Journal of Computer Science and Cybernetics, V.38, N.3 (2022), 245–256
DOI no 10.15625/1813-9663/38/3/17094

JOINT POWER COST AND LATENCY MINIMIZATION FOR SECURE COLLABORATIVE LEARNING SYSTEMS

NGUYEN THI THANH VAN[1], VU VAN QUANG[2,*], NGUYEN CONG LUONG[2]

[1]*Faculty of Electrical and Electronic Engineering, Phenikaa University, Nguyen Trac Street, Yen Nghia Ward, Ha Dong District, Ha Noi, Viet Nam*
[2]*Department of Computer Science, Phenikaa University, Nguyen Trac Street, Yen Nghia Ward, Ha Dong District, Ha Noi, Viet Nam*

Abstract. This work investigates the update security model in a collaborative learning or federated learning network by using the covert communication. The covert communication (CC) uses the jamming signal and multiple friendly jammers (FJs) are deployed that can offer jamming services to the model owner, i.e., a base station (BS). To enable the BS to select the best FJ, i.e., the lowest cost FJ, a truthful auction is adopted. Then, we formulate an optimization problem that aims to optimize the transmission power, jamming power, and local accuracy. The objective is to minimize the training latency, subject to the security performance requirement and budget of the BS. To solve the non-convex problem, we adopt a Successive Convex Approximation algorithm. The numerical results reveal some interesting things. For example, the trustful auction reduces the jamming cost of the BS as the number of FJs increases.

Keywords. Federated learning, covert communication, latency minimization, trustfulness, auction.

1. INTRODUCTION

Collaborative learning or Federated Learning (FL) has emerged as a decentralized machine learning that addresses the privacy issue in the traditional machine learning [1]. In the FL system, mobile devices as workers cooperatively train a global model, i.e., a deep learning model, required by a server. The training can be implemented in multiple iterations to achieve a target accuracy. This however requires a number of communications between the mobile devices and the server. As a result, FL faces wireless security issues such as eavesdropping, jamming, and inference attacks [2].

There exist countermeasures which can be used to address the attacks. In particular, to combat with the eavesdropping attacks, cryptographic methods [3] are used to encrypt the trained models. To prevent jamming attacks, frequency hopping can be used in which the model communications between the server and the mobile devices are implemented on carrier frequencies that are not jammed. To combat with the inference attack, a differentially private SGD algorithm is applied on the model parameters [4].

*Corresponding author.
E-mail addresses: van.nguyenthithanh@phenikaa-uni.edu.vn (N.T.T. Van); quang.vuvan@phenikaa-uni.edu.vn (V.V. Quang); luong.nguyencong@phenikaauni.edu.vn (N.C. Luong).

However, each existing countermeasure is designed to address a specific attack, while multiple attacks can be launched simultaneously. For example, the eavesdropping attacker can both eavesdrop on the trained model and launch jamming attacks to the model communication. Hence, it is necessary to design a unified and costly security solution to address multiple types of attacks simultaneously.

Recently, a novel security method, namely covert communication (CC), has been effectively used for the wireless security. In general, the CC prevents a warden, e.g., an attacker or an eavesdropper, from detecting the data transmissions from the legitimate users. As the warden is not able to detect the data transmissions, it cannot launch various attacks such as eavesdropping attack, poisoning attack, and jamming attack. Due to its advantages, CC has been recently proposed to enhance the security of the FL system as presented [5]. In the work in [5], the CC based on jamming signal is used to assist the secure FL system.

Similar to [5], in this work, we adopt the CC based on jamming signal for the secure model updates in FL. However, differently from [5], we consider multiple FJs in the system model. The FJs offer jamming services with different jamming costs to the mobile devices, i.e., the workers. To minimize the jamming cost that the BS pays the FJs, we adopt a truthful auction. The truthful auction guarantees the truthfulness and allows the BS to select the best FJ with the lowest cost. Furthermore, we consider the budget of the BS, which is also investigated in [6]. Specifically, we investigate a secure FL system. In the system, a BS that is equipped with a server has a deep learning (DL) model needed to train. The BS broadcasts the DL model, i.e., global model, to multiple mobile devices. The devices cooperatively train the DL model using their local datasets and then upload their DL models, i.e., local models, to the BS. There exists a warden, called Willie, that aims to detect the model transmissions of the trained models of the mobile devices. To prevent the warden from detecting the model transmissions, a covert communication solution using artificial noise (AN) is used. In particular, multiple friendly jammers (FJs) are deployed to offer the jamming services to the BS. Using the AN causes a jamming cost to the BS, and thus we adopt the auction to select the best FJ with the lowest cost for the BS. Specifically, to motivate the FJs to submit their true cost, we propose to use a truthful reverse auction, i.e., namely second-price reverse auction (SPRA). Then, we formulate a problem that optimizes the transmission power of the mobile devices, the jamming power of the selected FJ, and the local accuracy at the mobile devices. The objective is to minimize the total training latency while guaranteeing the security performance requirement and budget of the BS. To solve the non-convex problem, we adopt a Successive Convex Approximation (SCA) algorithm. We would like to highlight that our work is significantly different from the previous work [6]. First, the work [6] only considers a single FJ, while our work considers multiple FJs that better support the mobile devices. Second, the work [6] does not consider the low jamming cost and the truthfulness of the FJs, while our work does. Third, the work [6] does not introduce the auction mechanism, while our work does. Fourth, the work [6] only evaluates the FL latency versus the number of mobile devices and budget. Meanwhile, apart evaluating the FL latency versus the number of mobile devices and budget, our work evaluates the jamming cost versus the number of FJs and the covert probability versus the transmit and jamming power. Finally, our work introduces some baselines to demonstrate the proposed algorithm, while the work [6] does not.

The paper is organized as follows. Section 2 presents a secure FL model with multiple FJs,

the fundamentals of SPRA, the covert communication for the FL system, and the problem formulation. Section 3 represents the SCA algorithm. Section 4 discusses simulation results, and Section 5 concludes the paper.

2. SYSTEM MODEL

2.1. Network model

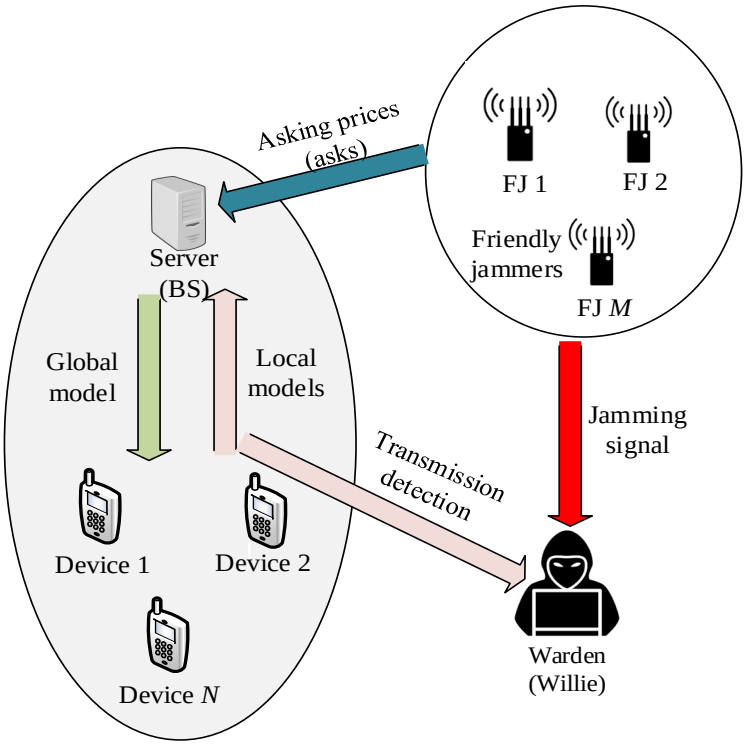

Figure 1: Covert communication for a federated learning system with assistance of multiple friendly jammers (FJs).

An FL system is shown in Fig. 1. In the system, there are N mobile devices, a BS (equipped with a server), M FJs, and a warden. We denote $\mathcal{N}$ as the set of the devices. The BS has a global model, and the devices cooperatively train the global model using their datasets. The warden attempts to detect the transmissions of local model from the devices, e.g., to extract the sensitive information from the models. To confuse the warden, the BS rends one of the FJs to transmit the AN (jamming) signal. Then, the BS will pay a jamming service cost to the selected FJ. Due to the limited budget, the BS should select the FJ with the lowest jamming cost. One question is that how the BS can select and pay the best FJ while motivating the FJs to offer the jamming service. In particular, if the BS pays a high cost to the selected FJ, the high cost occurs to the BS. However, if the BS pays a low cost to the selected FJ, the FJs has no incentive to offer the jamming service [7]. In the following, we propose to adopt an auction for the FJ selection and the payment of the BS.

2.2. Second-price reverse auction (SPRA) for FJ selection and payment

This section discusses how the second-price reverse auction (SPRA) is used for the BS to select the best FJ and to determine the price paid to the FJ.

2.2.1. Common terminologies used in auction theory

An auction is a type of trading mechanism of buying and selling items. In the area of networking, the items can be energy resources, e.g., energy units, or bandwidth resources, e.g., bandwidth blocks or bandwidth units, or a network service. The auction owns its rules that select the best winner and determine the corresponding payment. To further understand the use of auction in our work, we introduce basic terminologies as follows [8]:

- *Bidder and seller:* This is buyer who is willing to buy the item. In our work, the bidder is the BS that wants to buy the jamming energy resource or jamming service from the FJs to guarantee the covertness of the FJs. Meanwhile, the seller offers an item or a service to the buyers. In our work, there are multiple sellers that are the FJs.
- *Auctioneer:* The auction is conducted by an auctioneer. In our work, the auctioneer is also the buyer, i.e., the BS, that decides the best FJ and determines the corresponding payment.
- *Price:* This is the price or the cost that the BS needs to pay the selected FJ.

2.2.2. Second-price reverse auction (SPRA)

There are several types of auctions. The two most common auctions are the forward auction and the reverse auction. In the forward auction, there are multiple buyers that compete a single item. For this, the bidders bid for the item by offering high prices. On the contrary, in the reverse auction, there are multiple sellers and a single buyer. The sellers compete with each other by submitting their prices or asks to the seller. As such, the buyer can buy the item with the low price.

Note that with the reverse auction, the buyer can buy the item with the lowest cost. However, the sellers are rational, i.e., self-fish and they can untruthfully submits their asks. In other words, they have an incentive to submit their high asks so that they will receive higher payment from the buyer if they win the auction. In this case, the buyer will pay a higher cost to the winner. To address this issue, the buyer can adopt the second-price reverse auction (SPRA) in which the buyer will pay the winner with a price that is equal to the second-lowest price of the sellers. By this way, the seller (if it wins the auction) will be paid with a price higher than it expected. Thus, the sellers have no incentive to submit their untruthful asks. Given this advantage, in this work, we propose to use the SPRA for the FJ selection and payment. This will be further presented in the next section.

2.2.3. FJ selection and jamming payment based on SPRA

The FJ selection process and jamming payment based on SPRA is described as follows. Assume that the FJs have the same maximum jamming power. Each FJ m submits a cost per power unit c_m, e.g., \$ 0.2 per 1 mW, to the BS. Here, c_m means the cost that FJ m is willing to sell the power unit. In auction theory, the cost of c_m is called "ask" or "asking

price". After receiving the asks submitted from M FJs, the BS shorts the FJs in a descending order of their prices. The BS then selects the FJ with the lowest price, denoted by FJ j, as the winner as follows

$$j = \arg\min_{m} c_m. \tag{1}$$

It is natural that the FJs may not submit their true values or we say the FJs have not trustfulness. For example, the real cost for a power unit of FJ m is \$0.2 per 1 mW, but the FJ will not submit exactly \$0.2. Otherwise, the FJ will submit an ask higher than \$0.2, say \$0.25 to gain its benefit. As a result, the BS needs to pay a higher price to the FJ if FJ wins. To guarantee that the FJs submit their true costs, the BS uses the second-price reverse auction (SPRA) as described in Section 2.2.2. In the SPRA, the BS will select the FJ with the lowest cost, i.e., the lowest ask, as the winner. Then, the BS will pay the winner with the second-lowest price. As such, the winner will receive a price that is larger than the cost it submits. For example, if we have two FJs, FJ 1 submits an ask of \$0.2, and FJ 2 submits an ask of \$0.23. Then, according to SPRA, the BS will select FJ 1 as the winner of the aution. Also, the BS will pay FJ 1 a price of \$0.23. Since \$0.23 > \$0.2, FJ 1 is already happy, and thus the FJ will not have an incentive to submit the untrustfull ask, e.g., \$0.3. We denote this jamming charge as c_j. For simplification, we also denote the winning FJ as FJ, i.e., the FJ is the winner of the auction and pay.

2.3. Federated learning

We denote $d_{i,s}$, $d_{j,s}$, $d_{i,w}$, and $d_{j,w}$ as the distances from device i to the BS, from the FJ (the winning FJ) to the BS, from device i to the warden, and from the FJ to the warden, respectively. Also, we denote $h_{i,s}$ and $h_{i,w}$ as the channels between device i and the BS and between the device and the warden, respectively. Furthermore, the channels between the jammer and the BS and the jammer and the warden are denoted by $h_{j,s}$ and $h_{j,w}$, respectively. Here, $h_{i,s}$, $h_{i,w}$, $h_{j,s}$, and $h_{j,w}$ follows $\mathcal{CN}(0,1)$. In the FL system, the BS has a global model that needs to be trained and the corresponding global accuracy of ι. Let I_0 be the total of global iterations to achieve the global accuracy. Then, I_0 can be approximated by $\frac{a}{1-\eta}$ [9] where $a = \frac{2L^2}{\gamma^2\xi}\ln\frac{1}{\iota}$. Here, ξ is a constant value and L and γ are the parameters related to the FL loss function. Assume that each device i has D_i data samples. The model trained by each device is namely local model that has the same size (in bits) with the global model. We can denote S as the local model size (also global model size).

2.4. Covert communication-enabled federated learning

The overall training of FL includes three steps: local training at the devices, local model transmissions of the devices, global model aggregation of the BS, and global model transmission of the BS. In this work, the covert communication is adopted during the model transmission step of the FL process. For convenience, we first introduce the FL training latency and then we formulate the optimization problem of the covert communication-enabled FL.

2.4.1. Local training

According to [9], the time required for the local training at iteration i is

$$\tau_i = \frac{A_i \log_2(1/\eta)}{f_i}, \forall i \in \mathcal{N}, \tag{2}$$

where $A_i = vC_iD_i$ with C_i (cycles/bit), f_i presents the computation capacity of device i, and η is the local accuracy. We can also determine the number of local iterations required for the local computation at each device that is approximately $v \log_2(1/\eta)$, where $v = \frac{2}{(2-L\delta)\delta\gamma}$ with δ being the step size of training the local model [9].

2.4.2. FL latency

After the devices perform their local training, they can transmit the local models to the BS or keep silent to reduce the detection risk from the warden. Let $\Psi_{i,0}$ be the scenario in which device i does not transmit its model and $\Psi_{i,1}$ be the scenario in which device i decides to transmit its model. We also denote p_i as the transmission power that device i transmits its local model to the BS (when it decides to transmit the local model). We denote $\mathbb{P}_{\psi_{i,1}}$ as the probability that device i transmits its local model. Meanwhile, the winning FJ, i.e., the FJ is selected by the BS in the auction process, performs the jamming service by continuously transmitting jamming signals. We denote p_j as the jamming power that the FJ transmits. When the FJ transmits the jamming signal to cause interference to the warden, the jamming signal also causes the interference to the BS. Therefore, based on equation (4) in [10], the SINR at the BS is $\zeta_i = 0$ if $\Psi_{i,0}$ and $\zeta_i = \frac{p_i|h_{i,s}|^2}{\varrho(d_{j,s}^{\alpha}\sigma_{i,s}^2 + p_j|h_{j,s}|^2)}$ if $\Psi_{i,1}$, where $\varrho = (\frac{d_{i,s}}{d_{j,s}})^{\alpha}$ and α presents the path-loss exponent. Then, the data rate obtained by device i is determined by

$$r_i = \mathbb{P}_{\psi_{i,1}} \frac{B}{N} \log_2 \left(1 + \frac{p_i|h_{i,s}|^2}{\varrho(p_j|h_{j,s}|^2 + d_{j,s}^{\alpha}\sigma_{i,s}^2)}\right), \tag{3}$$

where $\mathbb{P}_{\psi_{i,1}}$ presents the probability of data transmission to the BS, B presents the total bandwidth of the FL system, and $\sigma_{i,s}^2 = B/N\sigma_0^2$ where σ_0^2 is the Gaussian noise, and B/N assigned to each device. Then, the model transmission time of device i is

$$t_i = \frac{S}{r_i}. \tag{4}$$

The training latency of device i over I_0 iterations is given by $T_i = \frac{a}{1-\eta}(\tau_i + t_i)$. The training latency is the maximum latency among the devices.

2.4.3. False alarm and miss detection probabilities

When device i transmits its local model to the BS, i.e., $\Psi_{i,0}$ is true, and the warden judges $\Psi_{i,1}$, then we say that a false alarm (FA) occurs. We denote $\mathbb{P}_{i,FA}$ as FA probability. Similarly, , a miss detection (MD) occurs when the warden judges $\Psi_{i,0}$ while $\Psi_{i,1}$ is true. We denote $\mathbb{P}_{i,MD}$ as the MD probability. Clearly, from the warden's perspective, $\mathbb{P}_{i,FA} + \mathbb{P}_{i,MD}$ should be minimum, meaning the warden correctly judges the local model transmission of

the device. For this, the warden determines a power threshold, i.e., denoted by η, by solving the following problem

$$\arg\min_{\vartheta} \mathbb{P}_{i,FA} + \mathbb{P}_{i,MD}. \tag{5}$$

We denote $\sigma_{i,w}^2$ as the background noise at the warden. Then, according to, the power threshold is found by solving the warden's optimization problem in (5). Similar to the method which is presented in Appendix B in [10], we have

$$\vartheta_i^* = \left(\frac{\psi_{i,0}\psi_{i,1}}{\psi_{i,0} - \psi_{i,1}}\right) \ln\left(\frac{\psi_{i,0}}{\psi_{i,1}}\right) + \sigma_{i,w}^2, \tag{6}$$

where $\psi_{i,0} = \dfrac{p_j}{d_{j,w}^{\alpha}}$ and $\psi_{i,1} = \dfrac{p_j}{d_{j,w}^{\alpha}} + \dfrac{p_i}{d_{i,w}^{\alpha}}$.

Given ϑ_i^*, from the BS's perspective, it aims to maximize $\mathbb{P}_{i,FA}(\vartheta_i^*) + \mathbb{P}_{i,MD}(\vartheta_i^*)$. Note that the BS may not know ϑ_i^*. However, in practice, we can assume the worse case in which the warden uses ϑ_i^* as the optimal value to minimize its error detection. In this case, we thus can assume that ϑ_i^* is known to the BS. Then, the BS tries to find the jamming power from the FJ and the transmit power of the devices so as to satisfy the following condition

$$\text{For any } \epsilon \geq 0,\ \mathbb{P}_{i,FA} + \mathbb{P}_{i,MD} \geq 1 - \epsilon,\ \forall i \in \mathcal{N}. \tag{7}$$

3. PROBLEM FORMULATION AND ALTERNATIVE ALGORITHM

In this work, we aim to minimize the FL latency while guaranteeing the security performance, i.e., the CC constraint. Thus, we formulate the problem as follows

$$\min_{\eta, \mathbf{p}_i = [p_i, p_j]} \max_{i \in \mathcal{N}} T_i(\eta, \mathbf{p}_i), \tag{8a}$$

$$\text{s.t. } p_i \leq p_i^{\max},\ \forall i \in \mathcal{N}, \tag{8b}$$

$$p_j \leq p_j^{\max}, \tag{8c}$$

$$\mathbb{P}_{i,FA}(\vartheta_i^*) + \mathbb{P}_{i,MD}(\vartheta_i^*) \geq 1 - \epsilon,\ \forall i \in \mathcal{N}, \tag{8d}$$

$$p_j c_j \leq \chi, \tag{8e}$$

$$0 \leq \eta \leq 1, \tag{8f}$$

$$\vartheta_i^* \text{ obtained by (6)}, \tag{8g}$$

where $p_i^{\max}$ and $p_j^{\max}$ are the power budgets of device i and the jammer, c_j is the price per power unit (c_j is set by the jammer), and χ is the budget of the server. The constraint in (8d) is the CC requirement. The constraint in (8e) refers to the budget constraint, i.e., the maximum price that the server can pay the jammer for the jamming service, and the constraint in (8f) represents the range of the local accuracy of the devices.

In the optimization problem given in (8), the objective function and the constraint in (8d) are nonconvex. Thus, the problem in (8) is nonconvex. While no exact algorithm can be proposed to solve it, we adopt the alternative algorithm given in [5] to solve it. Similar to [5], we use a new variable $\rho > 0$ such that $\frac{1}{\eta} = 1 + \frac{1}{\rho}$. Correspondingly, the problem (8)

is rewritten as follows

$$\min_{\rho,\mathbf{p}_i=[p_i,p_j]} \max_{i\in\mathcal{N}} T_i(\rho,\mathbf{p}_i), \tag{9a}$$

$$\text{s.t (8b), (8c), (8d), (8e),}$$

$$\text{and } \rho > 0. \tag{9b}$$

To solve the problem in (9) with low complexity, we divide (9) into two sub-problems, and then the sub-problems are solved in an iteration manner. For this, we denote $(\rho^{(\kappa)}, \mathbf{p}_i^{(\kappa)})$ as a feasible point of (9) that is found in iteration $(\kappa-1)$. In iteration κ, we fix $\rho = \rho^{(\kappa)}$ and determine $\mathbf{p}_i^{(\kappa+1)}$, then we fix $\mathbf{p}_i = \mathbf{p}_i^{(\kappa+1)}$ to determine $\rho^{(\kappa+1)}$.

First, we fix $\rho^{(\kappa)}$ and optimize the transmit power and jamming power. For this, we have the following sub-problem

$$\min_{\mathbf{p}_i=[p_i,p_j]} \max_{i\in\mathcal{N}} T_i(\mathbf{p}_i),$$

$$\text{s.t (8b), (8c), (8d), and (8e).} \tag{10}$$

The sub-problem given in (10) is still nonconvex, and we can use the SCA to solve it. This can be implemented similar to the SCA algorithm in [5].

In the second sub-problem, we fix the transmit power and jamming power $\mathbf{p}_i^{(\kappa)}$ while optimizing ρ. Accordingly, we have the following sub-problem

$$\min_{\rho} \max_{i\in\mathcal{N}} T_i(\rho),$$

$$\text{s.t (9b).} \tag{11}$$

The problem in (11) can be easily proven as convex problem by using the second derivative method. Thus, the standard CVX can be used to solve it.

4. PERFORMANCE EVALUATION

In this section, we present simulation results to evaluate the proposed algorithm. For the evaluation purpose, we assume that the number of devices participating the FL system is $N = 30$. The number of FJs is $M = 5$. Note that these values can be varied as discussed later. Each mobile device i has a power budget of 10 dBm and a dataset of 500 data samples. The budget for purchasing the jamming power of the BS is \$30, i.e., the maximum cost that the BS can pay the FJ. The asking prices, i.e., the asks, of the FJs (i.e., $c_m, \forall m \in \mathcal{M}$), are randomly taken within $[0.2, 0.5]$. Other simulation parameters are listed in Table 1.

We introduce two algorithms as baselines. The first algorithm is denoted as p-CCFL in which we fix the local accuracy $\eta = 1/2$ and we optimize $\mathbf{p}_i$. The second algorithm is denoted as η-CCFL in which we fix $\mathbf{p}_i$ and we optimize η.

First, we compare the FL latency obtained by the algorithms as illustrated in Fig. 2. As seen, the proposed algorithm outperforms the baselines in terms of training latency. Especially, when the number of devices increases, the performance gap increases. This shows that the proposed algorithm is effective and scalable. Note that with the increase of number of devices, the training latency obtained by all the algorithms increases due to the smaller division of the bandwidth B.

Table 1: Simulation parameters

Parameters	Value	Parameters	Value
$\mathbb{P}_{\psi_1}$	0.7	S	28.1 kbits
ϵ	0.1	α	2.5
$p_i^{\max}$, $p_j^{\max}$	10 dBm	$f_i^{\max}$	2 GHz
ι	10^{-3}	δ, ξ	1/10
B	20 MHz	D_i	500
M	5	c_m	$\mathcal{U}[0.2, 0.5]$

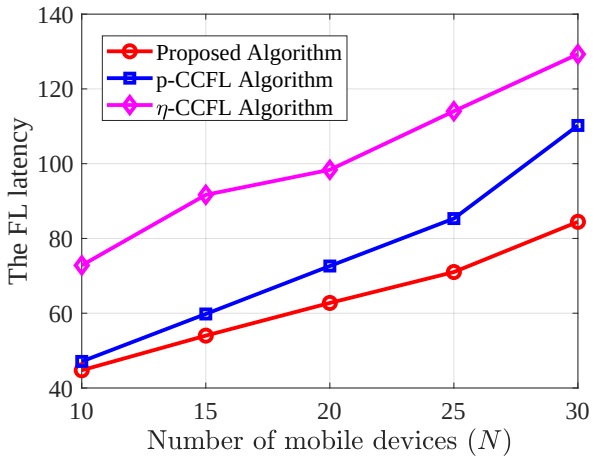

Figure 2: FL latency as the number of devices varies

Apart from the change of the number of devices, the number of FJs may vary over time. Thus, it is worth discussing the impact of the number of FJs on the jamming cost that the BS needs to pay for the jamming service. As shown in Fig. 3, the jamming cost that the BS needs to pay with the proposed algorithm is lower than that of the η-CCFL algorithm. Especially, when the number of FJs M increases, the jamming cost of the three algorithms decreases due to the following reason. As M increases, there are more FJs in the jamming service market. Thus, more FJs compete on the jamming cost with each other. Therefore, the BS has a higher probability to select the FJ with the low jamming cost. As a result, the jamming cost that the BS pays is lower as the number of FJs increases.

Note that the BS has a budget that is the maximum payment it can pay the FJ. Therefore, it is exciting to discuss the impact of the BS's budget χ on the FL latency. As shown in Fig. 4, as the budget of the BS varies, the FL latency obtained by the three algorithms changes. In particular, as the BS's budget increases from $\chi = 0.1$ to $\chi = 0.9$, the FL latency decreases. The fact is that the BS with the low budget buys a lower jamming power from the FJ, i.e., the winning jammer. Given the low jamming power, the devices decreases their transmission power to avoid the transmission detection from the devices. As a result, the SINR at the BS decreases and the FL latency increases. As the budget is high, the FL latency seems not to change. It is so because the BS already finds an optimal jamming power for the problem (8) with the low budget, and it does not need more jamming power. To guarantee the security requirement, the devices should keep the transmit power unchanged, and thus

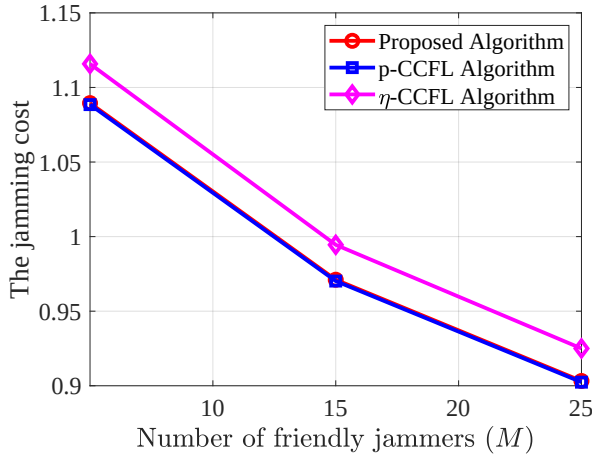

Figure 3: Jamming cost as the number of FJs varies

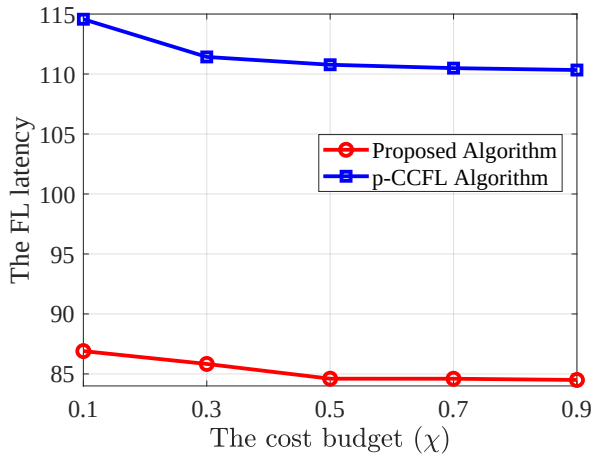

Figure 4: FL latency versus the BS's budget

the FL latency does not change. Next, we investigate how the security performance in terms of covert probability changes as the jamming power p_j varies, which is shown in Fig. 5. As seen, as $p_j/p_j^{\max}$ increases, the security performance increases. The reason is that as the increase of p_j increases the interference occurred to the warden. As a result, the warden is hard to detect the transmissions of the devices. Even though, the increase of p_j decreases the SINR at the BS.

5. CONCLUSIONS

We have investigated the secure local model transmissions of the devices in the FL system. Specifically, we propose a covert communication algorithm based on artificial noise that prevents the warden from detecting the local model transmissions from the mobile devices to the BS. We consider a general case in which multiple FJs are deployed to offer the jamming service to the BS. Then, we propose to adopt the second-price reverse auction that allows the

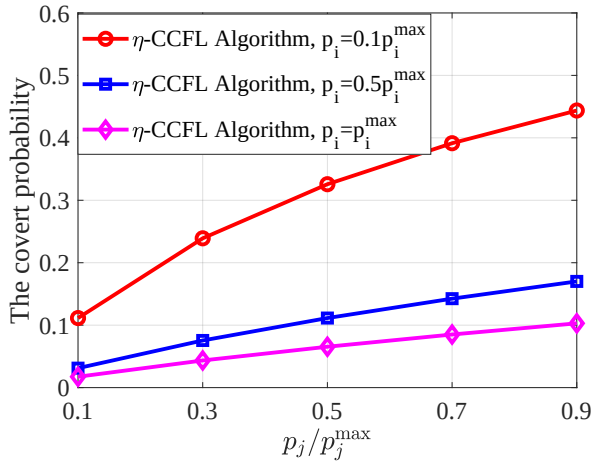

Figure 5: Covert probability versus $p_j/p_j^{\max}$

BS to select the FJ with the low cost while guaranteeing the trustfulness of the FJs. After that, we formulate the problem for the BS. The problem aims to minimize the training latency subject to the security threshold and the BS's budget. An SCA algorithm is deployed to solve the problem. The simulation results are provided that reveals some interesting things. For example, using the second-price reverse auction can further reduce the jamming cost of the BS as the number of FJs increases.

ACKNOWLEDGMENT

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.02-2019.305.

REFERENCES

[1] J. Tan, Y.-C. Liang, N. C. Luong, and D. Niyato, "Toward smart security enhancement of federated learning networks," *IEEE Network*, vol. 35, no. 1, pp. 340–347, Jan./Feb. 2020.

[2] Z. Yang, M. Chen, W. Saad, C. S. Hong, and M. Shikh-Bahaei, "Energy efficient federated learning over wireless communication networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1935–1949, Mar. 2020.

[3] S. Dey, "Sd-ei: A cryptographic technique to encrypt images," in *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. IEEE, 2012, pp. 28–32.

[4] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 308–318.

[5] N. T. T. Van, N. C. Luong, H. T. Nguyen, F. Shaohan, D. Niyato, and D. I. Kim, "Latency minimization in covert communication-enabled federated learning network," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 13 447–13 452, 2021.

[6] Y.-A. Xie, J. Kang, D. Niyato, N. T. T. Van, N. C. Luong, Z. Liu, and H. Yu, "Securing federated learning: A covert communication-based approach," *IEEE Network*, 2022. Doi: 10.1109/MNET.117.2200065.

[7] N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," in *IEEE International Conference on Communications*, 2018, pp. 1–6.

[8] N. C. Luong, P. Wang, D. Niyato, Y. Wen, and Z. Han, "Resource management in cloud networking using economic analysis and pricing models: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 954–1001, 2017.

[9] Z. Yang, M. Chen, W. Saad, C. S. Hong, and M. Shikh-Bahaei, "Energy efficient federated learning over wireless communication networks," *IEEE Transactions on Wireless Communications*, 2020.

[10] M. Forouzesh, P. Azmi, N. Mokari, and K. K. Wong, "Covert communications versus physical layer security," *arXiv preprint arXiv:1803.06608*, 1803.

Received on April 26, 2022
Accepted on September 16, 2022