NFV-based Scheme for Effective Protection against Bot Attacks in AI-enabled IoT

Vasileios A. Memos and Konstantinos E. Psannis, *Member, IEEE*

***Abstract*—Internet of Things (IoT) is the upcoming network that aspires to interconnect all the "things" each other and to the internet. Many such "things" like smart devices and wireless sensors have already connected to the internet improving human life worldwide. These things can also have Artificial Intelligence (AI), providing many capabilities to their users. However, such IoT-based devices hide risks since they are usually small devices with constrained resources, and hence, they do not have sufficient built-in security mechanisms. In addition, the increase of such devices with a geometric regression worries network administrators who must take countermeasures to restrict and eliminate attackers who aim to turn the IoT into a Botnet of Things (BoT) network, using the compromised devices as bots to unleash Distributed-Denial-of-Service (DDoS) and Man-in-the-Middle (MitM) attacks, or/and spread various types of malware. Thus, they can have unauthorized access and steal very sensitive data from users for malicious purposes. In this article, we highlight the problem caused by the uncontrolled development of insecure IoT-based devices and describe an effective Network Functions Virtualization (NFV) infrastructure in combination with emerging technologies that could provide smart management and enhanced protection against botnet attacks.**

***Index Terms*—Artificial Intelligence, Botnet Attacks, Cloud Computing, Honeynet, IoT, Machine Learning.**

I. Introduction

TODAY, Internet of Things (IoT) is an emerging global network that consists of a lot of devices that have access to the internet and complete specific tasks to satisfy human needs. In the next years, IoT is going to establish IPv6 as the main internet protocol, replacing IPv4. This is because IPv6 provides a variety of methods for dynamically assigning addresses to IoT-based devices, while it supports approximately 340 undecillion (or 340 trillion-trillion-trillion) unique IP addresses. As it is expected, the number of connected devices to the internet will grow to 28.5 billion by 2022 [1], a number that cannot be assigned by IPv4 protocol which supports only about 4.3 billion possible unique IP addresses. This number is constantly increased with geometric progress; hence IPv6 will soon be the successor of IPv4.

Using multiple ways to access the internet, humans enjoy new capabilities in many fields of their daily life, and thus their Quality of Life (QoL) is improved. The same goes for their Quality of Experience (QoE) using many devices that have access to the internet, such as laptops, tablets, smartphones, smart TVs, smart cars, smartwatches, etc. Moreover, the integration of Artificial Intelligence (AI) into these smart devices and things can boost even more the QoE, making the IoT a global AI of Things (AIoT). With the use of AI, interconnected things improve intelligence, enabling new innovative IoT systems and applications for smart cities. Therefore, citizens enjoy new opportunities for easier and more interactive access to e-services of governance, economy, education, business, environment, agriculture, retail, communication, buildings' management, transportation, etc [2].

Every day a large volume of data is produced by multiple IoT-based devices and transferred amongst them, causing concern for the data [3]. Especially in the case of sensitive data, such as financial or health data, the users' privacy must be ensured. Moreover, malicious users, known as "black-hat hackers" or "crackers", look up various methods and ways to intrude into the users' devices by taking advantage of their vulnerabilities, in order to steal their sensitive personal data and use these to their detriment.

In the case of the IoT network, the most common method of intrusion attack is the botnet. A "botnet" or bot network or also known as a "zombie" network is a large network of interconnected compromised devices that run as bots. "Bot" is derived from the known word "robot" since they are designed to perform predefined functions automatically in the same way as the robots. A bot is practically the device or more specifically a malicious program or service which runs on a host computer assisting the botmaster to control all of the host actions remotely. In a regular bot network, the attacker executes multiple commands from a Command-and-Control (C&C) Server to intrude and control the connected IoT devices [4].

Generally, a bot attack is accompanied by a Distributed-Denial-of-Service (DDoS) attack, Man-in-the-Middle (MitM) attack, malicious software (malware) spread, and other threats that target the IoT network utilizing the resources of the compromised connected devices. Thus, an AI-based IoT device as a part of the IoT network which is under a bot attack is vulnerable because such types of attack are very dangerous and resistant, or to spread malware into the large network and then, infect other networks too [4].

Based on the literature, the bot attack is regarded to be the

V. A. Memos is with the Applied Informatics Department, School of Information Sciences, University of Macedonia, Thessaloniki, Greece (e-mail: vmemos@uom.edu.gr).

K. E. Psannis is with the Applied Informatics Department, School of Information Sciences, University of Macedonia, Thessaloniki, Greece (e-mail: kpsannis@uom.edu.gr) (corresponding author).

widest type of network attack globally. With the great evolution of AI-enabled IoT networking, bot attacks have had a high impact in the last years and are spread worldwide with geometric regression. In the next years, the futuristic IoT network will certainly suffer from such attacks, and therefore intelligent and robust security mechanisms should be developed to protect both users' privacy and their devices. Although current security schemes have been proposed for better protection of AIoT, the evolution of technology with geometric progression has made these schemes ineffective due to the weak encryption algorithms and protection mechanisms of most IoT-based devices.

In this article, we propose a Network Functions Virtualization (NFV) infrastructure that makes use of emerging technologies to provide improved protection against various network threats driven by specialized botmasters. Especially for the revolutionary AIoT, such architecture can promise a novel and secure environment against botnets both for the protection and detection of potential malicious traces.

The rest of this article is structured as follows: In Section II, we highlight the problem definition and the necessity for improved security and privacy mechanisms for the IoT; in Section III, we classify and analyze the features of botnet attacks in both traditional and IoT networks; in Section IV, we describe the countermeasures against bot attacks; in Section V, we describe a proposed model for enhanced protection; and finally in Section VII, we conclude the article and give some potential future directions.

II. Problem Definition

Internet of Things (IoT) is a revolutionary technological concept that aspires to connect each device to the internet. The problem is that users globally can use many such devices (sensors, devices, systems, etc.) to access the internet, sometimes without paying attention to their privacy and without paying attention to take some countermeasures to improve the security of their device.

IoT-based devices have embedded firmware that is often vulnerable to intrusion attacks from hackers. Moreover, these devices have usually limited or no built-in security. Therefore, the quick and easy accessibility of these smart "things" can make the infrastructure vulnerable to black-hat hackers. Besides, weak login credentials to the management of these devices, such as "admin", root", "user", and "12345" for a password can easily be cracked by botnets like Mirai, giving unauthorized access to sophisticated attackers who can spy, steal sensitive data, or even use in this way these devices to organize and conduct DoS and DDoS attacks to many other connected devices into the network [6].

Strong encryption algorithms require more resources than those that can be provided by IoT-based devices. Hence, only weak encryption algorithms can be applied in IoT-based devices and wireless sensors, due to their extremely constrained resources (memory, CPU, battery), which means that these devices may attract hackers for various types of attacks converting an Internet of Things (IoT) to a Botnet of Things (BoT) global network. In other words, IoT-based devices are converted to bot devices due to insufficient primitive security or malware infection, e.g. malicious email attachment. Attackers can utilize such IoT-based devices to establish their bot network consisting of multiple devices that can be used for DDoS attacks, MitM attacks, and malware spreading [4].

A DDoS attack occurs when an attacker scans the whole IoT network using the host scanning technique which is a scan for devices with opened SSH and Telnet ports to intrude and inject them with a malicious script. This script is self-replicating since it can detect other - connected to the network - devices, and infect them with the same malicious script. Thus, the attacker can conduct a DDoS attack using these compromised devices as bots and a huge amount of bandwidth [5], causing network instability and operation errors to the victim server.

A MitM attack is another type of attack in which the attacker can interfere within the network and eavesdrop on the exchanged information between two entities [6]. Even worse, the attacker can inject false data into the exchanged information between the two entities. An attacker can also inject the connected devices with various types of malware, such as viruses, worms, trojan horses, etc, spreading them to the whole IoT network [7]. In this way, the attacker can command and control the compromised devices whenever wants.

Apart from the above-mentioned threats of DDoS and MitM attacks, various other threats can come additionally to them. Such threats driven by a botnet operator are spamming, traffic monitoring (sniffing), keylogging, mass identity theft, botnet spread, pay-per-click systems abuse, phishing, Structured Query Language (SQL) injection, zero-day exploit, Domain Name System (DNS) tunneling, etc.

III. Botnet Classification

Botnets can be divided into two main schemes based on the affected network scale and the involved types of computer devices: 1) traditional botnets, and 2) IoT botnets, as shown in Table I. For both schemes, the architecture is similar and generally, botnets can be classified into three categories [8]: a) centralized, b) decentralized, and c) hybrid.

Centralized botnet architecture has one only central Command and Control (C&C) server, where all the compromised devices that operate as bots, are directly connected to this server. The botmaster handles the C&C server to send commands to the connected bots. Centralized botnets are divided into two main categories depending on the protocol they use: the IRC-based botnets, and the HTTP-based botnets [9]. In a centralized architecture, the botmaster attacks the network from one source, which is the C&C server, and hence, it is easier to trace and detect it.

In contrast with the centralized architecture, decentralized botnet architecture uses various bot devices as C&C servers. The botmaster can convert anytime the devices of his/her own into C&C servers for an attack, making very difficult the discovery of the attack source, because the whole botnet is not controlled by a single C&C server. The most common type of

this botnet is the Peer-to-Peer (P2P)-based architecture, where all of the bot devices are connected to each other [9].

TABLE I. BOTNET FEATURES

Botnets	Traditional botnet	IoT botnet
Network scale	Medium scale networks: + LAN + MAN + WAN	Large scale networks: + IoT
Protocol	+ IPv4	+ IPv6
Architecture	Three (3) main: + Centralized + Decentralized + Hybrid	Three (3) main: + Centralized + Decentralized + Hybrid
Life cycle	Four (4) phases: + Injection + C&C Server(s) use + Attack + Post-attack	Four (4) phases: + Injection + C&C Server(s) use + Attack + Post-attack
Devices used	Desktop & Laptops: + PCs + Servers	Any "thing": + Smartphones + Smartwatches + IP web-cameras + Smart cars + Sensors + etc.
Infection	Medium	Easy
Detection mechanism	Medium	More difficult
Devices as bots	Many	Very many
Spread speed	Fast	Very fast
Impact	Medium	Huge

Finally, hybrid botnet architecture uses both centralized and decentralized architecture to benefit from both of them. A hybrid botnet makes use of an encryption key to hide the malicious traffic within the regular traffic, making it difficult to detect them. This type of botnet architecture uses random vulnerable ports to send encrypted messages from any bot device in the network.

IoT botnet has a similar lifecycle to the traditional botnet. In both cases, a botnet life consists of four (4) cycles which include initial injection, C&C use, attack, and post-attack, as depicted in Fig. 1. The first cycle refers to finding vulnerabilities and gaps in the devices for the initial injection with a malicious script; the second cycle includes the involvement of one or more C&C servers by an attacker to spread the malicious script across multiple interconnected devices; in the third cycle the attacker launches distributed attacks using the infected set of devices; the last fourth cycle refers to the peak of the attack or also known as a post-attack cycle, in which the attacker hides the traces and leads the malicious script to other network targets so that a new cycle of bot attacks can begin.

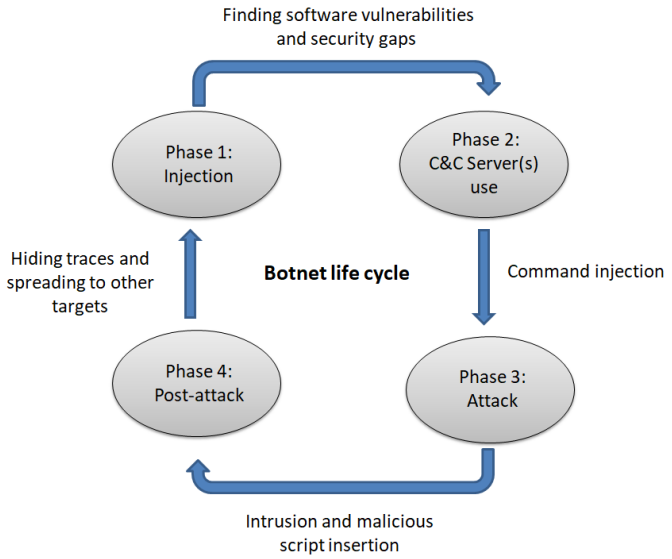

Figure 1. The four phases of a botnet life cycle.

As shown in Table I, the features of traditional and IoT botnets differ in some cases. The main difference between traditional and IoT botnets is their application and impact. Traditional botnets affect LANs, MANs, and WANs, while IoT botnets affect a wider network scale composed of very many IoT-based devices. Thus, IoT botnets have much more impact than traditional botnets, and as a consequence, due to the faster spread of IoT botnets too, the detection of them is more difficult than the traditional botnets. It is remarkable that infection is also easier in the IoT networks compared to traditional networks due to weak encryption algorithms and security mechanisms supported by IoT-based devices. Another important feature is that the detection of IoT botnets is more difficult compared to traditional botnets.

IV. Countermeasures Against Botnets

A. *Protection and Detection Methods*

There are many methods for the detection of botnets. Some of them detect specific botnet existence, whereas other methods can detect new botnets using heuristic analysis. A series of advanced tools can be used in an IoT network for an improved detection rate of botnets. These tools are based mainly on anomalies discovery or network rules violation. Such tools are NIDES/STAT, Haystack, Ossec System, Tripwire, Nessus, etc.

Other well-promising practices include the use of network tools like Network-based Intrusion Detection Systems (NIDS) and Network-based Intrusion Prevention Systems (IPS), the use of Transport Layer Security (TLS)/Secure Sockets Layer (SSL) protocol for secure communication between IoT devices and server, and the firmware update of the IoT devices for covering potential vulnerabilities which can be used as exploits for hackers to intrude to them [10].

Moreover, several data mining techniques can be used to catch bot attacks effectively with an improved detection rate. Such methods include Machine Learning (ML) algorithms,

such as Logistic Regression (LR), Naive Bayes (NB), Support Vector Machines (SVM), Random Forest (RF), Fully-Connected Neural Network (FCNN), etc.; data classification algorithms, such as Naive Bayes Classifier, Ibk classifier, Rule Decision Table, Trees, J48 classifier, etc.; and clustering like k-means [11].

Several cutting-edge technologies can be integrated to provide a better level of security to IoT-based devices and the whole IoT network. Moreover, various advanced protection practices can be applied by network administrators to detect and eliminate bot attacks, enhancing the protection of the IoT.

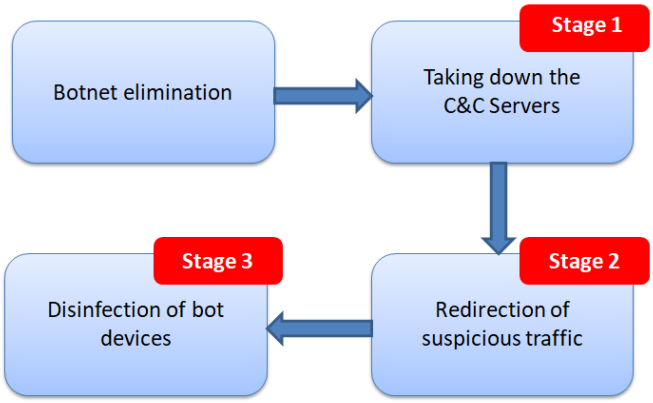

Figure 2. The disinfection stages for botnet elimination.

B. *Disinfection Stages*

To tackle a botnet, it is necessary to apply some specific offensive practices that can be categorized into three stages, as shown in Fig. 2. These stages for effective disinfection from a botnet attack are the following [12]:

1) Stage 1: Taking down the C&C server(s)

The destruction of the root of a bot attack leads to the elimination of the whole botnet. Hence, taking down the C&C server during a DoS attack or all of the C&C servers during DDoS attacks can be an effective method for a network administrator to protect the IoT network.

2) Stage 2: Redirection of suspicious traffic

Redirection of suspicious network traffic is another practice to prevent IoT devices from attacks by hackers. This procedure is also named “sinkholing” since suspicious traffic can be redirected to specific servers known as “sinkhole servers” or simply “sinkholes”. Thus, in the case of suspicious traffic which belongs to a bot attack, this procedure may stop its operation. Besides this, sinkhole servers can record suspicious network traffic to analyze it and determine if it is malicious or not. Sinkholes are regarded to be a good weapon at the hands of network administrators.

3) Stage 3: Disinfection of bot devices

Another robust and powerful practice is the use of strong firewalls, restricted rules and security policies, and up-to-date antivirus software. However, that is not feasible for many IoT devices that have only a few resources, and hence are not able to possess enough computing power to run security applications. Such IoT devices are smart TVs, IP cameras, Wi-Fi sensors, etc. Therefore, in such cases, we should concentrate on the network level using techniques like deep packet inspection (network traffic monitoring and filtering), intrusion prevention (recognizing potential types of attack), and behavior and anomaly detection methods (unusual and suspicious connection requests).

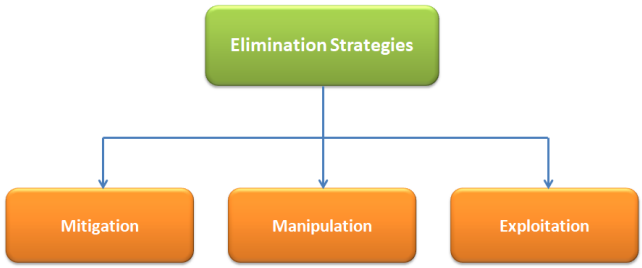

Figure 3. The elimination strategies against botnet attacks.

C. *Elimination Strategies*

Botnet elimination strategies can be divided into three categories as it is shown in Fig. 3. These strategies are the following [12]:

1) Mitigation

Mitigation is an elimination strategy against botnets that practically slows them down by consuming resources for instance. There are several mitigation techniques that offer this result, such as temporary DoS attempts against the malicious C&C servers, trapping and holding connections from infected devices, and blocking malicious domains.

2) Manipulation

Manipulation is referred to as the command layer. The objective of this strategy is to manipulate and inject commands based on the used protocols in the botnet. For example, alteration or removal of DDoS or spam commands can provide a universal cleanup of infected IoT-based devices in the entire network. Less invasive options include discarding collected personal data, such as credit cards or bank details, replacing them with fake information, or issuing orders to get bots to stop collecting. In addition, the use of encryption methods such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) may completely deny control of botnet data exchange.

3) Exploitation

Exploitation is a particular technique that uses errors found in bots. Such errors can be used to accomplish offensive actions on infected machines. Although this method is the strongest, it may hide dangers since exploits can easily crash or damage operating systems if not carefully applied.

V. A Proposed Approach

Emerging technologies of the last years can improve the protection of an AI-based IoT network. Although such technologies are used in some network administrative tools for secure traditional networks, new ways of use and integration of them can provide better effectiveness in the case of IoT networks. In this section, we provide a thorough description of

three effective technologies and highlight their advantages. Then, we propose a potential NFV architecture that integrates these technologies in such a way that could improve the detection of botnets, and hence the protection of AIoT against bot attacks.

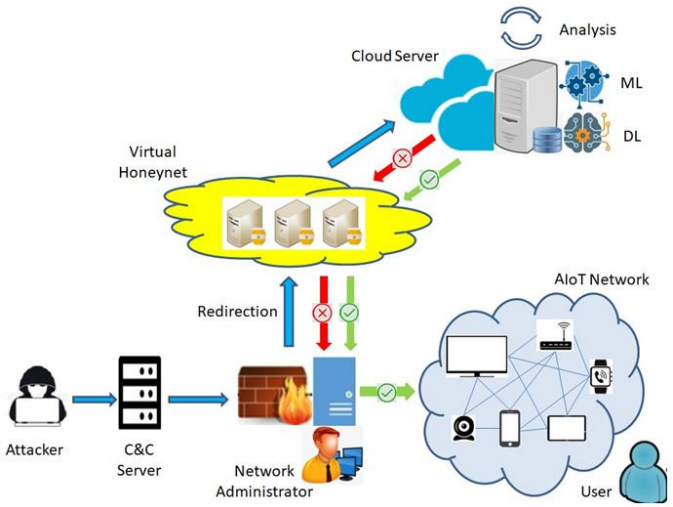

Figure 4. The proposed system architecture

A. *Involved Technologies*

Three emerging technologies can be involved in our scheme to enhance the protection of AIoT against bot attacks. These technologies are the following:

1) Virtual Honeynet (VHN)

Network Virtualization (NV) is a key technology to deal with security threats more effectively, as it allows administrators to create and control multiple zones within the network. Hence, they can apply different Virtual Network Functions (VNFs) for each zone. A honeynet is a network that consists of many honeypots. A honeypot is usually a virtual machine, which waits for attacks from C&C servers. Each honeypot acts as a trap for attackers [13].

Honeypots can deceive even the most specialized hackers who fall into these traps, because honeypots are within the real asset which is the attackers' target, and they are not separate machines, devices, or software. Honeypots are used to record these attacks and give the administrator a comprehensive image of the source and the attack methods. In this way, honeypots can provide continuous knowledge to the network administrator and can learn and stop even the stealthiest attacks.

In other words, the VHN infrastructure in our scheme can operate as a sandbox that is a security mechanism for the execution of potential unsafe actions, separating and protecting the real system from infection. Therefore, the honeypots in the VHN can be useful tools for network administrators to protect the whole AIoT infrastructure from such malicious activities and export important information and conclusions.

2) Cloud Computing (CC)

CC is a novel architecture that is designed to provide resources and services stored somewhere on the Internet, that is into cloud servers or commonly in the "clouds", to its users from anywhere and any device which has access to the Internet. CC offers a well-established and secure data allocation system, unlocking various capabilities for IoT users [14].

CC can provide many advantages to various scientific fields. In the field of Privacy and Security, CC can offer many benefits, but only if the cloud infrastructure is secure enough. This means that especially in the case of an AIoT network, administrators must be very careful when they design and evaluate the effectiveness of the infrastructure. As a consequence, the stored data into a Cloud Server (CS) must be secure to provide the users the feeling of security without concerns about their privacy. It should be noted that cloud resources can be managed and secured centrally by the network administrator for improved effectiveness.

Furthermore, CC is used by many security applications due to its proactive protection and detection capabilities. CC reduces the latency between the time a security exploit is discovered and when the corresponding protection is available for the users. File scanning for malware and virus signatures updates can be occurred in real-time and automatically. Besides, CC constitutes a very good method for devices with limited resources like IoT-based devices. These are the reasons that establish CC as a very effective technology in our proposed scheme for botnet detection and malware disinfection of the devices that operate as bots.

3) Artificial Intelligence (AI)

AI is the recreation of human brainpower performed by machines, specifically by a computer. In other words, AI is simply the integration of human intelligence into machines. Such a machine operates with intelligent behavior according to specific rules which are defined by an appropriate algorithm to solve various problems. This is the reason why this technology is called artificial intelligence. Thanks to AI, a machine has the ability to move and manipulate different objects, understand if someone raises his/her hands, and solve various complex problems.

New techniques like Machine Learning (ML) and Deep Learning (DL) have been integrated into AI during the last years for the optimized behavior of the machines. ML is a subfield of AI in computer science. An ML algorithm defines any computational method in which the output from previous events or decisions is used to improve predictions or decisions. DL is a method in which feature levels are not designed by humans to be learned from data using a general learning process. DL has an important impact on troubleshooting complex issues while strengthening the security of IoT [15].

In our proposed scheme, the combination of ML and DL – as subsets of AI – can be very useful to analyze cyber threats on the CS, achieving optimized bot detection results, and hence protecting the IoT network that is always a potential target for cyber attacks.

B. System Architecture

A proposed approach could be the integration of the above emerging technologies into robust system architecture to provide a better protection level in terms of proactive detection of botnets. The proposed scheme benefits from each technology, and thus it could provide maximum efficiency.

Fig. 4 depicts the proposed system architecture for valid and timely bot attack detection, and hence the protection of the AI-enabled IoT devices and generally, the whole AIoT network. As it is shown, each suspicious connection attempt launched by a potential attacker through the C&C Server is redirected to a VHN composed of many honeypots that operate as decoys. The connection data of each suspicious attempt are sent to a powerful CS in which a thorough behavior analysis takes place using AI, such as ML and DL methods to provide more accurate results.

In particular, the connection data include the input data of external suspicious connections, and the analysis takes place in the CS using ML algorithms in combination with probabilistic methods and DL techniques by other relevant malicious connections and infections to estimate the possibility of a botnet attack [4]. After this analysis, the CS can record the essential information of the potential attacks (source IP, suspicious actions, etc.), and return to the honeypot the decision about this connection (if it is malicious or benign). An AI-powered honeypot provides many benefits to network administrators. This is because AI methods cause honeypots to be less complicated, operate more quickly, and produce comprehensive notifications about the threats.

In our proposed model, AI in the honeynet is powered from the CS that is on 2-way communication with the honeypots of the VHN. If the connection request is identified as a variant of a known bot attack or estimated as a new unknown bot attack, the request to the real AIoT network is blocked and the attacker is trapped into the honeynet for the recording of their movements. There is continuous feedback between the honeynet and the CS since all of the actions inside the honeynet are recorded and sent to the CS for recognizing future relevant attacks, thanks to DL. Otherwise, for a benign connection attempt, the request is allowed and the user acquires privileges to access the real AIoT network and its resources that are the interconnected devices.

The above procedure can achieve three goals. Firstly, it can redirect the potential attack to a secure and safe virtual layer that is a honeypot or a group of honeypots that operate as sandboxes, protecting the real AIoT network from infection. Secondly, after a thorough analysis of the attack features in the CS using data mining techniques like ML and DL, the potential attack can be recognized if it is known or estimated if it is unknown, and can successfully be blocked in both cases.

Finally, in the case of positive detection of bot attack existence, the network administrator can have a comprehensive report about the source of the attack, the type, the malicious actions it does, and other meaningful information that can take into consideration to strengthen his/her network defense against future relevant attacks. It should be noted that the network administrator in an AIoT can be in constant interaction with the VHN having a thorough mapping of the network status. In this way, the administrator can set security zones, put restrictions, and take important decisions more easily.

VI. Conclusion

In this article, we highlight the problems of security and privacy in AIoT. Since the evolution of technology tends to establish IoT as a new global network of billion interconnected AI-based devices, security and privacy mechanisms and tools should be improved to provide better protection against bot attacks both in each device and in the whole network. Thus, we propose an AI-enabled NFV infrastructure for AIoT that could provide better network management and effective protection against botnet attacks. Future work may include the implementation of the proposed infrastructure using the components of Fig. 4. After the building of this model, it could be tested and evaluated against real-world known and zero-day botnet attacks using various malware samples collected into our security lab.

References

[1] A. Moubayed, T. Ahmed, A. Haque, and A. Shami, “Machine Learning Towards Enabling Spectrum-as-a-Service Dynamic Sharing”, 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2020, pp. 1-6, doi: 10.1109/CCECE47787.2020.9255817.

[2] M. Talebkhah, A. Sali, M. Marjani, M. Gordan, S. J. Hashim, and F. Z. Rokhani, “IoT and Big Data Applications in Smart Cities: Recent Advances, Challenges, and Critical Issues”, in IEEE Access, vol. 9, pp. 55465-55484, 2021, doi: 10.1109/ACCESS.2021.3070905.

[3] J. Granat, J. M. Batalla, C. X. Mavromoustakis, and G. Mastorakis, “Big Data Analytics for Event Detection in the IoT-Multicriteria Approach”, in IEEE Internet of Things Journal, Vol. 7, No. 5, pp. 4418-4430, May 2020, doi: 10.1109/JIOT.2019.2957320.

[4] V. Memos and K. Psannis, “AI-powered Honeypots for Enhanced IoT Botnet Detection”, 3rd World Symposium on Communication Engineering (WSCE 2020), University of Macedonia (Greece), October 09-11, 2020, doi: 10.1109/WSCE51339.2020.9275581.

[5] T. Shah and S. Venkatesan, “A Method to Secure IoT Devices Against Botnet Attacks”, in Internet of Things – ICIOT 2019, Lecture Notes in Computer Science, Vol. 11519, Springer, Cham, 2019, doi: 10.1007/978-3-030-23357-0_3.

[6] G. Liu, W. Quan, N. Cheng, D. Gao, N. Lu, H. Zhang, and X. Shen, “Softwarized IoT Network Immunity Against Eavesdropping With Programmable Data Planes”, in IEEE Internet of Things Journal, Vol. 8, No. 8, pp. 6578-6590, April, 2021, doi: 10.1109/JIOT.2020.3048842.

[7] L. Caviglione, M. Choraś, I. Corona, A. Janicki, W. Mazurczyk, M. Pawlicki, and K. Wasielewska, “Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection”, in IEEE Access, vol. 9, pp. 5371-5396, 2021, doi: 10.1109/ACCESS.2020.3048319.

[8] S. Haq and Y. Singh, “Botnet Detection using Machine Learning”, 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018, pp. 240-245, doi: 10.1109/PDGC.2018.8745912.

[9] R. U. Khan, R. Kumar, M. Alazab, and X. Zhang, “A Hybrid Technique To Detect Botnets, Based on P2P Traffic Similarity”, 2019 Cybersecurity and Cyberforensics Conference (CCC), 2019, pp. 136-142, doi: 10.1109/CCC.2019.00008.

[10] M. Gajewski, J. M. Batalla, A. Levi, C. Togay, C. X. Mavromoustakis, and G. Mastorakis, “Two-tier anomaly detection based on traffic profiling of the home automation system”, Computer Networks, Vol. 158, pp. 46-60, July 2019, doi: 10.1016/j.comnet.2019.04.013.

[11] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, “Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments”, Future Generation Computer Systems, Vol. 125, pp. 156-167, 2021, doi: 10.1016/j.future.2021.06.047.

[12] F. Leder, T. Werner, and P. Martini, “Proactive Botnet Countermeasures – An Offensive Approach”, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2009.
[13] I. M. M. Matin and B. Rahardjo, “The Use of Honeypot in Machine Learning Based on Malware Detection: A Review”, 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, pp. 1-6, October 2020, doi: 10.1109/CITSM50537.2020.9268794.
[14] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, “IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network”, IEEE Internet of Things Journal, Vol. 8, No. 7, pp. 5164-5171, April, 2021, doi: 10.1109/JIOT.2020.3033131.
[15] Y. Li, Y. Zuo, H. Song, and Z. Lv, “Deep Learning in Security of Internet of Things”, in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3106898.