Federated Learning Empowered End-Edge-Cloud Cooperation for 5G HetNet Security

Yunkai Wei, Sipei Zhou, Supeng Leng, Sabita Maharjan, and Yan Zhang

Abstract

The distributed and heterogeneous framework in the 5G heterogeneous network (HetNet) makes it vulnerable to attacks of different kinds. Nodes for improving the network security are therefore important to eliminate such critical threats. Without cooperation or with limited cooperation, these nodes are substantially restricted in their protecting capacity due to specific characteristics such as heterogeneity, hierarchy, and wide range in the 5G HetNet. In this article, we propose a federated learning empowered end-edge-cloud cooperation-based framework for enhancing 5G HetNet security. In this framework, nodes equipped with attack detection mechanisms are distributed in the end, edge, and cloud of the 5G HetNet. We then design cooperative training schemes to realize the full potential of these nodes in detecting attacks. Illustrative results demonstrate the superior performance of our proposed scheme compared to three different benchmark schemes.

Introduction

5G heterogeneous networks (HetNets) can connect a large number of nodes with different radio access technologies to provide universal high-rate coverage and seamless user experience. This distributed and heterogeneous framework of the 5G HetNet makes it vulnerable to attacks of different kinds such as denial of service (DoS), malware propagation, and malicious port scanning. The security issue is therefore an important concern in 5G HetNets. In this regard, we have observed some notable recent work to enhance the security in 5G HetNets. Secure frameworks for 5G wireless sensor networks and the 5G Internet of Things (IoT) were presented in [1, 2], respectively. The authors in [3] proposed a self-adaptive architecture for inspecting network flows in 5G mobile networks. Specialized schemes in distributed or centralized form were presented to improve the security of 5G HetNets in [4, 5]. Another group of work in this direction includes new enabling technologies, such as blockchain, cyber insurance, and artificial intelligence, to detect the anomalies [6, 7], and to enhance the security of 5G HetNets [8, 9].

It is a good approach to embed such techniques on appropriate nodes in 5G HetNets to provide enhanced attack detection capability. These nodes can be distributed in the access networks or the backbone of a 5G HetNet, and can be user nodes or dedicated nodes such as intrusion detection nodes. In general, these nodes are non-cooperative or have limited cooperation with each other. Few studies have attempted to address this issue. For instance, in [10, 11], the authors used federated learning to provide secure data sharing and to prevent user data leakage against attackers. In [12], the authors proposed a distributed machine-learning-based scheme for detecting cyber attacks in fog-to-things computing. Intelligent-module-based proactive network monitoring for security and protection of computing infrastructures was presented in [13]. These studies were conducted for specific network or application scenarios, and are therefore of limited use beyond those environments. This leads to the fact that the nodes are substantially restricted in the potential of enhancing the security in 5G HetNets, which is a mixture of wide-range HetNets and emerging applications.

Federated learning [14] is a distributed learning method allowing multiple parties to train a shared model by aggregating locally computed gradient updates without specific limitations on the location, technology, and architecture of the participants. Inspired by the ability of federated learning to integrate the learning capability of distributed, heterogeneous, and wide-range networks, we propose a federated learning empowered end-edge-cloud cooperation framework for enhancing 5G HetNet security. In our proposed architecture, nodes for attack detection are distributed in the 5G HetNet, including nodes from access networks (the end), the gateways of access networks (the edge), and the 5G backbone network (the cloud). We present the detailed schemes of the local training process at the end nodes and the edge nodes, respectively. Then, based on federated learning, we design cooperative training schemes among the end, the edge, and the cloud to improve their models for enhanced attack detection, and thus to realize their full potential in detecting attacks. Illustrative results demonstrate the performance of our proposed architecture and schemes, and show considerable improvement in detecting accuracy and training speed compared to three different benchmark schemes.

The rest of this article is organized as follows. We present the cooperative architecture for 5G HetNet security in the following section. Then we describe the detailed local model training schemes in the end and at the edge, respectively. The federated learning empowered cooperative model training among the end, edge, and cloud is

Digital Object Identifier:
10.1109/MNET.011.2000340

Yunkai Wei, Sipei Zhou, and Supeng Leng are with the University of Electronic Science and Technology of China;
Sabita Maharjan and Yan Zhang (corresponding author) are with the University of Oslo and Simula Metropolitan Center for Digital Engineering.

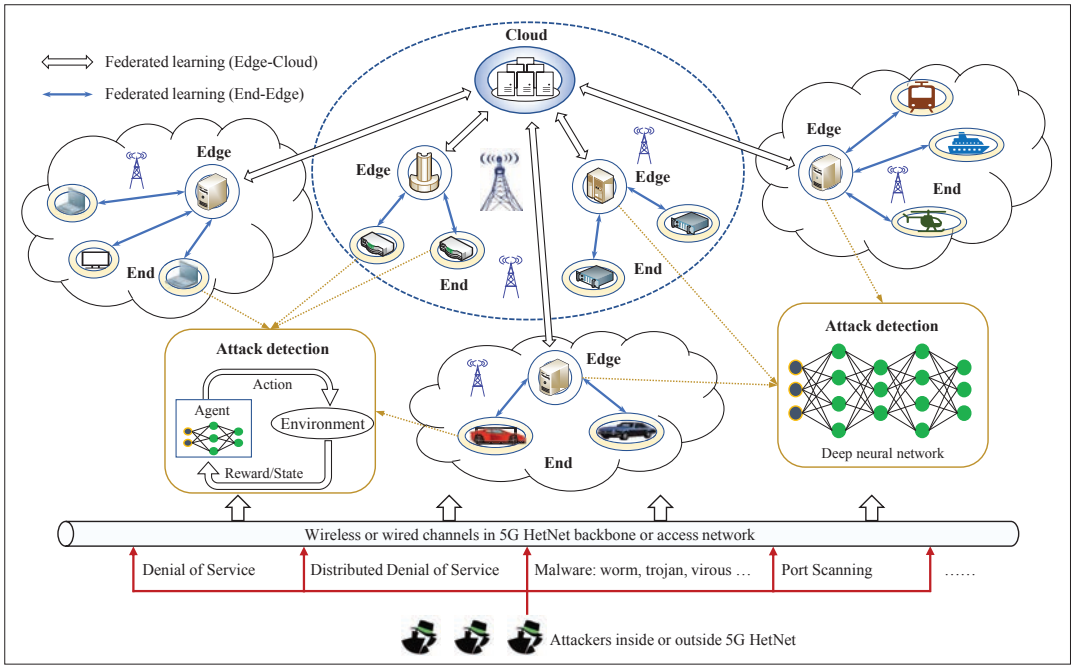

FIGURE 1. Federated learning empowered end-edge-cloud cooperation architecture for 5G HetNet security.

then highlighted. Following that, we illustrate the performance of our proposed cooperative framework through extensive numerical results. Finally, we conclude this article.

Our Proposed Architecture for 5G HetNet Security

The 5G HetNet has an end-edge-cloud hierarchical structure, and is thus vulnerable to various security threats distributed in the wide range of the HetNet. To address the security issues in such a distributed and heterogeneous framework, we propose a federated learning empowered end-edge-cloud cooperation architecture for 5G HetNet security. As shown in Fig. 1, attackers inside or outside 5G HetNet may launch attacks such as (distributed) DoS, port scanning, and malware propagation via wireless or wired channels in the backbone or access networks. To detect such attacks efficiently, nodes for detecting the attacks are distributed in three different layers of the 5G HetNet, that is, attack detecting nodes in the end, in the edge, and in the cloud, respectively. Model training cooperation among the layers can be conducted for enhanced capacity of attack detection. To highlight the attack detecting nodes, we only show the nodes with security function and omit other nodes from Fig. 1. The detailed description of the architecture is as follows.

Attack Detection in the End, Edge, and Cloud

Attack Detection in the End: The attack detection in the end, generally deployed in some powerful end nodes or devices in an access network, is responsible for detecting the attacks in this local access network. In our proposed architecture, the end node employs deep reinforcement learning (DRL) to train models for attack detection. Due to limited resources such as computing power or available training data, the end node will send the result from its local training to its responsible edge node to create an aggregated model with higher accuracy and wider adaptation. This can particularly benefit the end nodes when the nodes do not have enough computing resource to learn the whole dataset of this access network, or each end node has partial knowledge on the security of the access network and wants to have full knowledge on the security of this access network.

Attack Detection in the Edge: The edge is the intermediary between the end and the cloud. Attack detection in the edge is generally placed at the intersecting nodes of the local access network and the 5G backbone network. Consequently, the edge node has full knowledge on the security of the access network and partial knowledge on the security of the backbone network, and can detect the attacks at a higher level than an end node. In our proposed architecture, the edge node executes the following three functions:

- With federated learning, the edge node can help the end nodes in its coverage to improve the accuracy and training speed of their attack detecting models. Specifically, the edge node collects the model training results of the end nodes, conducts federated learning, achieves the integrated model, and returns it to the end nodes.
- The edge should execute its own deep learning module, which is different from the DRL module in the end, to detect the attacks in the local access network while connected to the backbone network.
- Directly connected to the backbone of a 5G HetNet, the edge node also faces the threat of various attacks originating from anywhere in the backbone network. It is essential to enhance the accuracy of the trained model for attack detection in each edge node by integrating the parameters from other appropriate edge nodes. Consequently, the edge node will participate in the federated-learning-based cooperation via the cloud.

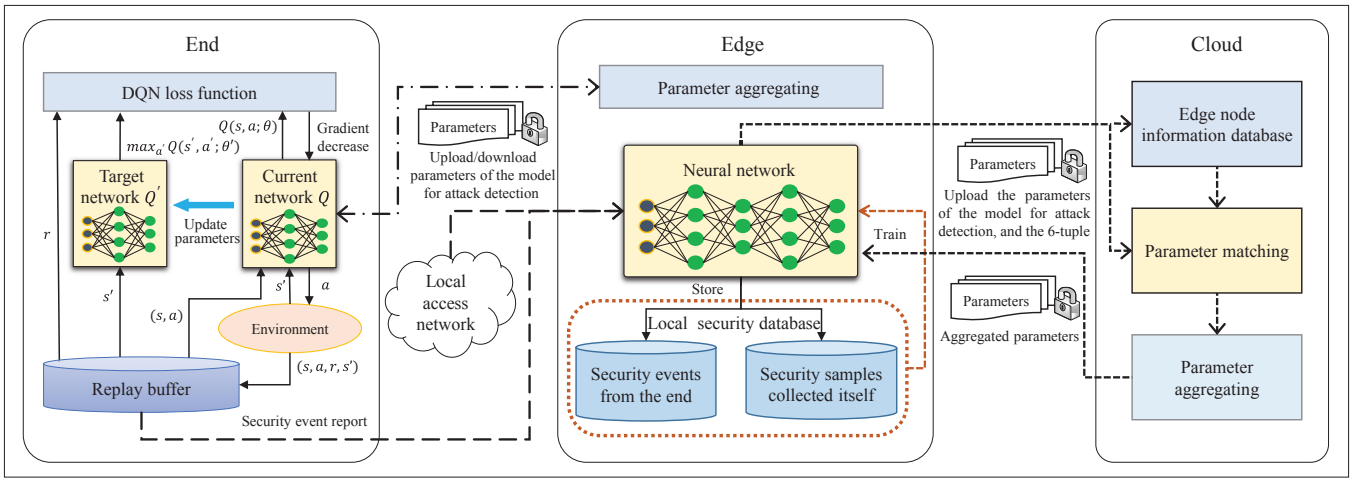

FIGURE 2. Model training in each layer.

Attack Detection in the Cloud: Attack detection in the cloud can be deployed on some dedicated servers or a data center inside the 5G backbone network, with a global perspective on the security of the whole network. The cloud can execute attack detection itself, as well as help the edge nodes to train more powerful models for attack detection. In this article, we concentrate on the latter function of the cloud. That is to say, the cloud collects the model parameters from the edge nodes, conducts parameter aggregation based on federated learning, and helps the edge nodes with enhanced models for attack detection.

Model Training Cooperation among Multiple Layers

In our proposed architecture, the nodes for attack detection in different layers cooperate with each other based on federated learning. With the parameter aggregation in the edge, the end nodes can improve the accuracy of the detecting models and speed up the training process. Meanwhile, the edge nodes send their model parameters to the cloud for aggregation in federated learning. According to the similarity of the edge nodes' network environments, the cloud can select appropriate model parameters, aggregate them in federated learning, and send the result back to the corresponding edge nodes to update the parameters in their local models for attack detection.

To this end, our proposed architecture can improve the attack detection effect and thus enhance the 5G HetNet security. Based on the federated learning empowered end-edge-cloud cooperation, the parameters of the model for attack detection in both the local access network and the 5G backbone network are flexibly and efficiently exchanged. This can achieve more accurate models for the multiple layers in detecting various attacks. The nodes for attack detection in each layer can inspect network behavior based not only on its own knowledge but also on the knowledge of its cooperators across the 5G HetNet. Such cooperation makes it easier to find hidden or distributed attacks, and it is more difficult for the attackers to break through the multi-layer security barrier. In addition, based on our proposed architecture, further actions such as tracing or locating the source of the attacks can also be easier, since the cooperation among the end, edge, and cloud can highlight the traces of the network behavior.

Besides the enhanced 5G HetNet security, our proposed architecture is expected to bring a variety of additional benefits, which are summarized below.

Practical Feasibility: The architecture facilitates cooperation among multiple layers of a 5G HetNet without demanding any major changes in current security systems and networks.

Compatibility: The architecture can be easily applied in different security systems beyond attack detection, such as intrusion prevention systems and vulnerability scanning systems.

Extensibility: The architecture can flexibly adapt to different scales of the target system, and support increasing or decreasing the number of attack detecting nodes of the multiple layers in real time as needed.

Model Training in Each Layer

In this section, we present the detailed schemes of the local training process at the end nodes and the edge nodes, respectively. The behavior of the cloud, which can help the edge nodes to train more powerful models for attack detection, is demonstrated in the model training cooperation later.

Model Training in the End

As a value-based reinforcement learning algorithm combined with deep learning, deep Q-network (DQN) can train agents to obtain the maximum reward in a dynamic environment. Consequently, models trained with DQN can adapt to changing network environments. In addition, DQN has the techniques of experience replay and interaction between current network and target network, and can thus prevent the end nodes from the sample correlation problem or the training instability problem during model training. We therefore adopt DQN to train the attack detecting models in the end nodes, as shown in Fig. 2. A 4-tuple (s, a, r, s') is used to store experiences, where s is the current state in the finite state space, a is the selected action in the finite action space, r is the returned reward from the environment after taking current action a, and s' is the next state. Two

action-value networks, that is, the current network Q and the target network Q', are used to improve the training stability. After sampling transitions (s_i, a_i, r_i, s_{i+1}) in the replay buffer, the current network Q can be updated by the gradient descent of the loss function

$$\left(r_i + \gamma \cdot \max_{a'} Q'(s_{i+1}, a'; \theta') - Q(s_i, a_i; \theta)\right)^2,$$

where γ is a discount factor of the future reward. The current network parameter Q will then be replicated to the target network Q' periodically.

The features of the transmitted packets in the local access network can indicate the state s of the end node. In the training period, with the finite training dataset, the state space $S = \{s\}$ is a finite set. The aim of the end node is to detect risks and protect the security of the local access network. Specifically, it will raise the alarm if any risk is detected in the local access network. Thus, the action space A of the end node can be denoted as $A = \{1, 0\}$, where 1 indicates that the end node detects a risk, and 0 indicates that it detects no risk.

According to the states and actions of the end node, the environment will return different rewards r. The reward space $R = \{r\}$ contains four cases:

- The local access network is secure, and the end node takes the correct action 0; the reward in this situation is +1.
- The local access network is at risk, but the end node takes the wrong action 0; the reward is −100.
- The local access network is secure, but the end node takes the wrong action 1; the reward is −1.
- The local access network is at risk, and the end node takes the correct action 1; the reward is +100.

Therefore, the reward space R of the end node is +1, −100, −1, +100.

After training, the end node executes attack detection in real time and reports attacking information to the edge node. Furthermore, to improve the accuracy of the models and to accelerate the training process, the end node will share the encrypted model parameters to the edge node to conduct federated learning. The detailed process is described below.

Model Training in the Edge

Deployed at the intersection of the local access network and the 5G HetNet backbone, the edge node should conduct not only its own model training, but also the preparatory work for the subsequent cooperation in training more powerful models for attack detection. Specifically, in our proposed architecture, the edge node participates in the model training process for the end nodes, trains its local deep learning model for attack detection, and also cooperates with the cloud to improve the performance of its local model. The process is described in more detail below.

First, the edge node can improve the detection accuracy and can accelerate the training speed of the end nodes in its local access network. The edge node collects the model parameters from the end nodes in its coverage. Based on federated learning, it can aggregate the model parameters, and then return the aggregated result to the end nodes. The parameters can be encrypted for secure transmission. The details are described later.

Second, the edge node executes the local attack detection function to protect the security of the local access network while connecting to the backbone network. The edge node trains the model for attack detection based on deep learning. For each training data x_k, it has an original label y_k^{lab}, which denotes whether this kind of transmitted packet is normal or malicious. Suppose the output of the model is y_k^{out} and the error associated with sample x_k in the model is $E_k = |y_k^{out} - y_k^{lab}|$. Then we can update the model using the gradient descent method by minimizing the average cumulative error $E = \Sigma_m E_k/m (0 \le k \le m)$, where m is the number of training data blocks. After training, the edge node can execute local attack detection. If attacks are detected, the edge node will take emergency measurements, inform other nodes, and store the attacking information in its local database. The edge node has two types of training samples in its local database according to the source of these samples, namely the security events from the end and the security samples collected by itself. These samples are stored in the local security database after essential processing by its neural network.

Finally, in order to improve the performance of the local model, the edge node can share local model parameters with the cloud and obtain a more accurate model after the periodic cooperation. As shown in Fig. 2, before sharing the model parameters, the edge node also sends a 6-tuple <type, location, scale, security level, density, topology> of the local access network to the cloud so as to identify its own network environment. The cloud will then aggregate the model parameters from the edge nodes with matched 6-tuple, as demonstrated below.

Model Training Cooperation among the End, Edge, and Cloud

In this section, we demonstrate the detailed cooperative model training schemes, including the federated-learning-based cooperation between the end and the edge, and that between the edge and the cloud. As Fig. 3 shows, to improve the ability of detecting various attacks aimed at the cloud, the edge, or the end of the 5G HetNet, the attack detecting nodes in the end and the edge upload their local parameters, download the aggregated parameters, and integrate them into their local models during cooperative model training. The detailed description of the cooperation procedure is as follows.

Model Training Cooperation between the End and the Edge

Based on federated learning, model training cooperation between the end and the edge can improve the attack detection accuracy of the trained model when each end node has limited training data, and can accelerate the training speed when the end nodes have limited computing resource.

Figure 3 shows the parameter aggregation process of the nodes in the edge for attack detection. The edge node collects the model parameters of

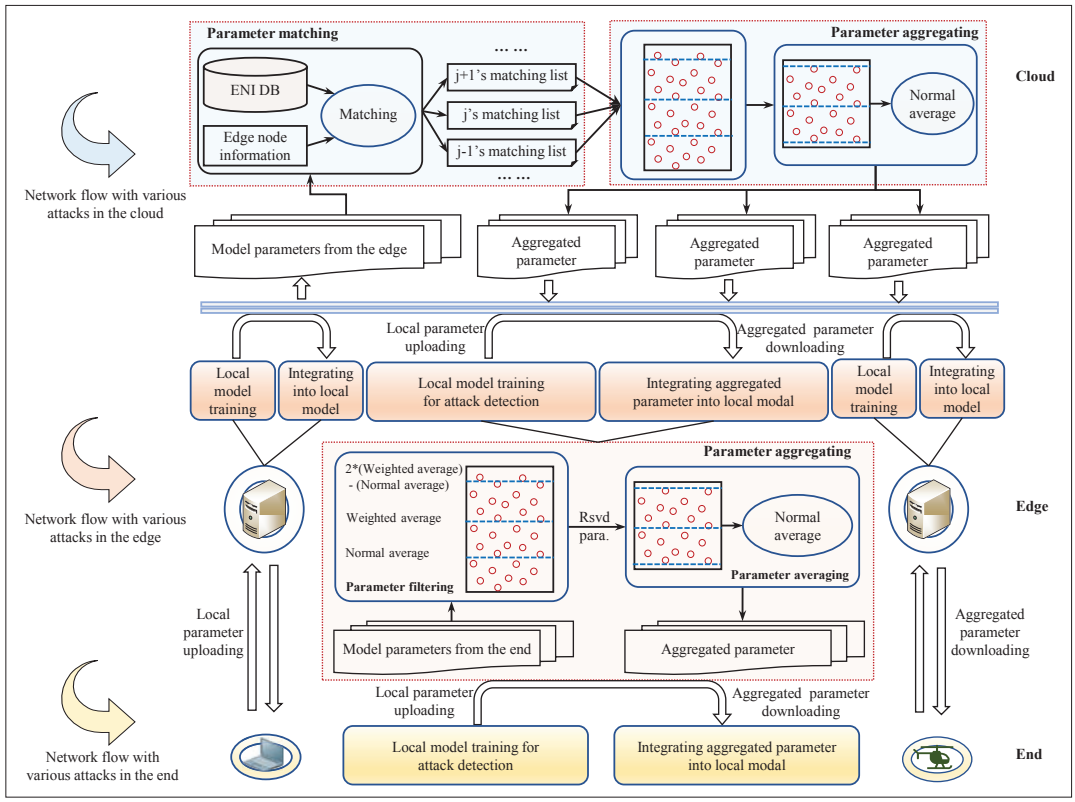

FIGURE 3. Model training cooperation, inner end-edge-cloud.

the end nodes in its coverage, and returns the aggregated results back to these end nodes. Then the end nodes can update their detection models with the aggregated parameters to obtain better performance. The detailed aggregation procedure is described below.

The number of end nodes for attack detection in the coverage of the edge node is n, and θ_i denotes the parameter of the reinforcement learning model in the end node i. The weight of θ_i is determined by the historical accuracy of the model in the end node i. In our proposed scheme, the edge node calculates both the weighted average and the normal average of the parameters from the end nodes in its coverage. Then two kinds of absolute values are calculated: the absolute value of the difference between the parameter $\theta_i (i = 1, ..., n)$ and the weighted average, and the absolute value of the difference between the normal average and the weighted average. If the former is no larger than the latter, parameter θ_i will be reserved for parameter aggregation. Otherwise, this parameter will be discarded. Afterward, the edge node calculates the new average of the reserved parameters as the aggregated result θ_{agg}, and sends it back to the end nodes.

Each end node integrates θ_{agg} into its own trained model for attack detection. To keep the local model stable, the end node uses a proportion τ to adjust the aggregation result θ_{agg} in the integration. The updated model of the end node i has new parameter $\theta_i' = \tau \cdot \theta_{agg} + (1 - \tau) \cdot \theta_i$. This model training cooperation can benefit the end nodes with higher detection accuracy and training speed without the need for full training data or redundant computing resources at these end nodes.

Model Training Cooperation between the Edge and the Cloud

Lying at the intersection of the local access network and the 5G backbone network, the edge node will face the security challenges from both the local access network and 5G HetNet. Consequently, an edge node needs not only the security knowledge of its own access network, but also that in other parts of the 5G HetNet. However, considering the heterogeneous and wide range of the 5G HetNet, the attacks in different access networks may be quite different from each other. For example, the attack types and characteristics in a vehicular network and an industrial network are fundamentally different. Simply aggregating the trained parameters of all the edge nodes in the 5G HetNet together cannot lead to enhanced attack detection.

Consequently, the cloud uses a parameter matching module to select the parameters of the edge nodes from a similar network environment, as shown in Fig. 3. When an edge node j submits its trained model parameters for attack detection to the cloud, the cloud will get the network information of this edge node, in the form of the aforementioned 6-tuple, and store it to an edge node information (ENI) database. Then, with a matching scheme, the cloud compares the network information of this edge node j with the other ones in the ENI database to find matching edge nodes deployed in a similar network environment. Specifically, the cloud calculates the Euclidean distances between the 6-tuples of the edge node j and the other edge nodes in the ENI database. If the Euclidean distance between the 6-tuples of the edge node j and another edge node k is less than a threshold ζ, these two edge nodes are in

a similar network environment and can match up with each other, and vice versa. Then the cloud forms an edge node set S_j as the matching result for the edge node j, which includes all the matched edge nodes and the node j itself.

The parameters of the edge nodes in the set S_j is sent to the parameter aggregating module to generate the aggregated result for edge node j. The parameter aggregating process is conducted separately for each edge node. For edge node j, the parameter aggregating module first conducts parameter filtering on the parameters in S_j. Then the reserved parameters are averaged to obtain the aggregated parameter for edge node j. Finally, this aggregated parameter is separately sent to edge node j for subsequent parameter integration.

Thus, based on federated learning, the cloud enhances the edge node's model with higher detecting accuracy on different attack types by aggregating the parameters of other matched edge nodes with similar network environments. This process can be conducted periodically to enhance the cooperation effect.

Illustrative Results

In this section, we illustrate the performance of our proposed architecture and schemes through extensive simulations. Based on the deep learning library called PyTorch, developed by Facebook Artificial Intelligence Research (FAIR), the simulations employ DQN for training the end nodes and the edge nodes. We use the dataset CICIDS2017 [15] with a total size of about 50 GB for model training and testing, which includes both normal packets and various attacking packets such as DoS, distributed DoS, and port scanning.

Figure 4 shows the performance of our proposed cooperative scheme based on federated learning between the end and the edge when the end nodes are trained for attack detection in the local access network. Each node has partial training data, containing both normal packets and attacking packets for DoS, distributed DoS, port scanning, and so on. We compared the performance of our proposed scheme with three different schemes: non-cooperative end nodes, traditional distributed machine learning, and traditional federated learning. All curves can converge to a stable value when the iteration number increases. The reward with our proposed cooperative scheme converges to 17, higher than the corresponding scenario without cooperation, which converges to 14. The reward of our proposed cooperation is larger than that without cooperation by about 21.43 percent. At the same time, the convergence speeds are different for the six curves. The scenario with 10 end nodes and the cooperative scheme shows the fastest training speed, converging after about 50,000 iterations. On the contrary, the training speed of the non-cooperative scenario is the slowest, converging after about 170,000 iterations. The training speed is improved by up to about 70 percent in our proposed cooperative scheme. Moreover, compared to traditional distributed machine learning and traditional federated learning, our proposed scheme outperforms them by up to 25 percent and 45 percent, respectively, in training speed.

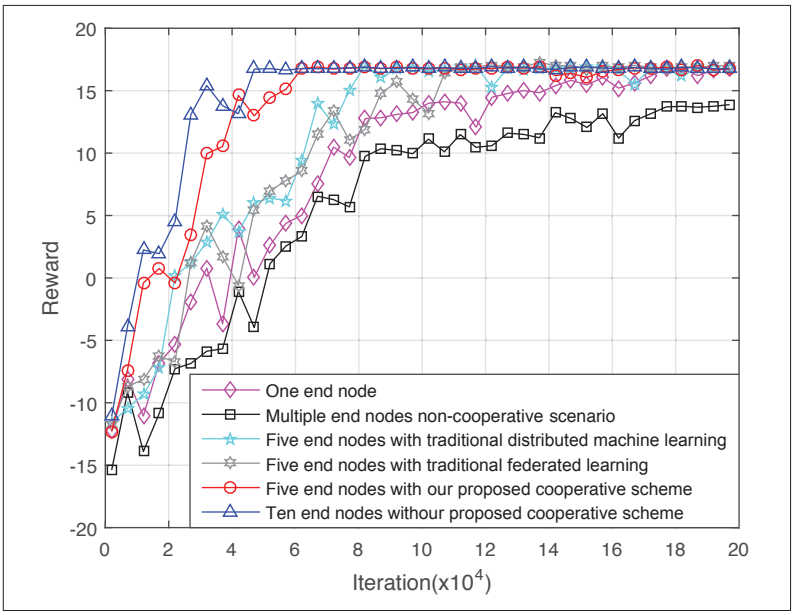

FIGURE 4. The average reward of the end nodes when the iteration number increases.

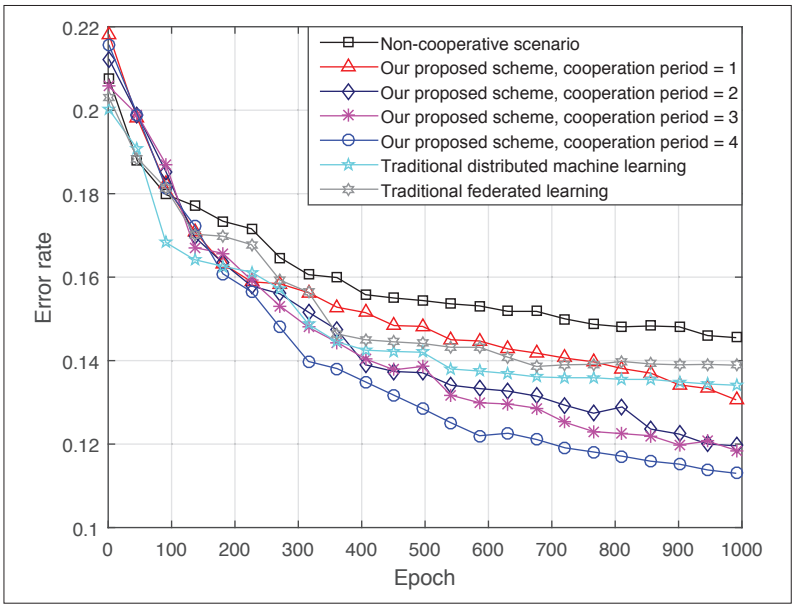

FIGURE 5. The attack detecting error rate of the edge nodes in different cooperation periods.

Figure 5 demonstrates the performance of our proposed cooperative scheme based on federated learning between the edge and the cloud when the edge nodes are trained for attack detection in the global environment of a 5G HetNet. A cooperation period equal to 0 means that there is no cooperation between the edge and the cloud. When the cooperation period is 1, the edge and the cloud have cooperated in model training for one round. Similarly, when the cooperation period is 2, they have cooperated for two rounds, and so on. As the epoch number increases, the performance of our proposed scheme is better than the non-cooperative, traditional distributed machine learning and conventional federated learning schemes. When the cooperation period is larger, the edge has a lower error rate in attack detection. After 1000 training epochs, compared

Simulations corroborate the gain our proposed architecture and scheme yield, showing considerable improvement in terms of both attack detection accuracy and training speed. Possible directions for future work include assessing and optimizing the cooperation efficiency among the end, the edge, and the cloud, and extending the schemes for detecting machine-learning-based intelligent attacks.

to the non-cooperative case, the error rate in the cooperative case with cooperation period of 4 is reduced by 23 percent. At the same time, our proposed cooperative scheme outperforms traditional distributed machine learning and traditional federated learning by up to 16 percent and 19 percent, respectively, in terms of the detection error rate.

Consequently, the numerical results verify that our proposed architecture and schemes can benefit the end with higher attack detecting accuracy and training speed without needing full training data or redundant computing resources, and can improve the attack detection accuracy of the trained models in the edge simultaneously.

Conclusion

In this article, we propose a federated learning empowered end-edge-cloud cooperation framework for 5G HetNet security. The training schemes of the local attack detection models were designed for the end nodes and edge nodes, respectively. Based on federated learning, the detailed cooperative model training schemes are presented among the end, the edge, and the cloud. The cooperative schemes can make the nodes in distributed and heterogeneous networks cooperate efficiently and flexibly, and thus realize their full potential in detecting attacks. Extensive simulations corroborate the gain that our proposed architecture and scheme yield, showing considerable improvement in terms of both attack detection accuracy and training speed. Possible directions for future work include assessing and optimizing the cooperation efficiency among the end, the edge, and the cloud, and extending the schemes for detecting machine-learning-based intelligent attacks.

Acknowledgments

This work was partly supported by the National Key R&D Program of China (No. 2018YFE0117500), the Science and Technology Program of Sichuan Province, China (No. 2019YFG0534), and the EU H2020 Project COSAFE (No. MSCA-RISE-2018-824019).

References

[1] C. Miranda *et al.*, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks," *IEEE Trans. Info. Forensics Security*, vol. 15, 2020, pp. 2602–15.
[2] L. Tseng *et al.*, "Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture," *IEEE Network*, vol. 34, no. 1, Jan./Feb. 2020, pp. 16–23.
[3] L. Fernández Maimó *et al.*, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," *IEEE Access*, vol. 6, 2018, pp. 7700–12.
[4] M. Ahmed *et al.*, "Secrecy Ensured Socially Aware Resource Allocation in Device-to-Device Communications Underlaying HetNet," *IEEE Trans. Vehic. Tech.*, vol. 68, no. 5, 2019, pp. 4933–48.
[5] E. Anthi *et al.*, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet of Things J.*, vol. 6, Oct. 2019, pp. 9042–53.
[6] Y. Zuo *et al.*, "An Intelligent Anomaly Detection Scheme for Micro-services Architectures with Temporal and Spatial Data Analysis," *IEEE Trans. Cognitive Commun. and Networking*, 2020.
[7] B. Hussain *et al.*, "Mobile Edge Computing-Based Data-Driven Deep Learning Framework for Anomaly Detection," *IEEE Access*, vol. 7, 2019, pp. 137,656–67.
[8] Z. Zhou *et al.*, "Blockchain-Empowered Secure Spectrum Sharing for 5G Heterogeneous Networks," *IEEE Network*, vol. 34, no. 1, Jan./Feb. 2020, pp. 24–31.
[9] X. Lu *et al.*, "Cyber Insurance for Heterogeneous Wireless Networks," *IEEE Commun. Mag.*, vol. 56, no. 6, June 2018, pp. 21–27.
[10] Y. Lu *et al.*, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Trans. Industrial Informatics*, vol. 16, no. 6, 2020, pp. 4177–86.
[11] Y. Lu *et al.*, "Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems," *IEEE Network*, vol. 34, no. 3, May/June 2020, pp. 50–56.
[12] A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," *IEEE Commun. Mag.*, vol. 56, no. 2, Feb. 2018, pp. 169–75.
[13] G. Nguyen *et al.*, "Deep Learning for Proactive Network Monitoring and Security Protection," *IEEE Access*, vol. 8, 2020, pp. 19,696–19,716.
[14] Q. Yang *et al.*, "Federated Machine Learning: Concept and Applications," *ACM Trans. Intelligent Systems and Technology*, vol. 10, no. 2, 2019, pp. 1–19.
[15] I. Sharafaldin *et al.*, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *Proc. 4th Int'l. Conf. Info. Systems Security and Privacy*, 2018, pp. 108–16.

Biographies

Yunkai Wei (ykwei@uestc.edu.cn) is currently an associate professor with the School of Information and Communication Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, where he received his B. Eng., M. Eng., and Ph.D. degrees. He was also a visiting researcher at California Institute of Technology during 2013–2014. His research interests include machine learning, network security, wireless communications and networks, and the Internet of Things.

Sipei Zhou (spzhou@std.uestc.edu.cn) is a graduate student at the School of Information and Communication Engineering, UESTC. His research interests include network cyberspace security, and wireless communications and networks.

Supeng Leng (spleng@uestc.edu.cn) is a full professor and a Vice Dean in the School of Information & Communication Engineering, UESTC. He is also the leader of the Ubiquitous Wireless Networks research group. He received his Ph.D. degree from Nanyang Technological University, Singapore. His research focuses on resource, spectrum, energy, routing, and networking in the Internet of Things, vehicular networks, broadband wireless access networks, and the next generation intelligent mobile networks. He has published over 180 research papers and 4 books/book chapters in recent years. He got the Best Paper Award at three IEEE international conferences. He has served as an Organizing Committee Chair and TPC member for many international conferences, as well as a reviewer for over 10 international research journals.

Sabita Maharjan [SM'19](sabita@simula.no) received her Ph.D. degree in networks and distributed systems from the University of Oslo and Simula Research Laboratory, Norway, in 2013. She is currently an associate professor in the Department of Informatics, University of Oslo, and a senior research scientist at Simula Metropolitan Center for Digital Engineering, Norway. Her current research interests include vehicular networks and 5G, network security, smart grid communications, the Internet of Things, and computational intelligence.

Yan Zhang [F'20](yanzhang@ieee.org) is a full professor in the Department of Informatics, University of Oslo. He is an Editor of several IEEE journals, including *IEEE Communications Magazine*, *IEEE Network*, *IEEE Transactions on Green Communications and Networking*, *IEEE Communications Surveys & Tutorials*, and the *IEEE Internet of Things Journal*. His current research interests include next generation wireless networks leading to 6G and cyber physical systems. He is an IEEE VTS Distinguished Lecturer and IET Fellow. Since 2018, he has received the "Highly Cited Researcher" (top 1 percent by citations) award from Clarivate Analytics.