CSCI6709 Project Proposal – SDN-based Federated Learning System for Detecting DDoS on IoT

Nathanael Bowley, Hongwei Zhang, Raham Moghaddam, Han Yang, Ehssan Mousavipour

I. OBJECTIVE

Internet of Things (IoT) devices have become ubiquitous with the number of Internet-accessible IoT devices anticipated for 2030 going from 25.4 billion as of Feb 20, 2021 [2] to 29.42 billion by 2030 [16] as of March 7, 2023. The creation of the Mirai malware in September of 2016 [1] coincides with the rise of the popularity of IoT and its exploitation. Other attacks include the enlistment of IoT devices into a botnet [2], launching a Denial of Service (DoS), or Distributed DoS (DDoS) [2]. Methods of detection and prevention of these attacks are critical to ensuring the confidentiality, integrity, and availability of IoT device services.

In [1], Nguyen *et al.* proposed a self-learning IoT anomaly detection system model called DÏoT which used federated learning to detect attacks before the Mirai malware could enter its infection stage. DÏoT was reported to only have an 88.96% true positive rate in detecting DoS attacks. Popoola *et al.* in [2] use federated learning to detect zero-day botnet attacks on IoT devices and also looked at DDoS and DoS, however, training was not solely designed for the purpose of detection of DDoS.

Our project proposes building on the research of [1] and [2] to train and deploy an existing federated learning-based DDoS attack detection system using the Edge-IIoTset IoT dataset [17]. We aim to train, test, and model our system as a SOHO (Small Office / Home Office) IoT environment using an emulated SDN approach.

II. BACKGROUND AND MOTIVATION

A. Internet of Things

Internet of Things (IoT) is a network architecture in which many smart devices with integrated processors, sensors, memory, communication modules, and other hardware are connected together to form an interconnected network of communicating devices also known as an IoT system [18]. Sensors, RFID, and communication technologies interact as the hardware and software that serves as the foundation of IoT, enable IoT devices to communicate with each other, and allow user interaction [19]. As IoT technology emerges from its technological infancy, novel applications can be expected to coincide with the roll-out of 5G technology.

B. Federated Learning

Federated Learning (FL) is a distributed machine learning scheme that coordinates many clients for training models through one or more central servers [20]. FL is suitable for application scenarios concerning data privacy, such as for IoT. In addition, the distributed model training scheme can enable machine learning on IoT devices under the hardware performance constraints [21].

C. Software-Defined Networking

Software-Defined Networking (SDN) is a new network architecture with the main feature of separating the control plane of network devices from the data plane, enabling network programmability and centralized traffic management [22]. SDN offers advantages in flexibility, scalability, and security, and thus can provide new solutions for IoT security [23].

D. Distributed Denial-of-Service

Distributed Denial-of-Service (DDoS) organizes a large number of attackers located in different locations to launch simultaneous attacks on the target which denies the target of performing normal functions by exhausting the network [24]. DDoS creates a great threat to IoT because both DDoS and IoT have a distributed feature, attackers can hijack a large number of IoT devices to form a botnet and thus launch attacks on servers [25].

Related Works

ML-based Intrusion Detection Systems (IDS) for IoT devices have shown their efficiency in both academia and industry for several years because of their accuracy and flexibility. Training a traditional ML model usually requires a large amount of data, however, in FL we use distributed ML; therefore, we need less amount of data for training the models locally, and the models can be aggregated on the controller. Federated learning allows clients to contribute to ML models to improve model performance without sharing full data, which has become one of the addressable solutions for running an ML-based IDS for IoT attacks. There are several previous works on malware detection utilizing federated learning on IoT, which we draw inspiration from for this project [1], [2].

Popoola *et al.* have proposed a zero-day botnet detection method on IoT-edge devices based on Federated Deep Learning (FDL) in [2]. The authors implemented FDL by denoting IoT-edge devices as clients, and the model parameter server as the server. Then they simulated a zero-day botnet attack scenario by using Mirai and BASHLITE to test the detection performance under the FDL. They compared the FDL with a localized deep learning model, and a centralized learning model under the same neurons and architecture. Finally, they found that FDL-based methods achieved better classification results with more security channels during model aggregations.

In [1], Nguyen *et al.* designed an anomaly IDS based on FL called DÏoT. To further reduce the false alarm rate of previous work, authors have considered data traffic homogeneity between IoT devices and developed an auto device-type Identification module that classifies IoT devices based on their type. For the same types of devices, they applied FL to train one global model which is fitting to all devices. Furthermore, they generate their own attack and benign dataset by infecting devices with the malware Mirai. Their system achieves zero false alarm rate and the true positive rate is around 95.6% on average.

However, for both previous works, the ML-based IDS was deployed on a traditional network for IoT malware detection. Maeda *et al.* have proposed a new IoT botnet detection system based on SDN architecture in [26]. In their work, the controller will extract the features of network traffic for training a DNN model to monitor the ongoing traffic, once the suspicious behaviour has been detected, controllers will create flow rules to block external communication and isolate infected hosts using VLANS. Since in SDN, the controller has a global view of the network, it can react fast to reduce the damage of attack once detected.

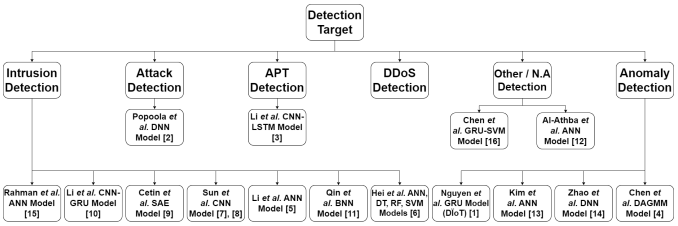

Fig. 1. Detection Targets of Related Federated Learning Articles

Approaches based on FL usually show higher reliability and higher classification performances compared with traditional methods [1], [2]. In addition, the SDN architecture has advantages over traditional networks such as easy configuration and management, efficient policy enforcement and so on. We believe that deploying an FL-based approach to detect IoT-based DDoS attacks using an SDN architecture can bring higher reliability and accuracy than previous work. In addition, Figure 1 displays a list of previous FL-based attack detection systems, the majority of previous FL-based IDS are focusing on detecting malware and none of those systems are specific to DDoS detection for IoT. To sum up, our claimed contributions to this project are the following:

1) Our project will be the first FL-based IDS for IoT DDoS detection which is deployed under SDN architecture.
2) Our project is focusing on DDoS detection on IoT devices which has not been covered by previous research.
3) Our system will set up open flow rules to block DDoS traffic when attacks are detected to reduce the affection of the attacks.

Motivation

Although prior research has explored the development of ML-based IDS for IoT devices, the inherent difficulties encountered in these systems necessitate the exploration of innovative approaches. In this regard, the current study proposes FL as a viable solution to these challenges. In addition to its potential applications in addressing DDoS attacks, FL represents a novel means of addressing various issues in the field that have yet to be fully explored. As such, this paper aims not only to present the findings of our study on FL but also to serve as a foundation for future research endeavours that will harness the potential of this approach more extensively.

III. SYSTEM OVERVIEW

As Figure 2 displays, there are three main components in our system, the controller, switch, and security gateway. The controller is used to take responsibility for network management and also acts as the model parameter aggregation server on the FL. The switch takes the responsibility of communication and will maintain a flow table for the purpose of routing. The security gateway is the access point of the network which will store the traffic data for IoT devices connected to it, and it will train localized ML models based on saved data. Lastly, the gateway will retrieve an updated global model from the controller, and then use it to monitor the communication traffic of the device it is connected to. The controller will inject flow rules on the switch when traffic arrives to it, and will pass them to the security gateway for attack detection purposes.

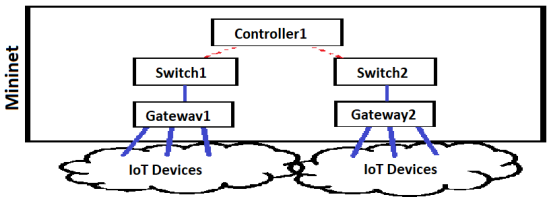

Fig. 2. System Architecture Overview

IV. CHALLENGES

In this project, we face several challenges. Firstly, we need to ensure the accuracy of the DNN model, which requires a reliable testing mechanism. Secondly, we must simulate IoT devices and their data transmission to the gateway. Thirdly, we need to identify the most suitable DNN architecture for our problem, given the variety of available options. Finally, we require a recovery mechanism to be in place after a DDoS attack has been detected.

V. NEXT STEPS

In the next step, we will use the Edge-IIoTset [17] to represent the IoT device data and employ a Federated Deep Neural Network (DNN) approach, specifically a Convolutional Neural Network (CNN), to address resource consumption and data privacy concerns [1], [2]. To test the effectiveness of our DNN model, we will use the TCP replay technique, which involves capturing and replaying packets of network traffic. Finally, we will ensure network isolation to prevent failure in other parts of the network [1], [2].

References

[1] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "Dïot: A federated self-learning anomaly detection system for iot," in *2019 IEEE 39th International conference on distributed computing systems (ICDCS)*, pp. 756–767, IEEE, 2019.

[2] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in iot-edge devices," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3930–3944, 2021.

[3] Z. Li, J. Chen, J. Zhang, X. Cheng, and B. Chen, "Detecting advanced persistent threat in edge computing via federated learning," in *Security and Privacy in Digital Economy: First International Conference, SPDE 2020, Quzhou, China, October 30–November 1, 2020, Proceedings 1*, pp. 518–532, Springer, 2020.

[4] Y. Chen, J. Zhang, and C. K. Yeo, "Network anomaly detection using federated deep autoencoding gaussian mixture model," in *Machine Learning for Networking: Second IFIP TC 6 International Conference, MLN 2019, Paris, France, December 3–5, 2019, Revised Selected Papers 2*, pp. 1–14, Springer, 2020.

[5] K. Li, H. Zhou, Z. Tu, W. Wang, and H. Zhang, "Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning," *IEEE Access*, vol. 8, pp. 214852–214865, 2020.

[6] Y. Sun, H. Esaki, and H. Ochiai, "Adaptive intrusion detection in the networking of large-scale lans with segmented federated learning," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 102–112, 2020.

[7] Y. Sun, H. Ochiai, and H. Esaki, "Intrusion detection with segmented federated learning for large-scale multiple lans," in *2020 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, 2020.

[8] B. Cetin, A. Lazar, J. Kim, A. Sim, and K. Wu, "Federated wireless network intrusion detection," in *2019 IEEE International Conference on Big Data (Big Data)*, pp. 6004–6006, IEEE, 2019.

[9] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "Deepfed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, 2020.

[10] Q. Qin, K. Poularakis, K. K. Leung, and L. Tassiulas, "Line-speed and scalable intrusion detection at the network edge via federated learning," in *2020 IFIP Networking Conference (Networking)*, pp. 352–360, IEEE, 2020.

[11] N. A. A.-A. Al-Marri, B. S. Ciftler, and M. M. Abdallah, "Federated mimic learning for privacy preserving intrusion detection," in *2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 1–6, IEEE, 2020.

[12] S. Kim, H. Cai, C. Hua, P. Gu, W. Xu, and J. Park, "Collaborative anomaly detection for internet of things based on federated learning," in *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 623–628, IEEE, 2020.

[13] Y. Zhao, J. Chen, Q. Guo, J. Teng, and D. Wu, "Network anomaly detection using federated learning and transfer learning," in *Security and Privacy in Digital Economy: First International Conference, SPDE 2020, Quzhou, China, October 30–November 1, 2020, Proceedings*, pp. 219–231, Springer, 2020.

[14] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of things intrusion detection: Centralized, on-device, or federated learning?," *IEEE Network*, vol. 34, no. 6, pp. 310–317, 2020.

[15] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, "Intrusion detection for wireless edge networks based on federated learning," *IEEE Access*, vol. 8, pp. 217463–217472, 2020.

[16] L. S. Vailshery, "Number of internet of things (iot) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030," Nov 2022.

[17] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022.

[18] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A review and state of art of internet of things (iot)," *Archives of Computational Methods in Engineering*, pp. 1–19, 2021.

[19] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[20] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," *Computers & Industrial Engineering*, vol. 149, p. 106854, 2020.

[21] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021.

[22] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in sdn: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 159, p. 102595, 2020.

[23] O. Blial, M. Ben Mamoun, and R. Benaini, "An overview on sdn architectures with multiple controllers," *Journal of Computer Networks and Communications*, vol. 2016, 2016.

[24] S. Yu and S. Yu, "An overview of ddos attacks," *Distributed Denial of Service Attack and Defense*, pp. 1–14, 2014.

[25] R. Vishwakarma and A. K. Jain, "A survey of ddos attacking techniques and defence mechanisms in the iot network," *Telecommunication systems*, vol. 73, no. 1, pp. 3–25, 2020.

[26] S. Maeda, A. Kanai, S. Tanimoto, T. Hatashima, and K. Ohkubo, "A botnet detection method on sdn using deep learning," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, IEEE, 2019.