
[57] D. Demeter, M. Preuss, and Y. Shmelev. (2019). *IoT: A Malware Story*. [Online]. Available: https://securelist.com/iot-a-malware-story/94451/
[58] U. Maroof, A. Shaghaghi, and S. Jha, "PLAR: Towards a pluggable software architecture for securing IoT devices," in *Proc. 2nd Int. ACM Workshop Secur. Privacy Internet Things*, 2019, pp. 50–57.
[59] S. Almutairi, S. Mahfoudh, S. Almutairi, and J. S. Alowibdi, "Hybrid botnet detection based on host and network analysis," *J. Comput. Netw. Commun.*, vol. 2020, pp. 1–16, Jan. 2020.

[60] H. Xia, L. Li, X. Cheng, X. Cheng, and T. Qiu, "Modeling and analysis botnet propagation in social Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7470–7481, Aug. 2020.
[61] P. England, A. Marochko, D. Mattoon, R. Spiger, S. Thom, and D. Wooten, "Riot foundation for trust in the Internet of Things," Microsoft Res., Tech. Rep., Apr. 2016, p. 17. [Online]. Available: https://www.microsoft.com/en-us/research/publication/riot-a-foundation-for-trust-in-the-internet-of-things/
[62] M. Samaniego and R. Deters, "Zero-trust hierarchical management in IoT," in *Proc. IEEE Int. Congr. Internet Things*, Dec. 2018, pp. 88–95.
[63] H. Chandra, E. Anggadjaja, P. S. Wijaya, and E. Gunawan, "Internet of Things: Over-the-air (OTA) firmware update in lightweight mesh network protocol for smart urban development," in *Proc. 22nd Asia–Pacific Conf. Commun. (APCC)*, Aug. 2016, pp. 115–118.
[64] E. Puggioni, A. Shaghaghi, R. Doss, and S. S. Kanhere, "Towards decentralized IoT updates delivery leveraging blockchain and zero-knowledge proofs," in *Proc. IEEE 19th Int. Symp. Netw. Comput. Appl. (NCA)*, Nov. 2020, pp. 1–10.
[65] O. Leiba, Y. Yitzchak, R. Bitton, A. Nadler, and A. Shabtai, "Incentivized delivery network of IoT software updates based on trustless proof-of-distribution," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 29–39.
[66] M. Waqas, K. Kumar, A. A. Laghari, U. Saeed, M. M. Rind, A. A. Shaikh, F. Hussain, A. Rai, and A. Q. Qazi, "Botnet attack detection in Internet of Things devices over cloud environment via machine learning," *Concurrency Comput., Pract. Exper.*, vol. 4, p. e6662, Oct. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.6662
[67] *IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*, Standard 2413-2019, 2019. [Online]. Available: https://standards.ieee.org/standard/2413-2019.html
[68] (2021). *ISO/IEC JTC 1/SC 41 Internet of Things and Digital Twin*. [Online]. Available: https://www.iec.ch/dyn/www/f?p=103:7:0:FSP_ORG_ID:20486
[69] N. Msadek, R. Soua, and T. Engel, "IoT device fingerprinting: Machine learning based encrypted traffic analysis," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8.
[70] A. Lara and B. Ramamurthy, "OpenSec: Policy-based security using software-defined networking," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 1, pp. 30–42, Mar. 2016.
[71] B. Khan. (2021). *DDoS Attacks Intensify—Driven in part by COVID-19 and 5G*. [Online]. Available: https://www.securitymagazine.com/articles/94570-ddos-attacks-intensify-driven-in-part-by-covid-19-and-5g
[72] W. Li, J. Jin, and J.-H. Lee, "Analysis of botnet domain names for iot cybersecurity," *IEEE Access*, vol. 7, pp. 94658–94665, 2019.
[73] C. A. Rivera A, A. Shaghaghi, and S. S. Kanhere, "Towards a distributed defence mechanism against IoT-based bots," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 449–452.
[74] M. Ozcelik, N. Chalabianloo, and G. Gur, "Software-defined edge defense against IoT-based DDoS," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Aug. 2017, pp. 308–313.
[75] Kaspersky. (2020). *Kaspersky Security Bulletin 2020 Statistics*. [Online]. Available: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

BEN STEPHENS (Student Member, IEEE) is currently pursuing the bachelor's degree in cyber security with Deakin University, where he is among the highest achieving students in the course with a GPA of 92/100. He has secured competitive scholarships, including the Deakin Scholarship for Excellence and a research scholarship from the Cyber Security Research and Innovation (CSRI). He has also been sponsored by Deakin University to complete cyber security certifications, including Certified Ethical Hacker (CEH) because of his outstanding university performance. He was involved in malware analysis, botnet takedown, removal, and reporting, as well as distribution of new malware to antivirus companies in the 2000's, when he ran IRC servers on the EFNet and Undernet IRC networks. His research interests include security in consumer and the industrial IoT, malware analysis, and privacy-enhancing technologies. He is currently a member of the Australian Information Security Association and the IoT Security Institute and has contributed as a peer reviewer, and a student member of Deakin's major course review for the bachelor's and master's in cyber security.

ARASH SHAGHAGHI (Member, IEEE) received the B.Sc. degree from Heriot-Watt University, the M.Sc. degree in information security from University College London (UCL), and the Ph.D. degree in computer science and engineering from UNSW Sydney, Australia. He is a Senior Lecturer in cyber security at RMIT University. He is also a Visiting Fellow at the School of Computer Science and Engineering, UNSW Sydney. He has previously been affiliated with Deakin University, UNSW Sydney, Data61 CSIRO, The University of Melbourne, and The University of Texas at Dallas. He is a multi-award winner cyber security educator and researcher with a track record of publications at competitive international conferences and journals. To this date, he has received a total funding of more than 300,000 AUD (as PI and CI combined) for his cyber security research from various internal and external sources, including the Australian Government. There have been several media coverage on his research activities by the Australian Broadcasting Corporation (ABC). He currently serves as an Associate Editor for *Ad Hoc Networks* journal and has had roles (a TPC member, an organizing member, and a reviewer) at prestigious journals and conferences.

ROBIN DOSS (Senior Member, IEEE) is a Professor and the Research Director of the Strategic Centre for Cyber Security Research and Innovation (CSRI), Deakin University. In this role, he provides scientific leadership for this multidisciplinary research center focused on the technical, business, human, policy, and legal aspects of cybersecurity. In addition, he also leads the next generation authentication technologies theme for the Critical Infrastructure Security Research Program of the Cyber Security Cooperative Research Centre (CSCRC). Prior to this role, he was the Deputy Head of the School of Information Technology, Deakin University. His research interests include the broad areas of systems security, protocol design, and security analysis with a focus on smart, cyber-physical, and critical infrastructures. His research program has been funded by the Australian Research Council (ARC), government agencies, such as the Defence Signals Directorate (DSD) and the Department of Industry, Innovation and Science (DIIS), and industry partners. He has contributed to large multi-year projects under the European Union's Framework Program (FP6) and been funded by the Indian Government under the Scheme for Promotion of Academic and Research Collaboration (SPARC). He is a member of the executive council of the IoT Alliance Australia (IoTAA). He has an extensive research publication portfolio and was the recipient of the "Cyber Security Researcher of the Year Award" from the Australian Information Security Association (AISA), in 2019. He is the Founding Chair of the Future Network Systems and Security (FNSS) conference series and is an Associate Editor of the *Cyber-Physical Systems* journal.

SALIL S. KANHERE (Senior Member, IEEE) received the M.S. and Ph.D. degrees from Drexel University, Philadelphia. He is currently a Professor of computer science and engineering with The University of New South Wales (UNSW Sydney), Australia. He also holds affiliations with CSIRO's Data61 and the Cyber Security Cooperative Research Centre (CSCRC). He has coauthored a book titled *Blockchain for Cyberphysical Systems*. His research interests include the Internet of Things, cyber-physical systems, blockchain, pervasive computing, cybersecurity, and applied machine learning. He is a Senior Member of the ACM, a Humboldt Research Fellow, and an ACM Distinguished Speaker. He has served on the organizing committee of several IEEE/ACM international conferences. He serves as the Editor-in-Chief for the *Ad Hoc Networks* journal and as an Associate Editor for the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *Computer Communications*, and *Pervasive and Mobile Computing*.