




Botnet Attack Detection with Incremental Online Learning

Mert Nakip¹(✉)  and Erol Gelenbe^{1,2,3,4} 

¹ Institute of Theoretical and Applied Informatics, Polish Academy of Sciences,
44-100 Gliwice, Poland

{mnakip,seg}@iitis.pl

² Yaşar University, Bornova/İzmir, Turkey

³ Lab. I3S Université, Côte d'Azur, 06200 Nice, France

⁴ Lab. A. De Moivre CNRS, London, UK

Abstract. In recent years, IoT devices have often been the target of Mirai Botnet attacks. This paper develops an intrusion detection method based on Auto-Associated Dense Random Neural Network with incremental online learning, targeting the detection of Mirai Botnet attacks. The proposed method is trained only on benign IoT traffic while the IoT network is online; therefore, it does not require any data collection on benign or attack traffic. Experimental results on a publicly available dataset have shown that the performance of this method is considerably high and very close to that of the same neural network model with offline training. In addition, both the training and execution times of the proposed method are highly acceptable for real-time attack detection.

Keywords: Internet of Things (IoT) · Botnet attacks · Mirai · Incremental learning · Auto associative neural networks · Dense random neural networks

1 Introduction

Since IoT devices in the Massive IoT segment are low-cost devices, they can often perform a single task at a time and their computational power is not sufficient to execute complex attack detection algorithms. Therefore, Massive IoT is vulnerable to network attacks. According to a study by HP [1], 70% of IoT devices are vulnerable to attacks, while one of the most common attacks is the Denial of Service (DoS) attack which comprises 20% of all attacks against the IoT [6].

Network attacks can include worms based on propagating software [37, 38], DoS attacks where an attacker or an infected device aims to prevent the normal functioning of a device (or a system) by forwarding superfluous requests [10, 11], and Botnets which are the subject of this work. Traffic which may cause attacks can be detected as a form of anomaly [22, 26] which is concealed as part of normal innocuous traffic.

© The Author(s) 2022

E. Gelenbe et al. (Eds.): EuroCybersec 2021, CCIS 1596, pp. 51–60, 2022.

https://doi.org/10.1007/978-3-031-09357-9_5

When a network attack occurs following the same techniques as DoS attacks, but affecting more devices it is called a Distributed DoS (DDoS) attack [14]. One of the most popular kinds of DDoS attacks is the Botnet attack which mainly targets IoT devices. In a Botnet attack, a victim device turns into a bot via malware and generates traffic that floods other servers and devices with meaningless requests that lead to threats [21].

Detecting Botnet attacks is an important task considering the high threat level for a massive number of devices. To this end, a recent trend of research has focused on developing Machine Learning (ML) based techniques. Most of earlier work [5, 13, 24, 28–30, 34–36, 39, 40, 42] in this trend develops techniques for classification by supervised learning; however, these techniques require large numbers of samples for both normal traffic and malicious traffic; collecting data for realistic malicious traffic is no easy task. Only a few works evaluated the lack of attack data during the training of ML models (via auto-associative learning) for Botnet attacks [33, 43] and for DoS attacks [15].

In 2016, a massive DDoS, Botnet, attack affected many web sites including Netflix, Reddit, Spotify, and Twitter through the Dyn service for domain name system (DNS) management [7, 23] as well as numerous IP addresses creating access through the servers of some cyber-security companies [41]. It is known that the botnets in this DDoS attack were infected by the Mirai malware, in which the infected devices generate traffic that overwhelms servers and other devices with nonsense requests, sometimes leading to threats [21]. Reference [4] has analyzed the characteristics of this class of attacks, while a recent work [27] has analyzed the characteristics of IoT traffic generated by Botnet. In addition, Reference [3] used blockchains to protect IoT networks against Mirai Botnet attacks.

1.1 Attack Detection with the Random Neural Network (RNN)

The RNN [17] with gradient descent learning [18] has been used to detect Denial of Service attacks in early work [34] and was recently used also to detect SYN attacks [15].

The Dense RNN was introduced in [16, 20] to address various pattern recognition problems, including character and object recognition. It has been previously used with auto-associative offline training to detect SYN attacks [8], and was used more recently also to detect Mirai Botnet attacks [33].

In this paper, we use a Dense Random Neural Network (Dense RNN) [16, 20] based Mirai Botnet attack detection method, but extend it specifically for incremental online learning. Similar to [8], this method learns the statistics of the IoT traffic under normal circumstances while the network is online (via auto-associative and incremental online learning); that is, it does not require the offline collection of any IoT traffic data (either benign or attack) for the learning procedure.

In the rest of this paper, Sect. 2 presents the methodology of the proposed method for Mirai Botnet attack detection while Sect. 4 presents the performance

evaluation of this method on a publicly available dataset. Lastly, Sect. 6 summarizes the paper.

2 Auto-Associative Dense RNN Based Botnet Attack Detection with Online Incremental Training

We now present the methodology of our Botnet Attack Detector (AD) based on Dense Random Neural Networks (Dense RNN) which is trained entirely online with only benign IoT traffic. Figure 1 displays the architectural design of this detector, which consists of three main stages:

1. Extracting metrics from IoT traffic with the “Metric Extractor” module,
2. Detection of potential attack packets with “Auto-Associative Dense RNN” and “Attack Decision Maker” modules and
3. Incremental online training of AA-Dense RNN with “Incremental Semi-Supervised Learning Algorithm”. In the rest of this section, we shall detail the methodologies of these stages.

3 Extracting Metrics from IoT Traffic

Considering that the Mirai botnet attacks aim to spread through the devices in the IoT network, a recent work [33] has proposed three metrics calculated using only the transmission times and lengths of packets. Since the correlation analysis presented in [33] has shown that these three metrics successfully captures the traces of Mirai botnet attack packets, this paper also uses these metrics, which are defined as follows:

- **Metric 1:** The total size of the last N transmitted packets,
- **Metric 2:** The average inter-transmission times of the last N packets,
- **Metric 3:** Total number of packets that are transmitted in last T seconds.

Furthermore, it has also been shown that an attack detector achieves its best performance using these metrics with importance coefficients. However, in order to design an attack detector with purely online training on only normal unlabeled traffic, we will treat these metrics equally, i.e. take each of their importance coefficients as $1/3$.

The Dense-RNN model, which allows direct connectivity between neuron cells (addition to the usual axon-dendrite interactions), has been proposed in [16, 20]. It is a specific form of the Random Neural Network (RNN) [12, 17] that uses clusters of RNN cells for deep learning.

Earlier research have shown the success of the conventional RNN model [19] in IoT systems for applications on the video quality evaluation [32], network design [9], and home climate control [25]. In the Dense RNN model, firing at any cell may trigger a direct firing at a neighboring cell as well as excite or inhibit any other cell in the neural network through corresponding weights. In addition, probability p that any other cell in the network fires when a given cell fires, represents the direct interaction between neuron cells.

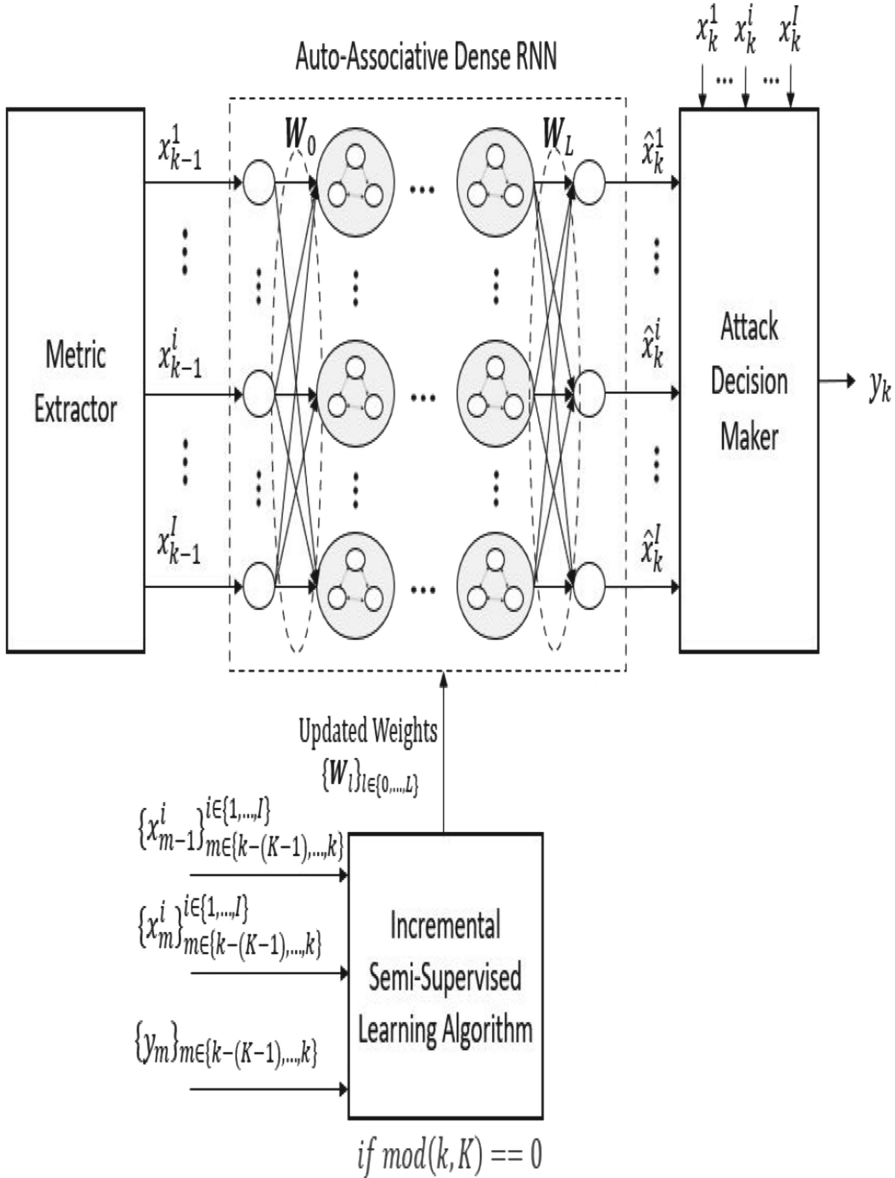


Fig. 1. The architectural design of AA-Dense RNN based Botnet attack detector with incremental online training

4 Experimental Results

In order to evaluate the performance of our AA-Dense RNN based Botnet attack detector with incremental online learning, we use publicly-available Kitsune

dataset [2,31] which contains 764,137 normal and malicious packets for Mirai Botnet attack. During the performance evaluation, we compare the performance of AA-Dense RNN under online training with that under offline training.

For AA-Dense RNN, we first set the number of neurons in each layer l as $n_l = I = 3$, and $p = 0.05$, $r = 0.001$ and $\lambda^+ = \lambda^- = 0.1$. We also set $N = 500$ packets and $T = 100$ secs for the extraction of metrics, and we set $\Theta = 0.02$ for Attack Decision Maker module.

First, we evaluate the performance of the proposed AD method for varying number of training packets K between 100 and 1000. In this way, we shall also select the best value of K and set it for the rest of this section.

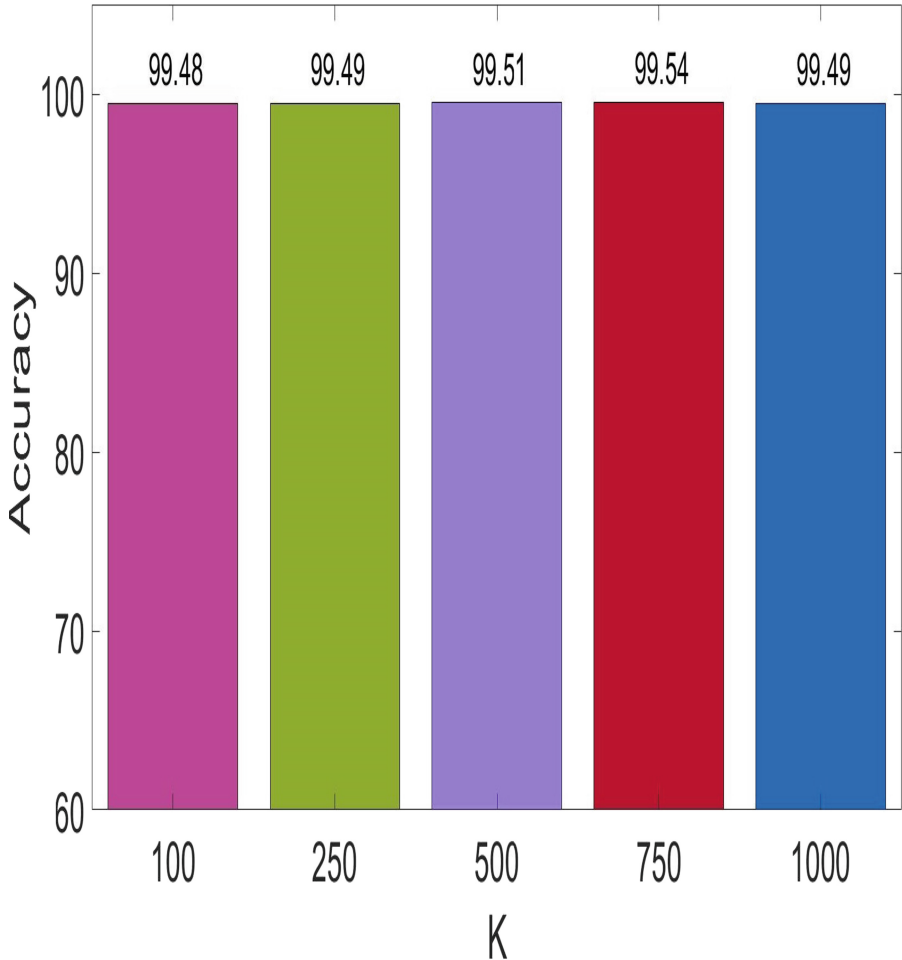


Fig. 2. Average accuracy of AA-Dense RNN attack detector with incremental online learning for different values of $K \in \{100, 250, 500, 750, 1000\}$

Figure 2 presents the average classification accuracy (over all packets) for each value of $K \in \{100, 250, 500, 750, 1000\}$. The results in Fig. 2 show that AA-Dense RNN with incremental online learning achieves its best performance for $K = 750$ packets, where the average accuracy equals 99.54. In addition, one may see that AA-Dense RNN achieves acceptable accuracy for all K .

5 Computation Time

For the proposed method, Table 1 presents the execution time (i.e. time elapsed) for making a decision on a single packet as well as the initialization and incremental update stages of the training algorithm for $K = 750$. Note that we measured the computation times on a PC with 32 GB ram and AMD Ryzen 7 3.70 GHz processor.

The results in this table first show that the execution time of AA-Dense RNN is very low and acceptable for real-time attack detection. Also, we see that the initialization and incremental online learning of our method take 15 ms and 4.3 ms, respectively. As observed in the evaluated dataset, 4.3 ms is slightly less than the minimum measured time for transmission of 22 packets; that is, the parameters of AA-Dense RNN will be updated until the transmission of the 22nd packet after the incremental online learning phase has begun.

Table 1. Training and online run-times of the proposed attack detection method with incremental online learning

Training time (for $K = 750$)	Initialization	15 ms
	Incremental update	4.3 ms
Execution time		0.11 ms

6 Conclusions

Devices in the Massive IoT segment are vulnerable targets for Mirai Botnet attacks as they are often deployed quickly with low-security measures. Therefore, in this paper, we developed a Mirai Botnet attack detection method based on Auto-Associative Dense Random Neural Network (AA-Dense RNN) with an incremental online learning algorithm. One of the main advantages of this method is that it learns the statistics of the normal (benign) IoT traffic when the IoT network is online, so it does not require collecting any (benign or attack) traffic beforehand.

We have evaluated the performance of the proposed method on a publicly available dataset containing 764, 137 packet transmissions and compared the performance of the proposed online AA-Dense RNN based attack detection method with that of offline trained AA-Dense RNN.

Our experimental results show that the proposed method achieves 99.54% accuracy with 99.79% TPR and 98.19% TNR while both training time (initialization and update) and execution time are very small and highly acceptable for real-time lightweight Mirai Botnet attack detection.

Our future work will extend our design to detect the various type of attacks via a single detector with incremental online training on only benign IoT traffic.

Acknowledgments. This research has been supported by the European Commission H2020 Program through the IoTAC Research and Innovation Action, under Grant Agreement No. 952684.

References

1. Hp study reveals 70 percent of Internet of Things devices vulnerable to attack. <https://www.hp.com/us-en/hp-news/press-release.html?id=1744676>
2. Kitsune Network Attack Dataset, August 2020. <https://www.kaggle.com/ymirsky/network-attack-dataset-kitsune>
3. Ahmed, Z., Danish, S.M., Qureshi, H.K., Lestas, M.: Protecting IoTs from Mirai Botnet attacks using blockchains. In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–6 (2019). <https://doi.org/10.1109/CAMAD.2019.8858484>
4. Antonakakis, M., et al.: Understanding the Mirai Botnet. In: Proceedings of the 26th USENIX Security Symposium (2017). <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>
5. Banerjee, M., Samantaray, S.: Network traffic analysis based iot botnet detection using honeynet data applying classification techniques. *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)* **17**(8) (2019)
6. Benzarti, S., Triki, B., Korbaa, O.: A survey on attacks in Internet of Things based networks. In: 2017 International Conference on Engineering & MIS (ICEMIS), pp. 1–7. IEEE (2017)
7. Biggs, J.: Hackers release source code for a powerful DDoS app called Mirai. TechCrunch, October 2018. <https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/>
8. Brun, O., Yin, Y., Gelenbe, E., Kadioglu, Y.M., Augusto-Gonzalez, J., Ramos, M.: Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 79–89. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95189-8_8
9. Cancela, H., Robledo, F., Rubino, G.: A grasp algorithm with RNN based local search for designing a wan access network. *Electron. Not. Discrete Math.* **18**, 59–65 (2004). <https://doi.org/10.1016/j.endm.2004.06.010>. <https://www.sciencedirect.com/science/article/pii/S1571065304010674>
10. Carl, G., Kesidis, G., Brooks, R., Rai, S.: Denial-of-service attack-detection techniques. *IEEE Internet Comput.* **10**(1), 82–89 (2006). <https://doi.org/10.1109/MIC.2006.5>
11. CISA: Understanding Denial-of-Service attacks. <https://us-cert.cisa.gov/ncas/tips/ST04-015>

12. Cramer, C.E., Gelenbe, E.: Video quality and traffic QoS in learning-based sub-sampled and receiver-interpolated video sequences. *IEEE J. Sel. Areas Commun.* **18**(2), 150–167 (2000)
13. Doshi, R., Apthorpe, N., Feamster, N.: Machine learning DDoS detection for consumer internet of things devices. In: 2018 IEEE Security and Privacy Workshops (SPW), pp. 29–35. IEEE (2018)
14. Douligeris, C., Mitrokotsa, A.: DDoS attacks and defense mechanisms: classification and state-of-the-art. *Comput. Netw.* **44**(5), 643–666 (2004)
15. Evmorfos, S., Vlachodimitropoulos, G., Bakalos, N., Gelenbe, E.: Neural network architectures for the detection of SYN flood attacks in IoT systems. In: Proceedings of the 13th ACM International Conference on Pervasive Technologies Related to Assistive Environments, pp. 1–4 (2020)
16. Gelenbe, E., Yin, Y.: Deep learning with random neural networks. In: 2016 International Joint Conference on Neural Networks (IJCNN), pp. 1633–1638 (2016). <https://doi.org/10.1109/IJCNN.2016.7727393>
17. Gelenbe, E.: Random neural networks with negative and positive signals and product form solution. *Neural Comput.* **1**(4), 502–510 (1989)
18. Gelenbe, E.: Learning in the recurrent random neural network. *Neural Comput.* **5**(1), 154–164 (1993)
19. Gelenbe, E., Stafylopatis, A.: Global behavior of homogeneous random neural systems. *Appl. Math. Model.* **15**(10), 534–541 (1991)
20. Gelenbe, E., Yin, Y.: Deep learning with dense random neural networks. In: Gruca, A., Czachórski, T., Harezlak, K., Kozielski, S., Piotrowska, A. (eds.) *ICMMI 2017. AISC*, vol. 659, pp. 3–18. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-67792-7_1
21. Goodin, D.: 100,000-strong Botnet built on router 0-day could strike at any time. *Ars Technica*, December 2017. <https://arstechnica.com/information-technology/2017/12/100000-strong-botnet-built-on-router-0-day-could-strike-at-any-time/>
22. Grenet, I., Yin, Y., Comet, J.-P., Gelenbe, E.: Machine learning to predict toxicity of compounds. In: Kůrková, V., Manolopoulos, Y., Hammer, B., Iliadis, L., Maglogiannis, I. (eds.) *ICANN 2018. LNCS*, vol. 11139, pp. 335–345. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01418-6_33
23. Hackett, R.: Why a hacker dumped code behind colossal website-trampling botnet, October 2016
24. Htwe, C.S., Thant, Y.M., Thwin, M.M.S.: Botnets attack detection using machine learning approach for IoT environment. *J. Phys. Conf. Ser.* **1646**, 012101 (2020)
25. Javed, A., Larijani, H., Ahmadinia, A., Gibson, D.: Smart random neural network controller for HVAC using cloud computing technology. *IEEE Trans. Industr. Inf.* **13**, 351–360 (2017)
26. Kim, H., Gelenbe, E.: Anomaly detection in gene expression via stochastic models of gene regulatory networks. In: *BMC Genomics*, vol. 10, pp. 1–10. BioMed Central (2009)
27. Kumar, A., Lim, T.J.: Early detection of Mirai-like IoT bots in large-scale networks through sub-sampled packet traffic analysis. In: Arai, K., Bhatia, R. (eds.) *FICC 2019. LNNS*, vol. 70, pp. 847–867. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-12385-7_58
28. Letteri, I., Del Rosso, M., Caianiello, P., Cassioli, D.: Performance of botnet detection by neural networks in software-defined networks. In: *ITASEC* (2018)
29. Liu, J., Liu, S., Zhang, S.: Detection of IoT botnet based on deep learning. In: 2019 Chinese Control Conference (CCC), pp. 8381–8385. IEEE (2019)

30. McDermott, C.D., Majdani, F., Petrovski, A.V.: Botnet detection in the Internet of Things using deep learning approaches. In: 2018 International Joint Conference on Neural Networks (IJCNN), pp. 1–8. IEEE (2018)
31. Mirsky, Y., Doitshman, T., Elovici, Y., Shabtai, A.: Kitsune: an ensemble of autoencoders for online network intrusion detection. In: The Network and Distributed System Security Symposium (NDSS) 2018 (2018)
32. Mohamed, S., Rubino, G.: A study of real-time packet video quality using random neural networks. *IEEE Trans. Circuits Syst. Video Technol.* **12**(12), 1071–1083 (2002)
33. Nakip, M., Gelenbe, E.: MIRAI botnet attack detection with auto-associative dense random neural network. In: IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2021)
34. Oke, G., Loukas, G., Gelenbe, E.: Detecting denial of service attacks with Bayesian classifiers and the random neural network. In: 2007 IEEE International Fuzzy Systems Conference, pp. 1–6. IEEE (2007)
35. Parra, G.D.L.T., Rad, P., Choo, K.K.R., Beebe, N.: Detecting Internet of Things attacks using distributed deep learning. *J. Netw. Comput. Appl.* **163**, 102662 (2020)
36. Prokofiev, A.O., Smirnova, Y.S., Surov, V.A.: A method to detect internet of things botnets. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus), pp. 105–108. IEEE (2018)
37. Sakellari, G., Gelenbe, E.: Adaptive resilience of the cognitive packet network in the presence of network worms. In: Proceedings of the NATO Symposium on C3I for Crisis, Emergency and Consequence Management, pp. 11–12 (2009)
38. Sakellari, G., Gelenbe, E.: Demonstrating cognitive packet network resilience to worm attacks. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 636–638 (2010)
39. Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R., Sakurai, K.: Machine learning-based IoT-botnet attack detection with sequential architecture. *Sensors* **20**(16), 4372 (2020)
40. Sriram, S., Vinayakumar, R., Alazab, M., Soman, K.: Network flow based IoT botnet attack detection using deep learning. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 189–194. IEEE (2020)
41. Statt, N.: How an army of vulnerable gadgets took down the web today, October 2016. <https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained>
42. Tuan, T.A., Long, H.V., Kumar, R., Priyadarshini, I., Son, N.T.K., et al.: Performance evaluation of botnet DDOS attack detection using machine learning. *Evol. Intell.*, 1–12 (2019)
43. Tzagkarakis, C., Petroulakis, N., Ioannidis, S.: Botnet attack detection at the IoT edge based on sparse representation. In: 2019 Global IoT Summit (GIoTS), pp. 1–6. IEEE (2019)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

