Federated Wireless Network Intrusion Detection

Burak Cetin, Alina Lazar
Youngstown State University
Youngstown, OH
bcetin@student.ysu.edu, alazar@ysu.edu

Jinoh Kim
Texas A&M University-Commerce
Commerce, TX
jinoh.kim@tamuc.edu

Alex Sim, Kesheng Wu
Lawrence Berkeley National Laboratory
Berkeley, CA
asim, kwu@lbl.gov

***Abstract*—Wi-Fi has become the wireless networking standard that allows short- to medium-range device to connect without wires. For the last 20 year, the Wi-Fi technology has so pervasive that most devices in use today are mobile and connect to the internet through Wi-Fi. Unlike wired network, a wireless network lacks a clear boundary, which leads to significant Wi-Fi network security concerns, especially because the current security measures are prone to several types of intrusion. To address this problem, machine learning and deep learning methods have been successfully developed to identify network attacks. However, collecting data to develop models is expensive and raises privacy concerns. The goal of this paper is to evaluate a federated learning approach that would alleviate such privacy concerns. This initial work on intrusion detection is performed in a simulated environment. Once proven feasible, this process would allow edge devices to collaboratively update global anomaly detection models, without sharing sensitive training data. On a set of tests with the AWID intrusion detection data set, we show that our federated approach is effective in terms of classification accuracy, computation cost, as well as communication cost.**

I. Introduction

With the evolution and increase in popularity of communication technology, mobile and IoT devices, Wi-Fi technology is widely used because of its advantages in terms of mobility and low price. Compared to wired computer networks, Wi-Fi networks are not only slower but also require additional security layers. The fact that data packets are transmitted through the air, and easily intercepted and tampered with makes Wi-Fi networks vulnerable to various kinds of attacks. Therefore, there is an urgent need for Wi-Fi security defense methods that are fast, cheap and efficient. The server-side intrusion detection is a good approach that can provide security by checking each network transfer to detect any wireless intrusion attacks.

Wireless intrusion detection systems (WIDs) built based on classical machine learning [1] or deep learning methods [2] provide good performance for detecting such anomalous events. However, collecting wireless network data to be used for server-side machine learning training, is not only expensive but raises user privacy concerns. Federated learning provides a feasible solution to this problem because only the local models are moved to the server instead of the local data.

Network anomaly detection [3], [4] can be defined as the process of identifying unusual activities or attacks taking place in the network. When designing and building intrusion detection tools, especially using machine learning algorithms, the main goal is to correctly predict intrusions. In addition, reducing the number of false positive instances or the attack instances classified as normal is a must. This type of data can be passively collected by computers directly connected to the routers or access points. Data from multiple routers would be sent to a central server where all the processing and modeling would occur. Based on the prediction and analysis results, alerts can be sent to the network engineers to take necessary action. All this requires high network bandwidth connections to the centralized servers in order to move the data, threatens the privacy of the users involved and introduces additional latency into the process.

A solution recently developed [5] uses deep learning neural networks to train models locally on computing devices associated with access points in this case. This approach should be able to identify attacks where they take place quickly, collect data and use the new data to adjust the local models. This allows the system to correctly identify instances of intrusion right where attacks take place.

II. Related Works

Anomaly detection is an important studied task that has applications to network intrusion and has been studied in the wired and wireless settings. A diverse set of implementation, ranging from statistical approaches [3], [4] to machine learning [1] and deep neural networks is available. The use of deep learning as a state-of-the-art approach for wireless intrusion detection has been investigated in several recent studies [2], [6], [7].

For example, Wang et al. [2] analyzed network attacks in the Wi-Fi setting by comparing the results of two Deep Neural Network (DNN) architectures and one Stacked Autoencoder (SAE) in terms of network attacks classification. The approach presented in this paper improves upon the method described by Thing [7]. According to the paper, they used the Aegean Wi-Fi Intrusion Dataset (AWID) reduced dataset and classified the network records into four categories: normal, injection attacks, impersonation attacks and flooding attacks. They report classification accuracy above 98.3% for three of the classes and 73% only for the flooding attack class. Also, [6] proposed a different architecture based on the popular ladder network implementation and achieved even better results with an overall accuracy of 98.54%.

The concept of federated learning is an emerging paradigm, initially proposed by Google researchers [5]. This first paper showed the applicability of deep convolutional neural networks

in the federated setting for image classification tasks and next word prediction tasks [5], [8]. While we aim to use a similar general architecture, we apply federated learning to the intrusion detection task. However, this problem is harder, compared to image classification tasks because of the data imbalance issue. The AWID dataset has a 10:1 ratio between the normal and abnormal instances.

Previous studies [9], [10], [11] describe experiments for the intrusion detection task in a federated environment using the KDD 1999 cup data and the AWID dataset respectively. In the study developed by Preuveneers [11], federated learning is combined with block-chain technology to prevent malicious cyber-attacks. The experiments described here were applied to a realistic intrusion detection use case (AWID dataset) and using SAE models for anomaly detection. They show that the addition to block chain has small effects on the performance of the federated learning.

III. Methods

In this paper, we propose and evaluate a federated learning [5] method for building WIDs models. This approach allows edge devices to use locally collected data to train their local models first. Next, a global model is constructed by averaging the local models. In this way, the edge devices do not have to share their raw training data that may contain sensitive information. Mobile or edge devices train a local model, and send only model parameters to the server, instead of the raw training data. We apply this federated learning approach to classify outgoing network transfers, namely predicting whether a transfer is normal or attack.

The approach to anomaly detection uses Stacked Autoencoders (SAE), a specialized kind of deep learning neural network, designed to capture a compressed representation of the anomalous observations. In the federated learning setting, these algorithms learn from the new observations and update the local and global models in order to identify new trends.

Methodological challenges we had to address in order to apply federated learning to perform intrusion detection include: feature selection, deep learning model choice and tuning the federated learning parameters. We also evaluated our methodology using the AWID wireless intrusion dataset.

To evaluate the federated intrusion detection approach we use performance metrics introduced by Caldas [8] for the benchmarking framework LEAF. To capture and analyze the distribution of training and testing performance across devices, the accuracy performance at the 10th and 90th percentiles are recorded for inspection and visualization. Another important metric for federated learning accounts for the total amount of computing resources and communication needs from the edge devices in terms of number of computer operations and number of bytes downloaded/uploaded.

IV. Datasets

To validate the proposed method, the Aegean Wi-Fi Intrusion Dataset (AWID) [1] was used. This dataset, published in 2015, contains records labeled "normal" and multiple types of attacks ("attack"). The number of normal and three main attack categories is shown in Table I. This dataset is currently the largest and most recent Wi-Fi network data publicly available. The data were captured using Wireshark [12] in a small wireless network environment comprised of 11 clients. There are training and testing subsets available.

TABLE I
AWID Dataset Distribution

Dataset	Normal	Injection	Impers.	Flooding
AWID-CLS-R-Trn	1,633,190	65,379	48,522	48,484
AWID-CLS-R-Tst	530,785	16,682	20,079	8,097
Total	2,163,975	82,061	68,601	56,581
Balanced	205,285	82,061	68,601	56,581

Before running any experiments, we follow the preprocessing, normalization and balancing procedure described by Ran [6]. The resulting balanced dataset has the same number of normal instances as all the attack instances combined. This is showed on the last row of Table I.

To perform federated learning experiments in a simulated environment, using dataset previously collected, we need to distribute the data among devices in a heterogeneous manner such that the number of records and the underlying data distribution varies. We use the LEAF approach [8] to create a AWID federated learning dataset with 1,000 devices. Initially, the dataset is divided between devices in a stratified manner. The statistics and distribution between clients is shown in Table II and Figure 1. Each device's dataset is split into training and test datasets and each set of data contains both normal and attack data instances.

TABLE II
Statistics of AWID Dataset

Number of devices	Total samples	Samples/device	
		mean	std
1000	107,553	1.98	213.22

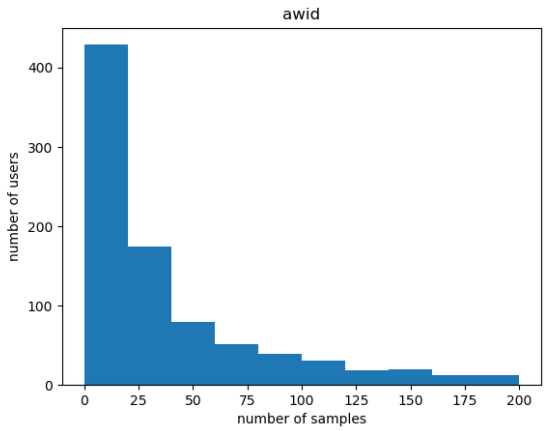

Fig. 1. Number of samples histogram

V. Experiment and Results

In our experiments, we prove the effectiveness of the FedAvg algorithm for the intrusion detection problem. Merging local models by averaging their weights on the central server works well even for a simple neural network model. In this case the input layer has a number of neurons equal to the number of attributes in the dataset (74), and the output layer has a number of neuron equal with the total number of classes (4). The neurons are equipped with the sigmoid activation function, and the loss is sparse softmax cross entropy.

We use a learning rate of 0.8, 10 devices per round and 20 rounds for all experiments. The convergence behavior of the FedAvg algorithm on a subset of 933 clients is shown in Figure 2. The train and test accuracies are comparable to the results reported by Wang in [2]. We also show the total communication cost in terms of bytes written and read during the training in Figure 3.

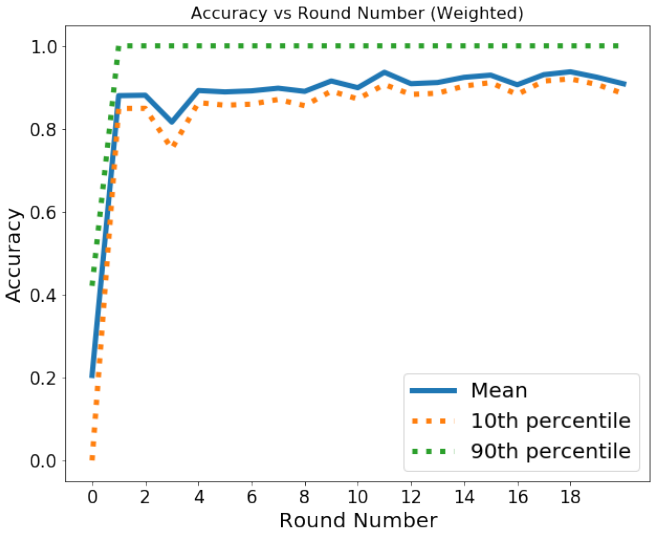

Fig. 2. Convergence behavior of the FedAvg algorithm on a subset of clients for the AWID dataset.

VI. Conclusion

In this work, we show how to build federated learning datasets using existing large datasets for performing federated learning experiments in simulated environments. The federated learning model built upon deep learning performs similar to the server-trained deep learning in terms of classification performance when applied to the wireless intrusion detection problem. Compared with the classical deep learning approach, the proposed model has the advantage that does not require moving the data to a central server, preserving user's privacy in this way that is very important for this particular problem.

In future we plan to design and run additional experiments to show the effectiveness of federated learning for the network intrusion detection problem. As a larger version of the AWID dataset is available, so the same experiments can be repeated in a larger setting with even more clients.

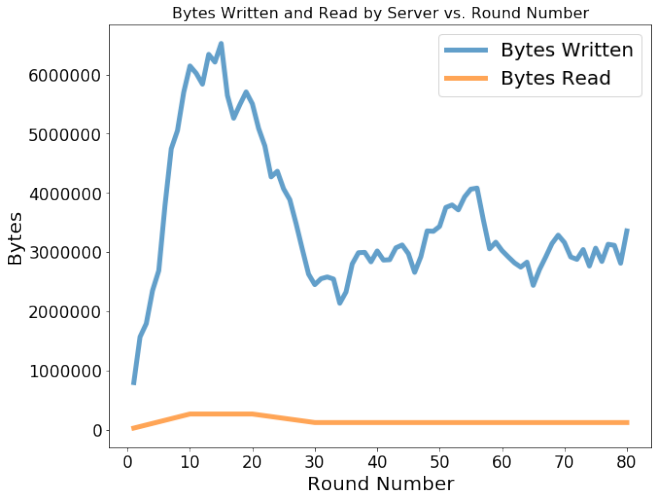

Fig. 3. Communication cost of the FedAvg algorithm on a subset of clients for the AWID dataset.

Acknowledgment

This work was supported by the Office of Advanced Scientific Computing Research, Office of Science, of the U.S. Department of Energy under Contract No. DE-AC02-05CH11231.

References

[1] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 184–208, 2016.

[2] S. Wang, B. Li, M. Yang, and Z. Yan, "Intrusion detection for WiFi network: A deep learning approach," in *Wireless Internet*. Springer International Publishing, 2019, pp. 95–104.

[3] S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques," *Procedia Comput. Sci.*, vol. 60, pp. 708–713, Jan. 2015.

[4] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, Jan. 2016.

[5] H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient learning of deep networks from decentralized data," Feb. 2016.

[6] J. Ran, Y. Ji, and B. Tang, "A Semi-Supervised learning approach to IEEE 802.11 network anomaly detection," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Apr. 2019, pp. 1–5.

[7] V. L. L. Thing, "IEEE 802.11 network anomaly detection and attack classification: A deep learning approach," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. ieeexplore.ieee.org, Mar. 2017, pp. 1–6.

[8] S. Caldas, P. Wu, T. Li, J. Konečný, H. Brendan McMahan, V. Smith, and A. Talwalkar, "LEAF: A benchmark for federated settings," Dec. 2018.

[9] J. Schneible and A. Lu, "Anomaly detection on the edge," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Oct. 2017, pp. 678–682.

[10] S. Xu, Y. Qian, and R. Q. Hu, "Data-driven edge intelligence for robust network anomaly detection," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2019.

[11] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, and E. Ilie-Zudor, "Chained anomaly detection models for federated learning: An intrusion detection case study," *NATO Adv. Sci. Inst. Ser. E Appl. Sci.*, vol. 8, no. 12, p. 2663, Dec. 2018.

[12] A. Nath, *Packet Analysis with Wireshark*. Packt Publishing, 2015.