

PPT: A Privacy-Preserving Global Model Training Protocol for Federated Learning in P2P Networks

Qian Chen, Zilong Wang, *Member, IEEE*, Wenjing Zhang, and Xiaodong Lin, *Fellow, IEEE*

Abstract—The concept of Federated Learning (FL) has emerged as a convergence of machine learning, information, and communication technology. It is vital to the development of machine learning, which is expected to be fully decentralized, privacy-preserving, secure, and robust. However, general federated learning settings with a central server can't meet requirements in decentralized environment. In this paper, we propose a decentralized, secure and privacy-preserving global model training protocol, named PPT, for federated learning in Peer-to-peer (P2P) Networks. PPT uses a one-hop communication form to aggregate local model update parameters and adopts the symmetric cryptosystem to ensure security. It is worth mentioning that PPT modifies the Eschenauer-Gligor (E-G) scheme to distribute keys for encryption. In terms of privacy preservation, PPT generates random noise to disturb local model update parameters. The noise is eliminated ultimately, which ensures the global model performance compared with other noise-based privacy-preserving methods in FL, e.g., differential privacy. PPT also adopts Game Theory to resist collusion attacks. Through extensive analysis, we demonstrate that PPT various security threats and preserve user privacy. Ingenious experiments demonstrate the utility and efficiency as well.

Index Terms—fully decentralized, federated learning, peer-to-peer networks, privacy-preserving, security, efficiency.

I. INTRODUCTION

MODERN machine learning (ML) is achieving unprecedented performance in natural language processing [1], computer vision [2], data mining [3], etc. However, along with the growing social privacy awareness and the rapid growth of data, ML seems to be hard to break new ground. Especially, the General Data Protection Regulation (GDPR) [4] enforces strict limitations on handling users' private data. Both industry and academia began to find a way performing ML with the demand of privacy. Recently, the concept of federated learning (FL) [5] has emerged and been recognized as the state-of-the-art distributed ML system, which provides privacy, security, communication efficiency, and improved robustness. FL allows users to collectively reap the benefits of shared models trained from rich data without the need to centrally store it. Massive data containing sensitive information, such as religion, income and e-mail, never leaves the users' devices.

A general FL system consists of two parties: a central server and a group of clients. The central server includes a coordinator and an aggregator. The aggregator aggregates

the local training results and updates the global model under the control of the coordinator, as shown in Fig. 1. At the beginning of an FL model training round, the central server distributes a pre-trained model. Subsequently, clients train the model using their local data and upload their model update parameters to the aggregator. Through aggregating the model update parameters, the central server updates the global model. The way of aggregating model update parameters reduces the communication overhead greatly, compared with collecting training data. To defend against powerful attackers obtaining sensitive information by executing model inversion attacks [9], FL system adopts some privacy-preserving techniques when uploading the model update parameters. Homomorphic Encryption (HE) [10], [11], Differential Privacy (DP) [12], and Secure Multi-Party Computation (MPC) [13] are the common privacy-preserving techniques in FL.

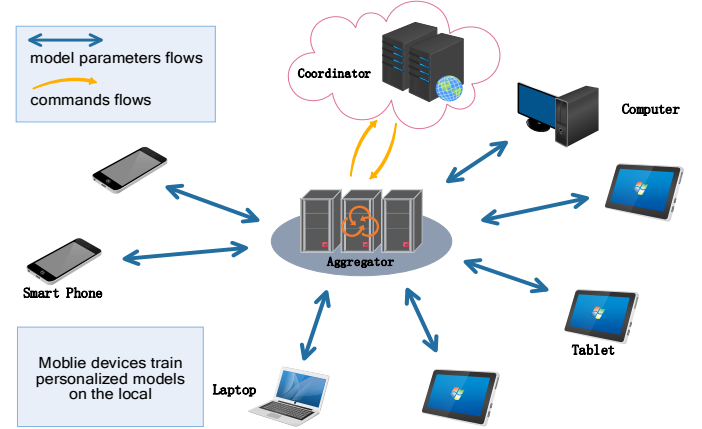


Fig. 1. Federated Learning with Central Server.

With the advantages of privacy preservation and communication efficiency, today's FL seems to be practical. However, in practice, clients are usually distributed in Peer-to-peer networks [17], such as Smart Home, Internet of Things, and Ad. Hoc. There are large amounts of clients not connected with a central server directly, due to the geographical location, signal strength, and other possible reasons. Although this part of clients can communicate with each other, they can't upload the model update parameters to a central aggregator directly. For example, the devices in Smart Home are usually not connected to a smartphone, which plays the role of an aggregator, in day time. It means a lot of time that could be used for aggregation will be wasted.

Fortunately, a central server could not be essential in FL. As demonstrated by Lian *et al.* [18], the central server may

Qian Chen and Zilong Wang are with the State Key Laboratory of Integrated Service Networks, School of Cyber Engineering, Xidian University, Xi'an, China (e-mail: xidianqianchen@gmail.com; zlwang@xidian.edu.cn).

Wenjing Zhang and Xiaodong Lin are with the School of Computer Science, University of Guelph, Guelph, Canada (e-mail: wzhang25@uoguelph.ca; xlin08@uoguelph.ca).

even become a bottleneck when the number of clients is very large. The survey in [19] also proposes a decentralized environment could motivate the design of the next generation of FL systems. Subsequently, a series of FL frameworks and algorithms without a central aggregator was proposed. Roy *et al.* [20] present BrainTorrent, a new FL framework in the highly dynamic P2P environment. Ramanan *et al.* [21] propose a blockchain based aggregator free FL framework, BAFFLE, which achieves high scalability and computational efficiency in a private Ethereum network. Lu *et al.* [22] propose a fully decentralized FL framework by leveraging two classic non-convex decentralized optimizations. Lalitha *et al.* [23] considers the problem of training a machine learning model in a fully decentralized framework. The proposed algorithm generalizes the prior works on FL and obtains a theoretical guarantee (upper bounds) that the probability of error and true risk are both small for every participant. Dubey *et al.* [24] devise FEDUCB for decentralized (peer-to-peer) FL to solve the contextual linear bandit problem. A fully decentralized FL approach proposed in [25] introduces a concept of student and teacher roles for model training.

However, all the above advanced decentralized works only present frameworks or algorithms. A formal description of decentralized FL settings and a general model training protocol are still absent. In this paper, the federated learning without a fully connected central server we refer to as *federated learning (FL) in peer-to-peer (P2P) networks*. We are interested in how to train a global model in the context of *FL in P2P networks* under the premise of privacy-preservation and security. Therefore, we design a Privacy-Preserving global model Training (PPT) protocol for *FL in P2P networks*. PPT generates a random noise for local model disturbance to guarantee the privacy. And the noise will be eliminated ultimately, which ensure the global model performance. PPT also distributes communication keys for encrypted communication to enhance the security. Besides, PPT adopts Game Theory method to resist collusion attacks. And a broadcasting method is used throughout for the robustness of the system. The main contributions of this paper are as follows:

Federated learning in P2P networks. We design a privacy-preserving global model training protocol, PPT, in the context of *FL in P2P networks*. To the best of our knowledge, this is the first collaboratively training protocol in the context of *FL in P2P networks*. Following our PPT protocol, a group of clients connected in P2P networks can collaboratively train a global machine learning model privately and securely. And the global model performance is surely better than other FL aggregation methods using noise-disturbance-based privacy-preserving techniques, e.g., DP.

Security and privacy-preserving protocol. We analyze the security strength and privacy-preservation ability of PPT. In particular, we analyze the connectivity of the communication key establishment scheme, which is indispensable for the security of data transmission.

Experimental evaluation. We evaluate the performance of the proposed PPT protocol by training a spam classification model on two real-world datasets, i.e. Trec06p and Trec07. We also research the client dropout situation to prove the

robustness against the dropout problem. Experimental results show that the proposed protocol is more efficiency than Google's Secure Aggregation[].

The rest of the paper is organized as follows. Section II demonstrates some primitive concepts. The system model, security requirements, and the design goal are formalized in Section III. In Section IV, we design the PPT protocol. In Section V, we analyze the security and privacy-preservation of PPT, followed by the experimental design and the results and performance evaluation in Section VI and VII, respectively. The limitation and future work are shown in Section VIII. Finally, we draw our conclusions in Section IX.

II. PRELIMINARIES

In this section, we briefly describe the data transmission form in P2P networks, the model training process, and the key pre-distribution scheme in the proposed PPT protocol.

A. Peer-to-peer networks and data transmission

Peer-to-peer (P2P) networks were popularized by file sharing systems such as the music-sharing application Napster. A P2P network is a distributed application architecture that tasks or workloads are partitioned between clients. Clients are equally privileged, equipotent participants. Different from Client-server (CS) networks, P2P networks, in which interconnected clients share resources amongst each other without the usage of a centralized administrative system, don't need central coordination by servers or stable hosts.

Data transmission in P2P networks usually follows a P2P transmission protocol, i.e., a sender upload the data, then any client connected to the sender can download the data directly. The transmission form is obviously efficient compared with CS networks.

B. Stochastic gradient descent and model training

Stochastic gradient descent (SGD) [28] is an iterative method for optimizing an objective function. In modern machine learning, SGD is usually regarded as a stochastic approximation of gradient descent optimization for loss function. Especially when the features are high-dimensional, SGD reduces the computational burden and achieves faster iterations to convergence.

In the FL context, n clients execute FederatedAveraging (or FedAvg) [5] algorithm. That is, each client executes a fixed number of iterations of SGD on the current model using its local data, then the central server takes a weighted average of the resulting local models to update the global model. The global model update process is demonstrated as

$$M^{R+1} \leftarrow \sum_{i=0}^{n-1} \frac{\omega_i}{\omega} m_i^R, \quad (1)$$

where M^{R+1} is the updated global model in the R th round, and m_i^R is the local model. The weights of the local model when aggregating are composed of the local training set size ω_i and the sum of local training set sizes $\omega = \sum_{i=0}^{n-1} \omega_i$.

C. Eschenauer-Gligor scheme

Eschenauer-Gligor(E-G) scheme [29] is first proposed as a random key pre-distribution scheme for distributed sensor networks. The basic idea is that clients randomly pick a certain number of keys from a large key pool and use the same keys as the communication keys with other clients. As a key-management scheme, the E-G scheme requires memory storage for only few tens to a couple of hundred keys and provides similar security and superior operational properties comparing to pair-wise private key-sharing schemes.

A typical E-G scheme consists of the following three phases:

- i) *Phase 1, key pre-distribution*: A trusted central server generates a large key pool containing η keys and key identifiers (IDs) offline. Each client randomly extracts l keys from the key pool with replacement to establish its own key ring and stores the key ring locally.
- ii) *Phase 2, shared-key discovery*: Each client broadcasts the lists of identifiers in the key ring to discover the same keys, called shared-keys, with its neighbor clients.
- iii) *Phase 3, path-key establishment*: A third-party client assigns a path-key to the pairs of clients that are connected but sharing no keys after the shared-key discovery phase.

III. SYSTEM MODEL, SECURITY REQUIREMENT AND DESIGN GOAL

In this section, we formalize the system model, security requirements, and identify our design goal.

A. System model

In the context of *FL in P2P networks*, all clients c_i distributed in P2P networks are potential clients. We mark the clients willing to participate global model training as target clients. And only a small part (even if one client) of them are connected to an aggregator directly. In the system model, we mainly focus on how to collaboratively train a global machine learning model among target clients. Every target client u_i trains a local model m_i using a central original model M and its own data, where $i = 0, 1, \dots, n-1$. The local training processes can be seen as executing stochastic approximation of gradient descent, i.e., SGD, for the central original model. A local update to the original model by a target client can be considered a product of a gradient and a step size. In this paper, we simply define the local model update parameters as x_i and denote as:

$$x_i = m_i - M \quad (2)$$

Considering the impact of different local models on the global model, different weights ω_i are set for corresponding local model updating parameters. Thus the global model update process is demonstrated as:

$$M^{new} = \frac{\sum_{i=0}^{n-1} \omega_i x_i}{\sum_{i=0}^{n-1} \omega_i} + M, \quad (3)$$

where M^{new} is the updated global model. We illustrate the system model in the left part of Fig. 2.

Communication model. The process of aggregating data can be easily finished in CS networks, as all clients just need to upload x_i to a central aggregator. When coming to P2P networks, it seems hard to transmit data to an aggregator, especially for clients not connected to the aggregator directly. However, a client can transmit the local model update parameters to a one-hop neighbor (neighbor client) directly within its communication range. The recipient adds its own data and transmits the aggregated data to its one-hop neighbor sequentially. We define this kind of transmission form as *one-hop transmission*.

B. Security requirements

Security and privacy preservation are crucial for the success of *FL in P2P networks*. In our security model, we consider the aggregator and clients are honest but curious. That is, local model update parameters are considered private. Meanwhile, there exists an adversary \mathcal{A} aiming to broke the global model training process. In addition, the adversary \mathcal{A} could also launch active attacks to threaten the data integrity. More seriously, two adversaries \mathcal{B} and \mathcal{C} could execute collusion attacks [27] to eavesdrop on the model update parameters. For instance, the upstream and downstream clients of a client u_i are adversaries \mathcal{B} and \mathcal{C} . \mathcal{B} transmits its data $x_{\mathcal{B}}$ to $u_{\mathcal{C}}$ directly after $u_{\mathcal{C}}$ receives the data $x_{\mathcal{B}} + x_i$ from u_i . Whereupon, $u_{\mathcal{C}}$ can calculate the data x_i . We illustrate the adversary model in the right part of Fig. 2. To prevent adversaries from learning the private model update parameters and to defend against malicious actions, the following security requirements should be satisfied.

Confidentiality. Protect individual local model update parameters from anyone but the client itself. Even the aggregator can only read the aggregated results rather than individual local model update parameters. Moreover, the parameter privacy will not be compromised even if there is a collusion attack.

Authentication and Data integrity. Authenticate the model update parameters that are really sent by a legal client and have not been altered during the transmission, i.e., if the adversary \mathcal{A} forges and/or modifies the model update parameters, the malicious operations should be detected.

Byzantine robustness. Defend against Byzantine attacks caused by consensus problems, i.e., if the adversary \mathcal{A} claims having the aggregated model update parameters, the malicious operations should be detected.

C. Design goal

Under the aforementioned system model and security requirements, our design goal is to design an efficient and privacy-preserving global model training protocol for *FL in P2P networks*. Specifically, the following two objectives should be achieved.

The security requirements should be guaranteed in the proposed protocol. As stated above, if the training process does not consider security, the users' privacy could be disclosed, and the global model could be destroyed. Therefore, the proposed protocol should achieve confidentiality,

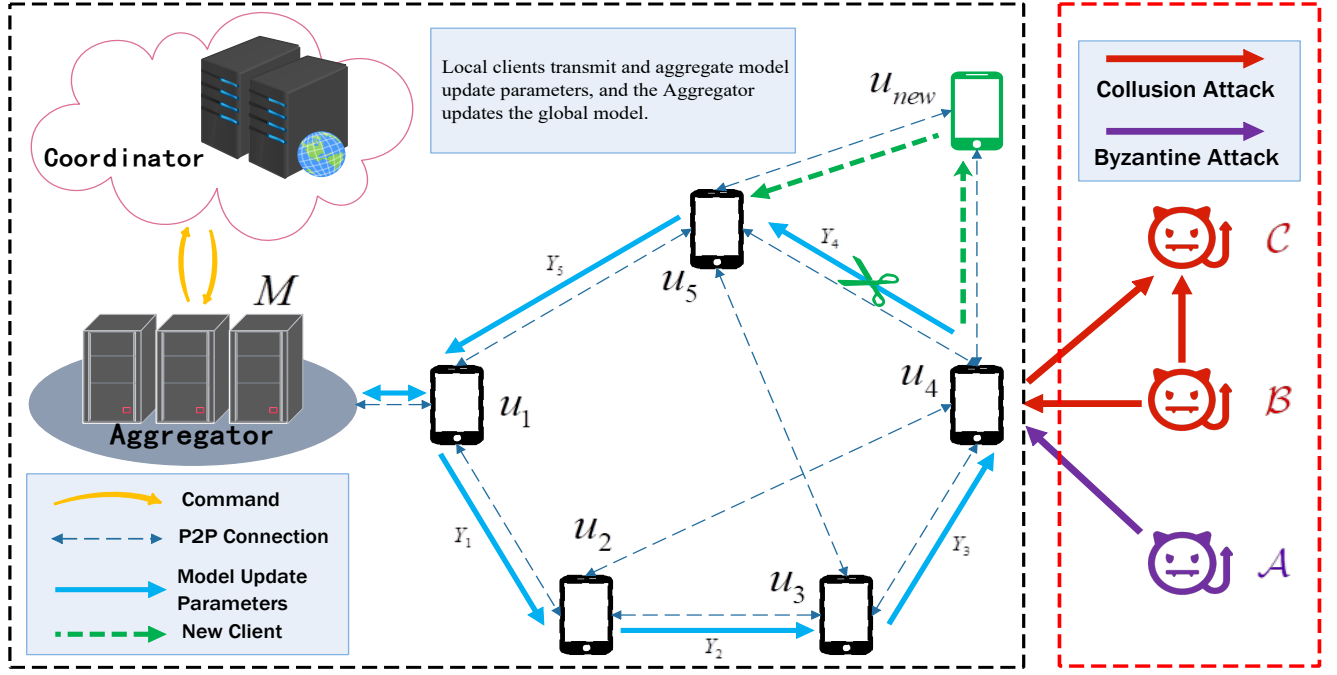


Fig. 2. System model under consideration.

authentication, data integrity, and Byzantine robustness [31] simultaneously.

Communication efficiency should be guaranteed in the proposed protocol. Although the communication among users in P2P networks is featured with high efficiency, to support hundreds and thousands of target clients aggregating local model update parameters, the arranged aggregating route should also consider the communication efficiency.

IV. SYSTEM DESIGN

In this section, we propose an efficient and privacy-preserving global model training protocol for *FL in P2P networks*, which mainly consists of the following five parts: communication key establishment, local model training and disturbance, model update parameters transmission and aggregation, global model update, and complementary mechanisms.

A. Communication key establishment

We first construct communication keys for potential clients. The operations that broadcasting the IDs of the keys in the key ring and path-key distribution leak the privacy of shared-keys obviously. We modify the E-G scheme and used it as our communication key establishment scheme. A large key pool is generated previously, which contains η keys and their identifiers (IDs). Every potential client c_i randomly extracts l keys from the key pool with replacement to establish the key ring $\{k_{i\alpha} | \alpha = 0, 1, \dots, l-1\}$. Afterwards, each client c_i broadcasts encrypted messages $\{A_{i\alpha} | \alpha = 0, 1, \dots, l-1\}$. Every $A_{i\alpha}$ is encrypted by every $k_{i\alpha}$ in c_i 's own key ring, and the encryption scheme is the symmetric cryptosystem. We represent the encryption process as

$$A_{i\alpha} \leftarrow \mathbf{EG.Enc}(a_{i\alpha}, k_{i\alpha}),$$

where $a_{i\alpha}$ is the plaintext of the message. The client c_j who receives $A_{i\alpha}$ reveals the challenge by executing the decryption process, shown as

$$a_{i\alpha} \leftarrow \mathbf{EG.Dec}(A_{i\alpha}, k_{j\alpha}).$$

Thereby, all neighbor clients can get the knowledge of keys held by both the broadcast client and themselves, respectively. All clients execute the above interactions mutually to obtain the same keys with each other, which are called shared-keys $\{k_{i,j}^r | r \in \mathbb{N}^*\}$. Any two adjacent clients c_i and c_j with more than e shared-keys execute XOR operations to compute their communication key, demonstrated as:

$$K_{i,j} = k_{i,j}^1 \oplus k_{i,j}^2 \oplus \dots \oplus k_{i,j}^e \oplus \dots$$

As for two clients connected directly but having no shared-keys, a third-party client distributes the keys that haven't been used to the two clients. Then, they choose some keys independently to obtain shared-keys and generate communication keys for themselves. A client will never choose all the received keys from the third-party client as its shared-keys. Otherwise, it will lead to privacy leakage, as the third-party client will calculate their communication key. Therefore, the communication keys are established for all potential clients.

In addition, we propose a *key revocation and update mechanism* to enhance the communication key establishment scheme. When a client is recognized as a malicious client, we execute the following operations to revoke the poison keys hold by the malicious client and rebuild communication keys for other participants:

- ① Coordinator broadcasts a countermand which contains the IDs of the poison keys.
- ② Clients delete the invalid keys from their key rings.

- ③ Affected clients rebuild communication keys.
- ④ When the key pool is used for a long time, the lifetime of keys expires. All clients restart the communication key establishment phase.

B. Local model training and disturbance

For the settings of *FL in P2P networks*, it is reasonable to assume an honest but curious server can coordinate the whole system. When the coordinator starts a training process for a global model, all target clients download the central original model M following the inherent P2P transmission protocol.

After local training, target clients obtain local personalized models m_i and prepare to uploads the weighted local model update parameters $\omega_i x_i$ and weights ω_i . To improve communication efficiency, clients encode the uploading data by attaching ω_i to the end of $\omega_i x_i$, which is defined by X_i , and denoted by:

$$X_i = (\omega_i x_i, \omega_i). \quad (4)$$

Then, the server chooses a target client which is connected to the server directly as the leader client u_0 . The transmission and aggregation route will start from the leader client. To protect u_0 's privacy, u_0 generates a noise s to disturb X_0 , shown as $X_0 + s$. Note that s has the same dimension as X_0 . Subsequently, the leader client u_0 can execute the transmission and aggregation process.

C. Model update parameters transmission and aggregation

The whole data transmission is following the inherent P2P transmission protocol, i.e., the sender uploads the data, then the recipient downloads the data directly. It is not conducive to planning a transmission route, as all neighbor clients can download the data from the sender.

Therefore, the leader client u_0 chooses a neighbor client as the downstream client u_1 . u_0 encrypts $X_0 + s$ using their communication key $K_{0,1}$. The encryption scheme is the symmetric cryptosystem. We write the encryption process as:

$$Y_0 \leftarrow \text{Enc}(X_0 + s, K_{0,1}).$$

Then, u_0 uploads Y_0 . Although every u_0 's neighbor client can still download Y_0 , only the chosen client u_1 can decrypt Y_0 .

After downloading Y_0 , u_1 executes the decryption process, shown as:

$$X_0 + s \leftarrow \text{Dec}(Y_0, K_{0,1}).$$

Afterward, u_1 adds its own data $X_1 = (\omega_1 x_1, \omega_1)$, denoted by $X_0 + s + X_1$. Whereafter, u_1 chooses a new neighbor client and executes encryption and uploading operations similar to u_0 .

The rest of target clients will execute the above operations successively until all participants finish data aggregation. Then, the aggregating data will be transmitted back to u_0 . u_0 subtracts the noise s and obtains the final aggregated data

$$\sum_{i=0}^{n-1} X_i = X_0 + X_1 + \dots + X_{n-1}. \quad (5)$$

The choice of the downstream client is the most important factor affecting aggregation efficiency. PPT adopts the *depth-first search algorithm in the graph* to enhance efficiency. The upstream client will always choose an unvisited client as the downstream client if possible. The algorithm explores as far as possible before backtracking.

In addition, due to the existence of an active adversary \mathcal{A} threatening the data integrity, a reliable digital signature is essential. In the proposed PPT protocol, we improve the function of digital signatures by signing a time stamp together with data to ensure timeliness. Noted that the digital signature scheme is the asymmetric cryptosystem, and the secret key SK_i and public key PK_i are initially deployed on every client u_i . The details of our signature scheme are as follows:

- ① The data holder u_i attaches a timestamp t_i to the encrypted data Y_i and signs on it using its secret key SK_i , which is shown as

$$\sigma_i \leftarrow \text{Sign}(Y_i, t_i, SK_i).$$

- ② u_i sends the encrypted data with signature $\langle Y_i, \sigma_i \rangle$ to the downstream client.

- ③ The recipient verifies the signature by u_i 's public key PK_i and check the time stamp, which is demonstrated as

$$\{1, 0\} \leftarrow \text{Verf}(\sigma_i, PK_i).$$

D. Global model update

After local model update parameters aggregation, the leader client u_0 uploads the aggregated data $\sum_{i=0}^{n-1} X_i$. The uploading data is encrypted and the signature is surely attached. The server confirms the aggregated data by verifying the signature and decryption. Then, the server decodes the aggregated data to aggregated weighted model update parameters $\sum_{i=0}^{n-1} \omega_i x_i$ and aggregated weights $\sum_{i=0}^{n-1} \omega_i$. Whereupon, the server updates the global model. The form of global model update is shown in Equation (3). Afterward, the updated global model will be distributed to all target clients to train and aggregate over and over again until the global model is converged. We demonstrate the global model update process in the R round as follows:

$$M^{R+1} = \frac{\sum_{i=0}^{n-1} \omega_i x_i^R}{\sum_{i=0}^{n-1} \omega_i} + M^R \quad (6)$$

E. Complementary mechanisms

The above design does well in efficiency and security when all participants are honest but curious. But in practice, there still exists active adversaries threatening the aggregation and transmission process. Besides, unlimited transmission and new client participation are not allowed. Hence, several complementary mechanisms are annexed to our basic design. The details of the complementary mechanisms are described as follows:

Neighborhood Broadcast Mechanism: To enhance the robustness and security, we propose a Neighborhood Broadcast mechanism. The mechanism dictates that every target client broadcasts the behavior and a timestamp τ to all neighbor

clients when executing an operation. The neighbor clients sequentially pass the broadcast to their neighbors until all clients receive the message. Based on the neighborhood broadcast mechanism, all operations are under the supervision of all clients, including the dropout and the new participation.

Termination Mechanism: In practice, the time of one global model training round is fixed and limited. Unlimited transmission, aggregation, and new client participation are not allowed. Thus, the following termination operations will be executed:

- ① The request of a newly joined client will be refused when one-half of the target clients have completed the aggregation process.
- ② PPT dictates executing the backtracking operation immediately when the time has passed two-thirds of the stipulated aggregation time.

Supervision and Report Mechanism: The collusion attack is common in distributed systems, which is no exception in the context of *FL in P2P networks*. To prevent collusion attacks, we propose the Supervision and Report Mechanism based on Game Theory [26]. The core idea is encouraging mutual reporting, and the process is as follows:

- ① All participants are required to pay a deposit d before starting the aggregation process. And the deposit will be returned at the end of the aggregation.
- ② We encourage mutual reporting aiming at malicious operations. If the alleged malicious operation is proven to be true, the defendant's deposit will be paid to the complainant.
- ③ If two participants report each other to get a pay, their deposits of them will be confiscated.

As long as the profit by collusion attack is lower than the deposit, i.e., $g < d$, the two parties will tend to execute the PPT protocol honestly. We analyze security based on Nash Equilibrium in Section V.

Integrating the main processes mentioned above and the complementary mechanisms, we propose our Privacy-Preserving Global Model Training (PPT) protocol in Fig. 3. Note that the red underlined parts are required to guarantee security under the active-adversary assumption (and not necessarily under the honest-but-curious assumption).

V. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed PPT protocol. In particular, following the security requirements discussed earlier, our analysis will focus on how the proposed PPT protocol can achieve local model update parameters privacy preservation, source authentication and data integrity, and Byzantine robustness. Besides, we analyze the connectivity based on the communication key establishment scheme, which is indispensable for the security of data transmission.

A. Privacy of clients

The local model update parameters are privacy-preserving. According to the proposed PPT protocol, the local model update parameters are uploaded in the form of ciphertext. Only the client chosen by the sender can decrypt the ciphertext

using the communication key. For any other honest-but-curious client and server in P2P networks, as long as the encryption algorithm is secure, it is impossible to obtain any information of the model update parameters. As for a chosen downstream client u_ν , he can only obtain aggregated parameters with noise $\sum_{i=0}^{\nu-1} X_i + s$.

The authentication and data integrity of clients' model update parameters are achieved in the proposed PPT protocol. In the proposed PPT protocol, each client signs on the ciphertext, when uploading the aggregated parameters. Therefore, if the adopted digital signature scheme is provably secure, the source authentication and data integrity can be guaranteed. As a result, the adversary \mathcal{A} 's malicious behaviors can be detected.

The Byzantine robustness is achieved in the proposed PPT protocol. In the proposed PPT protocol, All operations are under the supervision of all clients based on the neighborhood broadcast mechanism. Only the operation achieving consensus by all clients can be accepted. Even if an adversary \mathcal{A} forges aggregated parameters to confuse a target client, the target client can confirm the correct aggregated parameters by comparing received broadcasts from other clients.

B. Defense against collusion attack

The proposed PPT protocol is a strong defense against collusion attacks. All clients abide by the Supervision and Report mechanism. Regarding the collusion attack by adversaries \mathcal{B} and \mathcal{C} as a game based on Game Theory. There is a basic assumption in Game Theory that the participants are selfish but rational. We generalize the assumption to the context of *FL in P2P networks*.

Assumption 1: The adversaries \mathcal{B} and \mathcal{C} are selfish but rational in collusion attacks.

Theorem 1: A client's model update parameters are private against collusion attacks under *Assumption 1*.

Proof 1: According to the Supervision and Report mechanism, \mathcal{B} and \mathcal{C} have the same two strategies, i.e., collusion and counter-collusion. We assume the deposits of the two parties \mathcal{B} and \mathcal{C} are d , and the profits of executing collusion attacks successfully are g . Thereby, we can get the pay-off matrix in TABLE I.

TABLE I
PAY-OFF MATRIX

$\mathcal{B} \backslash \mathcal{C}$	collusion	counter-collusion
collusion	(g, g)	$(-d, d)$
counter-collusion	$(d, -d)$	<u>$(0, 0)$</u>

We definitely hope there is no collusion attacks, i.e., the Nash Equilibrium [26] of the game should be (counter-collusion, counter-collusion). Therefore, as long as $g < d$, the two adversaries tend to follow the proposed PPT protocol honestly.

C. Analysis of full connectivity

The limits of the inherent P2P transmission protocol preclude the transmission of private data. Ensuring the secure connectivity rate based on communication keys being maximum

Privacy-Preserving Global Model Training Protocol for FL in P2P networks

- **Setup:**
 - A large key pool containing η keys is generated offline.
 - Every potential participant c_i randomly extracts l keys from the key pool with replacement.
 - c_i stores the extracting keys and the IDs of the keys to establish the key ring $\{k_{i\alpha} | \alpha = 0, 1, \dots, l-1\}$.
 - θ kinds of noise generation algorithms are built in every client in advance as well as the public & private key PK_i and SK_i .
 - **Phase 0 (Communication key establishment):**
 - c_i broadcasts l encrypted messages $\{A_{i\alpha}\}$ using every $k_{i\alpha}$ in $\{k_{i\alpha}\}$ respectively, shown as $A_{i\alpha} \leftarrow \text{EG.Enc}(a_i, k_{i\alpha})$.
 - The client c_j who receives $A_{i\alpha}$ s tries to decrypt the messages, shown as $a_i \leftarrow \text{EG.Dec}(A_{i\alpha}, k_{j\alpha})$. Thereby, all recipient clients get the keys held by both the broadcast client and themselves.
 - All potential clients execute the above interactions mutually to obtain the shared-keys $\{k_{ij}^r | r \in \mathbb{N}^*, r < e\}$.
 - Adjacent two clients c_i and c_j with more than e shared-keys execute XOR operations to compute their communication key, shown as $K_{i,j} = k_{i,j}^1 \oplus k_{i,j}^2 \oplus \dots \oplus k_{i,j}^e \oplus \dots$
 - Consider the situation that two clients are connected directly but don't have shared-keys, a third party client distributes the keys that haven't been used for the shared-key establishment to the two clients. Then, they choose some keys independently to obtain shared-keys and generate the communication key.
 - If a client is recognized as a malicious client, the affected clients execute the Key Revocation and Update Mechanism to rebuild communication keys.
 - When the key pool is used for a long time, the lifetime of keys expires. All potential participants execute the Key Revocation and Update Mechanism to rebuild communication keys
 - If more than half of the potential clients are identified as malicious clients, abort.
 - **Phase 1 (Local model training and disturbance):**
 - Participants broadcast that they complete local training and will participate in the global model update.
 - The coordinator chooses a client as the leader client u_0 randomly. (To increase the success rate of the protocol, the coordinator prefers a client that has completed the protocol before as the leader client.)
 - The leader client u_0 generates a disturbed noise s by the built-in noise generation algorithms and disturbs the encoding local model updating parameters X_0 , which is shown as $X_1 + s$.
 - If the leader client drops out, abort. The coordinator selects a new leader client and restarts Phase 1.
 - **Phase 2 (Model update parameters transmission and aggregation):**
 - u_0 chooses a neighbor u_1 and broadcasts a message to all neighbors that it will transmit the aggregated data to u_1 . A timestamp τ_0 is attached to the message.
 - u_0 uses its corresponding communication key $K_{0,1}$ to encrypt the disturbed data, shown as $Y_0 \leftarrow \text{Enc}(X_0 + s, K_{0,1})$.
 - u_0 attaches a timestamp t_0 to the ciphertext Y_0 and signs on it, shown as $\sigma_0 \leftarrow \text{Sign}(Y_0, t_0, SK_0)$.
 - u_0 sends the encrypted data with the signature $\langle Y_0, \sigma_0 \rangle$ to u_1 .
 - When u_1 receives the data, it verifies the signature and checks the timestamps, shown as $\{1, 0\} \leftarrow \text{Verf}(\tau_0, \sigma_0, PK_0)$.
 - If u_1 confirms that the data truly comes from u_0 , u_1 decrypts the encrypted data, shown as $X_0 + s \leftarrow \text{Dec}(Y_0, K_{0,1})$.
 - If not, wait for the correct aggregated data from u_0 .
 - u_1 aggregates the plaintext $X_0 + s$ and its own data X_1 , shown as $X_0 + X_1 + s$.
 - u_1 executes the above broadcast, encryption, timestamp attachment, signing, and transmission operations as u_0 did.
 - If u_0 doesn't receive the broadcast from u_1 , u_0 chooses a new neighbor as u_1 and executes the data aggregation process.
 - The same operations are executed among all participants successively until all participants complete aggregation.
 - The selection of the downstream client follows the *depth-first search algorithm*.
 - If all neighbor clients have received the aggregating data already, the current client passes the data back to the previous client.
 - The protocol dictates that every honest user can only aggregate the local model update parameters once.
 - As for the clients receiving encrypted data again, they only execute signature verification, decryption, encryption, signing, broadcast, and transmission operations.
 - Finally, u_0 receives the aggregated result $\sum_{i=0}^{n-1} X_i + s$
 - u_0 subtracts the disturbed noise s and obtains the encoding global model update parameters $X_0 + X_2 + \dots + X_{n-1}$.
 - If u_0 doesn't receive aggregated result after the stipulated time, abort.
 - **Phase 3 (Global model update):**
 - u_0 uploads the encoding global model update parameters $X_0 + X_2 + \dots + X_{n-1}$ to the aggregator.
 - The aggregator decodes the encoding global model updating parameters to $\sum_{i=0}^{n-1} \omega_i x_i$ and $\sum_{i=0}^{n-1} \omega_i$.
 - The aggregator updates the global model and broadcasts a message that the global model has been updated.
 - If the aggregator doesn't receive the model updating parameters after the stipulated time, abort.
- All clients follow the Supervision and Report Mechanism in the whole data aggregation process.
- PS:**
- **For a newly joined client:**
 - Start the Communication key establishment phase for the newly joined client u_{new}
 - u_{new} requests for participating in the global model training process.
 - u_{new} joins in the data transmission process according to the *depth-first search algorithm*.
 - **Termination:**
 - The protocol rejects the request of a newly joined client when one-half of the clients have completed the aggregation process.
 - The protocol executes backtracking operation immediately when the time has passed two-thirds of the stipulated aggregation time.

Fig. 3. Detailed description of the Privacy-preserving Training Protocol. Red, underlined parts are required to guarantee security under the active-adversary assumption (and not necessarily under the honest-but-curious assumption).

possible is of vital importance. We first recall the monotonicity of Random Graph [33].

Let $G(n, p)$ is a random graph, where n is the number of clients and p is the probability that a link exists between two clients.

Lemma 1: Given a desired connectivity probability P_c for a graph $G(n, p)$, the threshold function p is defined by:

$$P_c = \lim_{n \rightarrow \infty} \Pr[G(n, p) \text{ is connected}] = e^{-e^{-c}}, \quad (7)$$

Where $p = \frac{\ln n}{n} + \frac{c}{n}$ and c is any real constant.

Laurent *et al.* [29] give the trade-off between the sizes of the key pool and the key ring.

Lemma 2: For a given p , the trade-off between the key pool size and the key ring size follows the equality:

$$p = 1 - \frac{((\eta - l)!)^2}{(\eta - 2l)! \eta!}, \quad (8)$$

Where η is the size of the key pool, and l is the size of the key ring.

Theorem 2: The communication key establishment phase in the proposed PPT protocol satisfies the requirement of private data transmission by choosing proper sizes of the key pool and the key ring.

The proof of *Theorem 2* is obvious. It is possible for P2P networks to achieve a specific probability p based on the communication key establishment scheme, for example, 0.999. Similarly, the sizes of the key pool and the key ring can be adjusted according to actual demands to achieve both higher security and the inter-client higher connectivity rates according to *Lemma 2*. Thus, the whole data transmission process is well protected.

VI. EXPERIMENTAL DESIGN

In this section, we conduct the simulation experiments for the proposed PPT protocol in a spam classification scenario. All simulations are implemented on the same computing environment (Linux Ubuntu 16.04, Intel i7-6950X CPU, 62 GB RAM, and 3.6TB SSD) with Tensorflow, Keras and, PyCryptodome.

In our experiments, There are 200 potential clients in P2P networks and only half of them are target clients. The communication keys are established for all potential clients. We first train a central original model M^0 and distribute M^0 to all target clients. Then, the 100 target clients collaboratively train a global model based on the proposed PPT protocol. We also design a dropout simulation to evaluate the robustness. In the remainder of this section, we give the details of our experiments.

Database

The database used in our experiments consists of two different parts. One part is Trec06p which contains 37822 English emails from the real world in 2006. There are 12910 hams and 24912 spams in the main corpus with messages. The other part is Trec07 which is also a real-world English email database consisting of 25220 hams and 50199 spams.

A. Simulation of model training

Firstly, we train a central original model using Convolutional Neural Network (CNN) [34] for spam classification. In the beginning, we construct a word vocabulary for Trec06p. For each sample, we generated a corresponding word embedding matrix. Then, we divide the Trec06p database into a training set and a testing set in a 3:1 scale uniformly. The training samples are sent to a CNN consisting of two convolution layers, two pooling layers, and three fully connected layers. We set the loss function as the *cross-entropy error* and the active function as the *sigmoid*. We use SGD for gradient descent, where the learning rate is 0.1. And the central original model is saved as M^0 . The training process is given in Algorithm 1.

Algorithm 1 Original Model Training

Input: D is the Trec06p dataset; Z is cross-validation times; CNN contains two convolution layers, two pooling layers, and three fully connected layers; SGD is the stochastic gradient descent algorithm.

Output: the original model M^0 ; $trainSet$ and $testSet$ are the training set and testing set; evaluation result res .

- 1: $\{Matrix\} \leftarrow$ (generate word embedding matrix for every sample in D);
 - 2: $(trainSet, testSet) \leftarrow$ split $\{Matrix\}$;
 - 3: $S_i \leftarrow$ (split $trainSet$ in equal parts of Z);
 - 4: **for** each fold $i = 1, 2, \dots, Z$ **do**:
 - 5: $\{vSet, tSet\} \leftarrow \{S_i, S - S_i\}$;
 - 6: **for** each epoch **do**:
 - 7: $M_i^0 \leftarrow$ modelFit($CNN, SGD, tSet$);
 - 8: $r_i \leftarrow$ modelEvaluate($m_i, vSet$);
 - 9: **end for**
 - 10: **end for**
 - 11: $M^0 \leftarrow$ averageModel($\{(M_i^0, r_i) | i = 1, 2, \dots, Z\}$);
 - 12: $res \leftarrow$ modelEvaluate($M^0, testSet$);
-

Secondly, we survey the e-mail amounts of 100 Gmail users. Our user study involves 100 participants, including 59 males and 41 females whose ages range from 16 to 85. All participants come from different regions and countries, including different skin tones. The participants are recruited using the questionnaire www.wjx.cn by WeChat.

Algorithm 2 Local Training

Input: M^0 is the central original model; 100 clients are indexed by i ; D_i is the data set for each client u_i .

Output: the local model set $\{m_i | i = 0, 1, \dots, 99\}$.

- 1: **for** each client u_i **do**:
 - 2: Initialize the central original model M^0 on local;
 - 3: $trainSet_i \leftarrow (D_i)$;
 - 4: $m_i \leftarrow$ LocalmodelFit($M^0, CNN, SGD, trainSet_i$);
 - 5: **end for**
-

We split the Trec07 database into two parts. A portion is assigned to 100 clients as training sets to train their local models. Every client's spam and ham e-mail amounts are assigned strictly according to the results of our user study.

Another portion is used as a testing set to evaluate the proposed PPT protocol.

Thirdly, we simulate the local training processes. 100 target clients re-train M^0 using their local training sets respectively. We give the first round local training algorithm flow in Algorithm 2.

B. Simulation of data aggregation

We simulate the interactions of the proposed PPT protocol. The dropout situation is considered, too. We take the assumption that a fixed number of target clients drop out to reveal the robustness against dropout.

Firstly, we randomly generate 200 potential clients and their connections to simulate a P2P network topology. Next, we construct communication keys for the 200 potential participants. According to the E-G scheme in the proposed PPT protocol, we set the size of the key pool as 2000 and the key ring size 20. We illustrate the connections among potential participants based on the communication keys as the gray lines in Fig. 4. We also generate 100 pairs of secret and public keys $\{(SK_i, PK_i) | i = 0, 1, \dots, 99\}$ for signature.

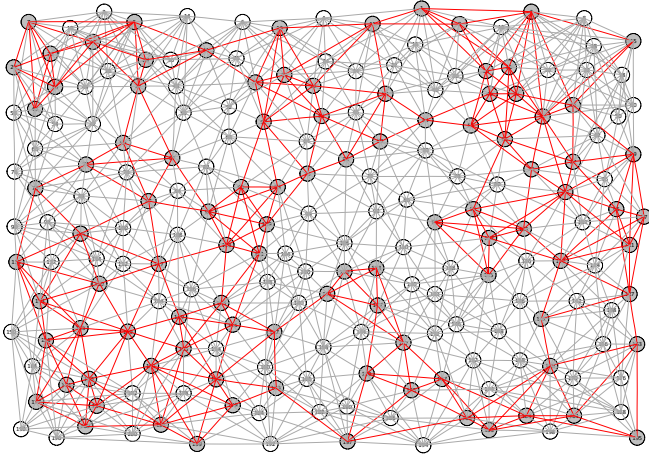


Fig. 4. Clients in a P2P network.

Secondly, we randomly select 100 target clients $\{u_i, i = 0, 1, \dots, 99\}$, which are shown as the gray node in Fig. 4. Then, we mark one of them as the leader client u_0 . A data transmission route for the 100 target clients according to the *depth-first search algorithm* is confirmed subsequently. We illustrate the transmission route as the red line in Fig. 4.

A noise s is generated to disturb the data of the leader client. In the experiments, we take the AES [35] as the encryption algorithm, where the keys are the communication keys. And the signature scheme is designed to use the ElGamal-based signature algorithm [36].

Finally, we aggregate the encoding model update parameters according to the designed transmission route and encryption algorithm and complete the first round of global model training:

$$M^1 = \frac{\sum_{i=0}^{99} \omega_i x_i}{\sum_{i=0}^{99} \omega_i} + M^0. \quad (9)$$

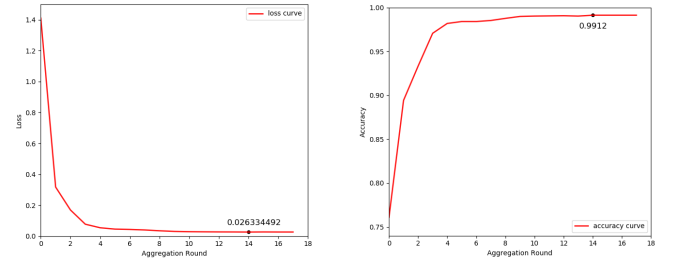
Through several rounds of global model training, the global model will converge.

Afterward, we design a series of dropout clients as the contrast experiments to demonstrate the robustness of the proposed PPT protocol. Besides, we evaluate the efficiency of our privacy-preserving method based on noise addition compared to secret sharing which is deployed in Google's Secure Aggregation protocol [6].

VII. EXPERIMENTAL RESULT AND PERFORMANCE

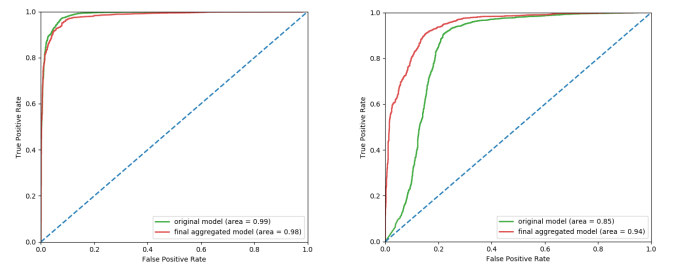
In this section, we present the experimental results and evaluate the performance of the proposed PPT protocol in terms of correctness, robustness, and efficiency. The final updated global model is accurate in classifying the samples both in the trec07 testing set and the trec06 testing set.

After 14 epochs of training in the trec06p training set, the central original model achieves the accuracy of 99.99% and 99.88% classifying the samples in the trec06p validation set and testing set, respectively. When classifying the samples in the trec07 testing set, the accuracy is only 76.10%. In the no dropout experiment settings, the global model converges at the 14th round, which is shown in Fig. 5(a). And the accuracy of the final global model is 99.12% in the trec07 testing set, which can be seen in Fig. 5(b). Meanwhile, the final updated global model performs well in the trec06p testing set, whose accuracy is 90.95%. In Fig. 5., we compare the performances of the central original model and the final global model by illustrating the receiver operating characteristic (ROC) and the area under the curve (AUC). The final global model performs better than the central original model in the trec07 and trec06p testing set.



(a) Loss value in Trec07 testing set. (b) Accuracy in Trec07 testing set.

Fig. 5. Performance of the final global model in the Trec07 testing set.



(a) ROC in Trec06p testing set (b) ROC in Trec07 testing set

Fig. 6. ROC of the original model and final global model.

While randomly choosing dropout clients, the updated models still have good performances. Fig.6. shows the accuracies in the trec07 testing set when the amounts of dropout clients are 1, 5, 10, and 15 respectively. Despite dropout, the final global model still achieves an accuracy of 91.02% at least. What's more, the communication key and global model aggregation form support the dropout situation. The averaging amounts of one-hop transmission in one aggregation round are shown in TABLE II.

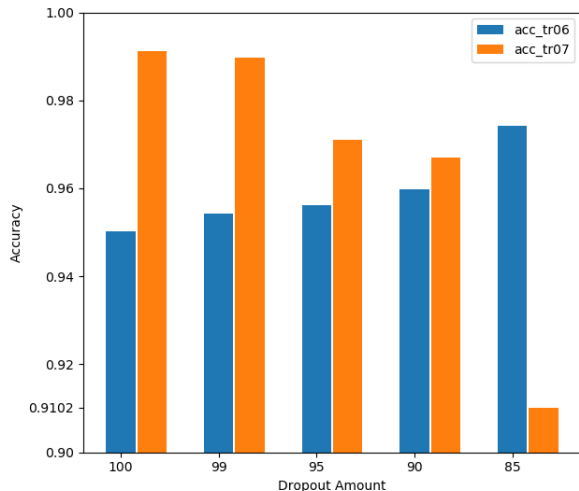


Fig. 7. Accuracy when meeting dropout situation.

TABLE II
AVERAGING DATA TRANSMISSION AMOUNT

Client amount	100	99	95	90	85
Transmission amount	190	185	183	171	163

The computational performance for one client is exhibited in TABLE III. Compared to the secret sharing deployed in Google's Secure Aggregation protocol, The PPT protocol requests less computational resources and offers more efficiency for clients.

TABLE III
PERFORMANCE

Index	Operations ¹	Time(ms/1000byte)
1	Secret sharing	23.3164
2	Secret reconstruction	9.8632
3	Noise generation	1.2548
4	Noise addition	0.1422
5	Noise subtraction	0.1506
6	Encryption(AES-128bit)	170.8248
7	Decryption(AES-128bit)	0.0282
8	Signature(Elgamal-2048bit)	0.0003
9	Verification(Elgamal-2048bit)	0.0071

¹ We execute a series of operations on a 114MB file of local model updating parameters in the form of plaintext. And the encrypted result is 440.1MB.

VIII. LIMITATION AND FUTURE WORK

In this section, we briefly discuss the limitation of the proposed PPT protocol. We also have a vision of the future

works.

PPT is designed for the *FL in P2P networks* where clients are usually not directly connected with a central server. Despite inheriting the data transmission speed from P2P networks, the one-hop transmission form is obviously less efficient. When the amount of participants is larger enough, the communication efficiency of PPT is not so high. What's more, the communication key establishment scheme is more proper for a static network. In some dynamic P2P networks, especially Internet of Vehicles (IoV) and Ad Hoc Networks scenarios, clients are always mobile. Thus, the future research direction point to the efficiency of *federated learning in large-scale and dynamic P2P networks*.

The supervision and report mechanism is based on a pure strategy game, i.e., adversaries' strategies are equiprobable. Nevertheless, adversaries' strategies are complex in practice, especially the probability of different strategies. Improving the supervision and reporting mechanism based on Game Theory more in line with the real scenario will be our next research.

Besides, ecological validity is a challenge to our user study. Our study mainly recruits students in the university. These participants are usually more active in using e-mail applications. Thus the performance evaluation may vary with other populations. In future works, we will conduct a large-scale user study involving more participants to perform a more intensive evaluation of our protocol.

IX. CONCLUSION

The status lacking a trusted central server necessitates the development of *federated learning in P2P networks*. This research provides an instance of such a context, along with guarantees on both its communication efficiency and privacy. While there have been prior works on federated learning and collaboratively training, our work is the first to provide a privacy-preserving global model training protocol in the none central aggregator setting from the secure and efficient transmission perspective. Besides, our training protocol is dropout-robust, which is of practical significance. And our experiments conducted on two real-world datasets suggest that our training protocol is practical.

REFERENCES

- [1] J. Hirschberg and C. D. Manning, "Advances in natural language processing," *Science*, vol. 349, no. 6245, pp. 261-266, Jul. 2015.
- [2] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition CVPR*, pp. 2818-2826, Las Vegas, NV, USA, Jun. 2016.
- [3] X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, "Data mining with big data," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 1, pp. 97-107, Jan. 2014.
- [4] P. Voigt and A. V. d. Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide (1st Ed.)*, Springer, 2017.
- [5] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. Int. Conf. Artificial Intelligence and Statistics AISTATS*, vol. 54, pp. 1273-1282, Fort Lauderdale, FL, USA, Apr. 2017.
- [6] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proc. ACM SIGSAC Conf. Computer and Commun. Security CCS*, pp. 1175-1191, Dallas, TX, USA, Oct.-Nov. 3. 2017.

- [7] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," in *NIPS Workshop on Private Multi-Party Machine Learning*, Barcelona, Spain, Dec. 2016. [Online]. Available: <https://arxiv.org/abs/1610.05492>
- [8] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečný, S. Mazzocchi, H. B. McMahan, T. V. Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards federated learning at scale: System design," in *Proc. Conf. Syst. and Machine Learning SysML*, Stanford, CA, USA, Mar.-Apr. 2. 2019.
- [9] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in *Proc. ACM Conf. Computer and Commun. Security CCS*, pp. 1322–1333, Denver, CO, USA, Dec. 2015.
- [10] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphism," *Foundations of Secure Computation*, pp. 169–180, Academic Press, 1978.
- [11] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. ACM Symp. Theory of Comput. STOC*, pp. 169–178, Bethesda, MD, USA, May-Jun. 2. 2009.
- [12] C. Dwork, "Differential privacy," in *Proc. Int. Colloquium on Automata, Languages and Programming ICALP*, vol. 4052, pp. 1–12, Venice, Italy, Jul. 2006.
- [13] A. C. Yao, "Protocols for secure computations," in *Proc. IEEE Annual Symp. Foundations of Computer Science SFCS*, pp. 160–164, Chicago, IL, USA, Nov. 1982.
- [14] N. Agarwal, A. T. Suresh, F. X. Yu, S. Kumar, and H. B. McMahan, "cpSGD: Communication-efficient and differentially-private distributed SGD," in *Proc. Neural Inf. Processing Syst. NIPS*, pp. 7575–7586, Montréal, Canada, Dec. 2018.
- [15] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," in *Proc. Int. Conf. Learning Representations. ICLR*, Vancouver, BC, Canada, Apr.-May. 3. 2018.
- [16] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *Trans. Intelligent Syst. and Technology*, vol. 10, no. 2, p. 12, Feb. 2019.
- [17] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proc. Int. Conf. Peer-to-Peer Comput. P2P*, pp. 101–102, Linköping, Sweden, Aug. 2001.
- [18] X. Lian, C. Zhang, H. Zhang, C.-J. Hsieh, W. Zhang, and J. Liu, "Can decentralized algorithms outperform centralized algorithms? A case study for decentralized parallel stochastic gradient descent," in *Proc. Neural Inf. Processing Syst. NIPS*, pp. 5330–5340, Long Beach, CA, USA, Dec. 2017.
- [19] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji *et al.*, "Advances and Open Problems in Federated Learning," *arXiv preprint arXiv:1912.04977*, 2019.
- [20] A. G. Roy, S. Siddiqui, S. Pölsterl, N. Navab, and C. Wachinger, "Braintorrent: A peer-to-peer environment for decentralized federated learning," *arXiv preprint arXiv:1905.06731*, 2019.
- [21] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conf. Computer and Commun. Security CCS*, pp. 41–47, Washington, DC, USA, Nov. 2002.
- [22] P. Ramanan and K. Nakayama, "BAFFLE: Blockchain based aggregator free federated learning," in *Proc. IEEE Int. Conf. on Blockchain*, pp. 72–81, Rhodes Island, Greece, Nov. 2020.
- [23] S. Lu, Y. Zhang, Y. Wang, and C. Mack, "Learn electronic health records by fully decentralized federated learning," in *NIPS Workshop on Federated Learning for Data Privacy and Confidentiality in Conjunction*, Vancouver, Canada, Dec. 2019.
- [24] A. Lalitha, O. C. Kilinc, T. Javidi, and F. Koushanfar, "Peer-to-peer federated learning on graphs," *arXiv preprint arXiv:1901.11173*, 2019.
- [25] A. Dubey and A. Pentland, "Differentially-Private Federated Linear Bandits," *arXiv preprint arXiv:2010.11425*, 2020.
- [26] T. Wittkopp and A. Acker, "Decentralized federated learning preserves model and data privacy," *arXiv preprint arXiv:2102.00880*, 2021.
- [27] J. F. Nash, "Equilibrium points in n-person games," in *Proc. National Academy of Sciences*, vol. 36, no. 1, pp. 48–49, Jan. 1950.
- [28] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE Trans. Dependable and Secure Comput. TDSC*, vol. 12, no. 1, pp. 98–110, Jan.-Feb. 1. 2015.
- [29] L. Bottou, "Large-scale machine learning with stochastic gradient descent," in *Proc. Int. Conf. Computational Statistics COMPSTAT*, pp. 177–186, Paris, France, Aug. 2010.
- [30] M. Yu, M. Zhou, and W. Su, "A secure routing protocol against byzantine attacks for MANETs in adversarial environments," *Trans. Vehicular Technology*, vol. 58, no. 1, pp. 449–460, Jan. 2009.
- [31] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Programming Languages and System*, vol. 4, no. 3, pp. 382–401, Jul. 1982.
- [32] R. E. Tarjan, "Depth-first search and linear graph algorithms," *SIAM J. Comput.*, 1972.
- [33] P. Erdős and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci.*, vol. 5, no. 1, pp. 17–60, 1960.
- [34] S. Lai, L. Xu, K. Liu, and J. Zhao, "Recurrent convolutional neural networks for text classification," in *Proc. AAAI Conf. Artificial Intelligence AAAI*, vol. 29, no. 1, pp. 2267–2273, Austin, TX, USA, 2015.
- [35] J. Daemen and V. Rijmen, "The Rijndael block cipher: AES proposal," *First candidate conference (AES1)*, pp. 20–22, Aug. 1999.
- [36] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.
- [37] I. Colin, A. Bellet, J. Salmon, and S. Cléménçon, "Gossip dual averaging for decentralized optimization of pairwise functions," in *Proc. Int. Conf. on Machine Learning ICML*, vol. 48, pp. 1388–1396, New York, NY, USA, Jun. 2016.
- [38] H. Tang, X. Lian, M. Yan, C. Zhang, and J. Liu, " D^2 : Decentralized training over decentralized data," in *Proc. Int. Conf. on Machine Learning ICML*, vol. 80, pp. 4848–4856, Stockholm, Sweden, Jul. 2018.
- [39] A. Koloskova, S. U. Stich, and M. Jaggi, "Decentralized stochastic optimization and gossip algorithms with compressed communication," in *Proc. Int. Conf. on Machine Learning ICML*, vol. 97, pp. 3478–3487, Long Beach, CA, USA, Jun. 2019.