Article

Detection Mechanisms for Peer-to-Peer Botnets

Mahmood A. Al-Shareeda [1] and Selvakumar Manickam [1,*]

[1] National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
* Correspondence: selva@usm.my; Tel.: +604-653-3004 (S.M.)

Version July 26, 2022 submitted to Entropy

Abstract: Cybercrimes are becoming a bigger menace to both people and corporations. It poses a serious challenge to the modern digital world. According to a press release from 2019 Cisco and Cybersecurity Ventures, Cisco stopped seven trillion threats in 2018, or 20 billion threats every day, on behalf of its clients. According to Cybersecurity Ventures, the global cost of cybercrime will reach $6 trillion annually by 2021, which is significantly more than the annual damage caused by all natural disasters and more profitable than the global trade in all major illegal narcotics put together. Botnets are the most common and have a significant negative impact on any civilization among malware programmes. As a result, this study will explore various P2P botnet detection algorithms by outlining their essential characteristics, advantages and disadvantages, obstacles, and future research.

Keywords: P2P botnet; Cybersecurity; detection mechanism

1. Introduction

The majority of Internet users utilise the Internet to conduct many of their usual daily activities, including routine work, social interactions, and personal leisure. Nearly all Internet users claim that their everyday activities and routines would be altered if they lost access to the Internet [1–8]. Our lives have altered in every way because to the internet and communication technologies. Internet has a lot to offer us in terms of valuable services and applications. However, security risks, often known as cybercrimes that affect people and companies, are one of the biggest downsides of the Internet [9–13]. Malicious software, sometimes known as malware, has thus risen to prominence in today's high-tech society. Malwares are made up of a wide range of programmes, including Trojans, worms, spyware, keyloggers, and botnets. The most pervasive and significant threat to computing assets among the various types of malicious software is posed by botnets. The increasing dependence on the internet over the past few decades has made it difficult to manage the integrity, confidentiality, and security of user data and computing resources [14–19]. This is due to the fact that the majority of cyber-security-related problems are caused by malicious software that is operating undetected on user computers and may jeopardise the security of the user's data, especially in critical infrastructure, government, business, and academic settings[20].

A botnet is a group of compromised computers that the attackers covertly control and utilise for a variety of harmful purposes [21–24]. A bot master, who controls a botnet's command and control for remote process execution, is the attacker. The infiltrated computers or other devices in a botnet are known as zombies or bots [25]. Using a set-up C&C channel, Botmaster has the capacity to remotely control the behaviour of bot malware, making bot operations more adaptable and customising instructions to suit its requirements. The bot master uses the botnet he controls to carry out a variety of malicious activities, including Distributed Denial of Service (DDoS), sending spam emails with viruses attached, phishing, spreading malware, cracking passwords, stealing identities, committing internet fraud, key logging, and extorting online businesses, among others [26–28]. The bot master needs powerful computational power in order to carry out the nefarious acts. Thus, a bot master makes

 doi:10.20944/preprints202207.0415.v1

various social engineering and exploiting attempts to attack weak computers or devices (systems with fewer protection mechanisms) on a network. Once the computers or devices are infected, the legitimate owner or user will not even be aware of it, and without his or her consent, the computers or devices will become a member of their botnets, where the personal data and credentials that are stored there will be stolen or they will engage in other malicious activities as directed by the bot master[9].

This paper focuses solely on discussing numerous P2P botnet topics, including P2P botnet design, C&C communication, P2P detection methods, and observations and difficulties. The following are some of its noteworthy contributions: (I) P2P botnets' life cycle of development is discussed; (II) It presents the taxonomy and thorough analysis of the various detection frameworks and models; and (III) The research observation and difficulties in using these P2P botnet detection methods are discussed.

The reminder of this paper is organized as follows. Section 2 covers the background and related surveys. The various P2P detection techniques are discuss in Section 3. In Section 4, it will presenting the identified research observation and challenges. Finally the Section 5 presents the summary and the directions for future research work.

2. Background and Related Survey

A group of infected computers that are managed by the bot master via command and control (C&C) channels is referred to as a botnet. A botnet usually consists of three different kinds of software. As follows: (I) Server program: To control infected computers or bots, these programmes are placed on the command and control (C&C) server [9], (II) Client program: To control infected computers or bots, these programmes are placed on the command and control (C&C) server [9]; and (III) Malicious program: These applications or programmes fall under the category of malware since they are used to infect or compromise susceptible machines online. Malware like Gnuman and VBS that is managed by a bot master has been found to compromise computers. Trojan.Peacomm, Gnutella, SdDrop, and others [9].

The botnet's communication system is another crucial element. Bots are always in communication with the C&C server, receiving instructions to engage in nefarious activity. The bots then continuously listen for commands, carry out the tasks as directed, and backup the acquired data to the C&C server. They are divided into three groups based on how the botnets communicate: IRC botnets, HTTP botnets, and P2P botnets.

2.1. IRC Botnet

The earliest botnet in existence is the IRC botnet. They are not classified as malicious bots in the design of these bots. In actuality, the majority of bots are useful and necessary for the operation of the Internet. Internet Relay Chat (IRC) protocol chatroom functioning was facilitated by the first internet bots.

There is a moral and legal grey area surrounding the use of commercial internet bots for automated trading, auction bidding, and monitoring of product positioning and reviews [29]. The IRC protocol was first created for extensive data distribution and conversation among end users, as shown in the examples above. The IRC protocol's inherent flexibility and scalability have been used by criminals to carry out a variety of nefarious activities. IRC botnets are regarded as having a centralised C&C architecture. In other words, a single C&C server is in charge of all the bots. (View Figure 1) As a result, it is susceptible to single point of failure due to the centralised architecture. The entire botnet will disintegrate as soon as the server is identified and taken offline [9].

2.2. HTTP botnet

It is comparable to the IRC botnet in this HTTP (Hypertext Transfer Protocol) botnet. The bot masters set up HTTP servers so that they may communicate with the infected computers using the HTTP protocol. The HTTP botnet also falls under the category of centralised C&C architecture, and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 July 2022 doi:10.20944/preprints202207.0415.v1

it can be developed into a hierarchical design with specific subgroups of bots structured for load balancing and for specific content distribution, such as spam [29]. The centralised C&C structure is reliable and simple to put into practise. Bot master has the capacity to tell all bots to react, respond, and attack simultaneously over communication. Due to the fact that the C&C server contained information about the whole botnet, a single point of collapse resulted [30].

2.3. P2P botnet

If the C&C server is discovered, the entire botnet could be destroyed, as is understood with the IRC and HTTP botnets. As centralised botnet mitigation became commonplace, botnets advanced to a decentralised C&C architecture (See Figure 1). Instead of being connected to a central C&C server, the bots with a decentralised architecture are connected to the neighbouring bots in the botnet. Because of this, the decentralised botnet is frequently referred to as a peer-to-peer (P2P) botnet. The P2P architecture eliminates the vulnerability of a single point of disruption because every bot in the P2P botnet can act as either the client or server, but it increases the cost of reaction time [9]. The most recent botnet architecture makes use of social media sites like Twitter and Facebook, therefore the term "botnet" now refers to an automated social media account rather than a hijacked computer or other device.

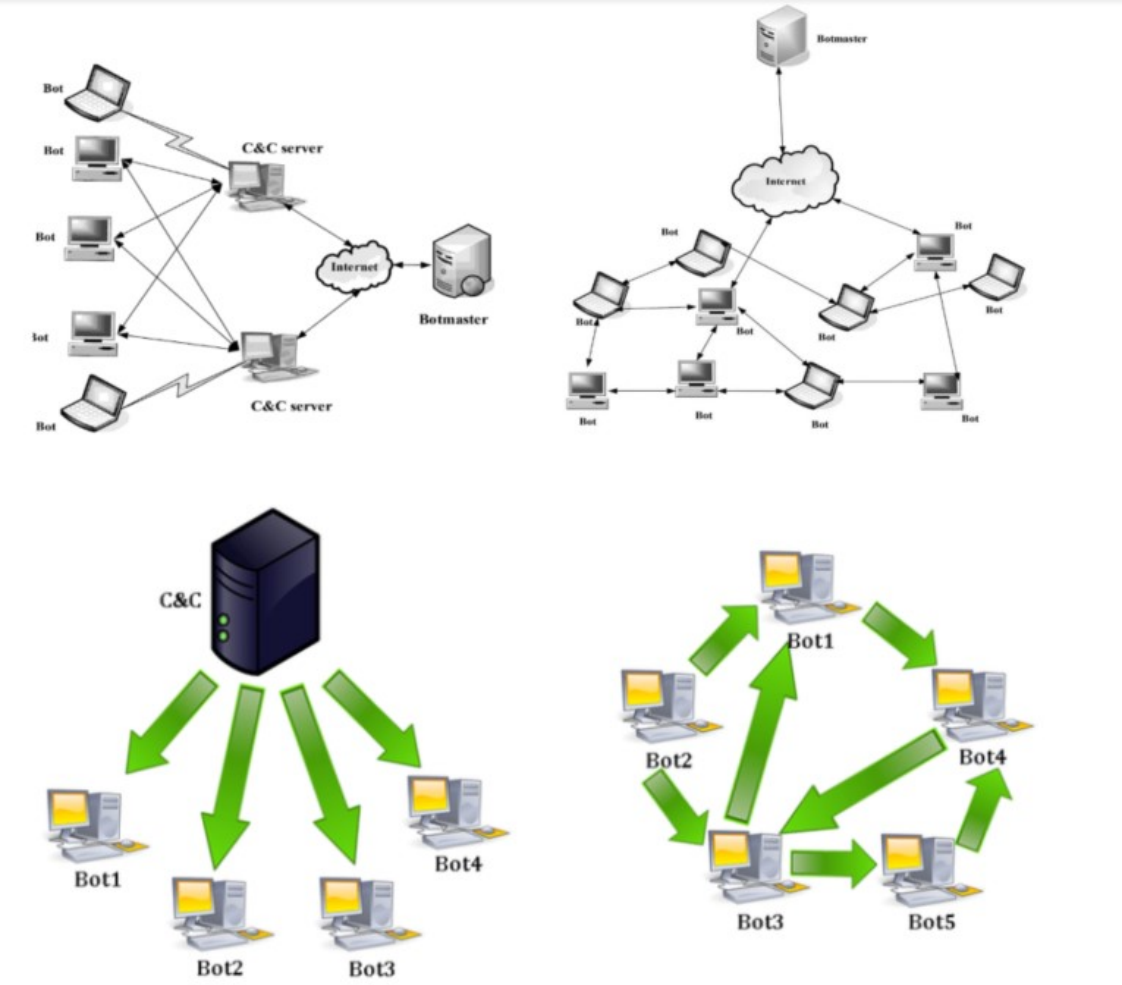

Figure 1. A typical Centralized Botnet VS Peer to Peer Botnet Architecture.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 July 2022 doi:10.20944/preprints202207.0415.v1

2.4. Botnet Development Lifecycle

A product development model is employed to provide a taxonomy and lifecycle for botnets. The product development lifecycle of a botnet has numerous stages, including infection and propagation, communication and control, application and reaction, and update and maintenance. Below is a detailed explanation of each phase [25,29].

- Infection & propagation. The motivation of the bot master is a major factor in whether or not they will construct a botnet. Money, entertainment, ego, and other factors are among the motivations that are described above. It can boost the dissemination by taking advantage of flaws in any of the many malware attack vectors, including websites and browsers, email, and social media platforms [29]. The initial infection of the vulnerable nodes progresses to secondary infection (Zombie conversion), which spreads to the neighbouring nodes.
- Communication & control. At this level, communication between internal and external botnets as well as potential vulnerability nodes is involved. It's crucial to distinguish botnets from other malware types by their communication capability. For connecting freshly infected nodes to the botnet channel, internal communication relies on the C&C architecture, whilst external communication uses the Domain Name Service (DNS) to request the resolution of IP addresses. So that the weak nodes can conceal the identity of the infected node.
- Application & Response. By leasing the botnet's services or selling the code, the botnet can become profitable once the potential motivation level in terms of economic value is met.
- Update & maintenance. Updates and maintenance, such as claiming dormant peer bots, are needed for the infected nodes that joined the active botnet. In order to strengthen the prevention strategy, the executable C&C server may need to migrate, replace the C&C super peers that were removed after being discovered, and update the binaries on all afflicted nodes.

2.4.1. Command and Control Mechanisms

The bots are instructed by distant systems through the command and control (C&C) channels. Based on the C&C protocols, multiple C&C architectures can be categorised, including IRC, HTTP, P2P, Bluetooth, email, social networks, DNS, and other unique protocols. The botnet is based on the demands that either P2P or non-P2P protocols be used for C&C communication. The pull and push mechanisms in botnets are the 2 main C&C activities. When using a pull system, bot masters post instructions at predetermined sites, where peer bots can subscribe and actively accept them. The bot subsequently follows the instructions and also notifies its list of neighbouring peers [25]. To execute the commands, C&C servers push or advance them to their neighbouring peers via the push technique.

3. P2P Botnet Detection Techniques

To categorise the attacks, the common botnet detection methods can be divided into three categories. (1) Botnet traffic, (2) Command and Control (C&C) servers, and (3) PCs with bot infections. Nowadays, a lot of proposed detection schemas are based on one or more of the aforementioned criteria. This study groups the numerous ideas into the following subcategories based on these three characteristics: traffic-based detection, behavior-based detection, DNS-based detection, graph-based detection, data mining-based detection, soft computing-based detection, and general framework. More information on each detection approach will be provided in the next section.

3.1. Traffic-based Detection

The P2P bots interact with a large number of other peer bots to carry out push/pull mechanisms, provide the bots instructions to gather data, or deliver updates from the bot master to infected PCs. Consequently, it continually produces anomalous network traffic [25]. For the objective of observing network patterns and monitoring network traffic in order to identify the presence of botnets, a number of traffic-based detection approaches have been presented. Multi-phased flow model is one of the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 July 2022 doi:10.20944/preprints202207.0415.v1

well-known P2P traffic-based detection techniques. When acting as the sole peer in a P2P botnet, a bot must establish connections with as many neighbour peers as possible in order to build bot networks. As a result, by developing the modelling in a Markov chain framework, the traffic flows are grouped into models based on the states [31].

The researcher also suggested a different method based on the flow dependence of C&C network data to identify P2P botnets. By assuming that typical network traffic has complex short-term network flow dependence, this method distinguishes P2P networks from conventional P2P application network traffic [25]. This method likewise relies on looking into the well-known network flow relationships. This approach may have trouble identifying network flow dependencies if the network flows haven't happened frequently in the past. Additionally, a lot of trace network sample patterns that represent synthetic P2P botnet traffic must be collected for this technique to function fairly. As a result, this technique is not excellent for scaling because it requires a lot of labour to rebuild the modelling[25].

3.2. Behavior-based detection

The behavioural characteristics of the botnet have been thoroughly analysed. Bots typically have a wide range of common features, including structured behaviour, maintaining consequence connections to communicate with and respond to neighbouring bots, as well as receiving commands from the bot master via a C&C server. This method looks at the P2P botnets' behaviour and network characteristics, which are thought to be very closely related to their fundamental architecture and mode of operation. This technique focuses on the network behaviour that is done by the botnet after getting the order from the C&C server will behave unlikely to be human behaviour rather than analysing the network traffic flow as per network-based detection.

The monitoring network must have several infected bots for this strategy to be effective. Additionally, threshold attacks launched by bot masters can avoid the thresholding metrics filtering in the list of behaviour metric attributes.

Table 1. Summary of detection techniques

Detection Techniques	Detection Type	Network and structure bots	Real time Bots	Accuracy
Traffic-based detection	Known	P2P	Yes	Detect P2P bots only in a monitored network
Traffic-based detection	Known	P2P	Yes	Detect P2P bots only in a monitored network
Behavior-based detection	Known	P2P, structured	Yes	Detect P2P bots only in a monitored network
DNS-based detection Both	P2P	Yes	Detect P2P bots only in a monitored network	
Graph-based detection	Both	P2P, Structured	Yes	Detect P2P bots only in a monitored network
Data Mining-based detection	Known and detected any new detection type	P2P	Yes	Detect P2P bots which feature had been identified before
Machine learning-based detection	Both	P2P	Yes	High
Generic Frameworks	Known	P2p	Limited	Low

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 July 2022 doi:10.20944/preprints202207.0415.v1

Table 2. Strengths and limitation of P2P botnet detection techniques

Detection Techniques	Strengths	Limitation and Challenges
Traffic-based detection	* Behavior & Traffic Analysis, Multi-phased flows model * C&C Traffic detection * Flow dependencies, Independent of malicious Traffic * Structure & protocol independent, Pattern based features * Real-time & large scale	* Not detected by using a legitimate P2P network * Higher false positive * Not detected by blended peer bots and randomization * Not detected on traffic tunneling through Tor network * Detect P2P bots only in a monitored network
Behavior-based detection	* Exploit Traffic pattern * Bots group behavior * Host-network cooperation, Independent of topology & protocol * Resilient to encryption & obfuscation * Temporal resource sharing mode * Monitoring resource sharing behavior	* Multiple bots dependency, Vulnerable to threshold attack * Evasion by bots: using benign domains * Used only for parasite P2P botnets * Source should be popular and short life
DNS-based detection	* Group Activity Detector, Online unsupervised known, Unknown * Scalable, Real-time	* Requires multiple bots
Graph-based detection	* Reachability & centrality properties * C&C channels detection, Monitoring bot activities * C&C patterns in overlay topology * Large-scale, Clustering techniques	* Vulnerable to random delay * P2P protocols dependency, False negatives * Bootstrap information required
Data Mining-based detection	* Mining Concept-Drifting Data Stream * Packet features are extracted and aggregated into Flow characteristics * Analysis of traffic features – Fingerprint botnet C&C channels * Created application profile from known P2P applications * Based on high-level statistical traffic features	* Requires monitoring traffic at each host * Sampling may miss useful communications patterns * Evasion by random message padding * Dependency on the dialog-like pattern * Deals with the signaling flows as a whole * Evasion by randomization of inter-packet delays
Soft computing-based detection	* Traffic behavior, Detection in C&C phase * Detection rate 98% * Anomalous Network traffic * Real-time detection in C&C phase & attack phase	* Dependency on features selection * High computational requirement * Sampling can skip botnet flows * Vulnerable to obfuscation
Generic Frameworks	* Anomaly-based-behavior, traffic-based analysis * Independent to protocol and C&C structure, Realtime * Network traffic, Bot behavior, Detect Bots * No prior information required * Remote control process-analysis * Active-informed probing, Fast, Scalable, Real time	* Detect only active bot(s) * Targets enterprise network only * Threshold attack * Content analysis required * False positives advanced encryption * Delayed port binding

3.3. DNS-based Detection

The fundamental characteristic of the bots is a cluster of activity, and they frequently use the domain name system (DNS) to rearrange C&C servers, update their bots' code, and conduct attacks. On rare occasions, the same DNS's bot traffic—which is distinct from that of actual users—dominates the DNS traffic [25]. In terms of security, DNS traffic can be a rich information source. The majority of these DNS-based detection methods enable the identification of infected computers only based on the network traffic created by botnets. Untrustworthy computers can then be examined throughout the botnet lifespan. These methods can identify botnets that have not yet launched an assault and may still be in the formation stage. Unfortunately, as DNS traffic volume grows tremendously, security network administrators and analysts must contend with the difficulty of gathering, retrieving, and analysing DNS traffic in order to respond to contemporary Internet threats. In other words, the majority of DNS research is detrimental to this field. The DNS-based anomaly detection methods are described and assessed in this study [32].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 July 2022 doi:10.20944/preprints202207.0415.v1

This study suggested Botnet Group Activity Detector, an online unsupervised botnet detection method (BoTGAD)[33]. BotGAD is only concerned with DNS flow analysis, with which it attempts to identify coordinated bot activity. A number of sensors have been put in various parts of the network to identify such activity, and bots use the DNS protocol to resolve the address of potential threats' domain names. Additionally, all running bots will deliver results in a synchronous way, which will increase the resemblance between each network session set up for bots to communicate with each other's masters. For example Elastic Zombie [34] and Blackshaded [33] botnets sends control packet to C&C confirming activity at specified time, response time are 30 seconds. and 45 seconds respectively. As a result, synchronous activity can be seen during a variety of botnet operations.

3.4. Graph-based detection

Numerous research use various graph-based features to find network anomalies. The spatial relationships are mostly used by the graph-based features to understand the botnet network activity. The characteristic patterns of the botnets can be discovered through the graphical analysis of the botnet communication interaction. BotGrep is a well-known example of a graph-based detection. The examination of network flows gathered over numerous big networks, such as ISP networks, is how the BotGrep finds P2P botnets.

3.5. Data Mining-based detection

Based on data mining techniques, various research projects have been proposed to identify malicious activities carried out by botnets. These methods are capable of categorising actual unseen threat samples, recognising the threat families of malicious samples, and deducing the feature. In essence, these strategies involve the two steps of feature extraction and categorization.

In this stage, the file samples are classified into appropriate groups or classes based on the examination of feature categories produced by the feature extraction process, using intelligent approaches like classification or clustering [25]. As a result, the primary differences between these data mining-based detection strategies relate to the feature category and the data mining techniques used. Effective threat detection, whether from known or unidentified botnets, heavily depends on the quality of the trained model. Depending on the learned model that is utilised in the system, the classification algorithm can either identify a sequence of unknown input file samples as dangerous or legitimate applications.

3.6. Machine learning-based detection

Based on network traffic, network activity, and a number of additional features for study, there are numerous approaches to identify P2P botnets. Utilizing a botnet architecture with supervised machine learning algorithms is another method. This method uses a framework that extracts conversation-based features via learning from random forests [25].

3.7. Generic Frameworks

Additionally, other general frameworks for detecting botnets have been put out and are based on traffic correlation analysis and behaviour tracking. One common framework for locating the botnet is BotMiner. This method is applicable on a small scale and does not scale well since it relies on network packets and flow analysis, which takes a lot of fine-grained data to study the network [25].

4. Observations and Challenges

Botnet detection methods are compared based on their performance in identifying known and unknown bots, protocol and structure bots, encrypted C&C channel bots, real-time bots, and accuracy. This comparison are summarize into Table 1 and Table 2 below:

5. Conclusion

This research provided a thorough analysis of several facets of P2P botnets. There is no one detection method that can consistently identify evolving botnets because each detection method has its own strengths, weaknesses, and scope. Furthermore, the majority of detection techniques rely on offline analysis, grouping, and classification, and as a result, do not take into account the needs of real-time detection. As a result, the need to build a real-time detection technique for clustering and categorising botnet traffic as well as on-the-fly mining of the botnet traffic is now very important.

1. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sensors Journal* **2020**, *21*, 2422–2433.
2. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Yassin, A.A. Vppcs: Vanet-based privacy-preserving communication scheme. *IEEE Access* **2020**, *8*, 150914–150928.
3. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S.; Hanshi, S.M. Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. *IEEE Access* **2020**, *8*, 144957–144968.
4. Al Shareeda, M.; Khalil, A.; Fahs, W. Realistic heterogeneous genetic-based RSU placement solution for V2I networks. *Int. Arab J. Inf. Technol.* **2019**, *16*, 540–547.
5. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network. *Symmetry* **2020**, *12*, 1687.
6. Al-Shareeda, M.A.; Anbar, M.; Alazzawi, M.A.; Manickam, S.; Al-Hiti, A.S. LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. *IEEE Access* **2020**, *8*, 170507–170518.
7. Hamdi, M.M.; Audah, L.; Rashid, S.A.; Al Shareeda, M. Techniques of Early Incident Detection and Traffic Monitoring Centre in VANETs: A Review. *J. Commun.* **2020**, *15*, 896–904.
8. Al-shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S.; Abdullah, N.; Hamdi, M.M. Review of prevention schemes for replay attack in vehicular ad hoc networks (vanets). 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP). IEEE, 2020, pp. 394–398.
9. Baruah, S. Botnet detection: analysis of various techniques. *International Journal of Computational Intelligence & IoT* **2019**, *2*.
10. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. *International Journal of Engineering and Management Research* **2020**, *10*.
11. Al Shareeda, M.; Khalil, A.; Fahs, W. Towards the optimization of road side unit placement using genetic algorithm. 2018 International Arab Conference on Information Technology (ACIT). IEEE, 2018, pp. 1–5.
12. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Review of prevention schemes for modification attack in vehicular ad hoc networks. *International Journal of Engineering and Management Research* **2020**, *10*.
13. Hamdi, M.M.; Mustafa, A.S.; Mahd, H.F.; Abood, M.S.; Kumar, C.; Al-shareeda, M.A. Performance Analysis of QoS in MANET based on IEEE 802.11 b. 2020 IEEE international conference for innovation in technology (INOCON). IEEE, 2020, pp. 1–5.
14. Alazzawi, M.A.; Al-behadili, H.A.; Srayyih Almalki, M.N.; Challoob, A.L.; Al-shareeda, M.A. ID-PPA: robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network. International Conference on Advances in Cyber Security. Springer, 2020, pp. 80–94.
15. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Khalil, A.; Hasbullah, I.H. Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey. *IEEE Access* **2021**, *9*, 121522–121531.
16. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H.; Abdullah, N.; Hamdi, M.M.; Al-Hiti, A.S. NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs). *Appl. Math* **2020**, *14*, 1–10.

17. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. A Secure Pseudonym-Based Conditional Privacy-Preservation Authentication Scheme in Vehicular Ad Hoc Networks. *Sensors* **2022**, *22*, 1696.
18. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. SE-CPPA: A Secure and Efficient Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. *Sensors* **2021**, *21*, 8206.
19. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Access* **2021**.
20. Khehra, G.; Sofat, S. Botnet Detection Techniques: A Review. 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2018, pp. 1319–1326.
21. Al-shareeda, M.M.A.; Anbar, M.; Alazzawi, M.A.; Manickam, S.; Hasbullah, I.H. Security schemes based conditional privacy-preserving in vehicular ad hoc networks. *Indonesian Journal of Electrical Engineering and Computer Science* **2020**, *21*.
22. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks. *Applied Sciences* **2022**, *12*, 1383.
23. Al-shareeda, M.A.; Alazzawi, M.A.; Anbar, M.; Manickam, S.; Al-Ani, A.K. A Comprehensive Survey on Vehicular Ad Hoc Networks (VANETs). 2021 International Conference on Advanced Computer Applications (ACA). IEEE, 2021, pp. 156–160.
24. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H.; Khalil, A.; Alazzawi, M.A.; Al-Hiti, A.S. Proposed efficient conditional privacy-preserving authentication scheme for v2v and v2i communications based on elliptic curve cryptography in vehicular ad hoc networks. International Conference on Advances in Cyber Security. Springer, 2020, pp. 588–603.
25. Rawat, R.S.; Pilli, E.S.; Joshi, R.C. Survey of peer-to-peer botnets and detection frameworks. *Int. J. Netw. Secur.* **2018**, *20*, 547–557.
26. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks. *Applied Sciences* **2022**, *12*, 5939.
27. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. CM-CPPA: Chaotic Map-Based Conditional Privacy-Preserving Authentication Scheme in 5G-Enabled Vehicular Networks. *Sensors* **2022**, *22*, 5026.
28. Al-Shareeda, M.A.; Manickam, S. Security Methods in Internet of vehicles. *arXiv preprint arXiv:2207.05269* **2022**.
29. Wainwright, P.; Kettani, H. An analysis of botnet models. Proceedings of the 2019 3rd International Conference on Compute and Data Analysis, 2019, pp. 116–121.
30. Zhuang, D.; Chang, J.M. Enhanced peerhunter: Detecting peer-to-peer botnets through network-flow level community behavior analysis. *IEEE Transactions on Information Forensics and Security* **2018**, *14*, 1485–1500.
31. Kwon, J.; Lee, J.; Lee, H.; Perrig, A. PsyBoG: A scalable botnet detection method for large-scale DNS traffic. *Computer Networks* **2016**, *97*, 48–73.
32. Ostap, H.; Antkiewicz, R. A concept of clustering-based method for botnet detection. International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Springer, 2017, pp. 223–234.
33. Chang, W.; Mohaisen, A.; Wang, A.; Chen, S. Measuring botnets in the wild: Some new trends. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015, pp. 645–650.
34. Alonso, S.G.; de la Torre-Díez, I.; Hamrioui, S.; López-Coronado, M.; Barreno, D.C.; Nozaleda, L.M.; Franco, M. Data mining algorithms and techniques in mental health: a systematic review. *Journal of medical systems* **2018**, *42*, 1–15.