Internet of Things, Ad Hoc and Sensor Networks Technical Committee Newsletter

(IoT-AHSN TCN)

Volume 1, No. 20

June, 2024

CONTENTS

PREFACE

The IEEE ComSoc Ad Hoc and Sensor Networks Technical Committee (IoT-AHSN TC) sponsors papers, discussions, and standards on all aspects of IoT, ad hoc and sensor networks. It provides a forum for members to exchange ideas, techniques, and applications, and share experience among researchers. Its areas of interest include systems and algorithmic aspects of sensor and ad hoc networks, networking protocols and architecture, embedded systems, middle-ware and information management, novel applications, flow control and admission control algorithms, network security, reliability, and management. In an attempt to make all the TC members as well as the IoT-AHSN worldwide community aware of what is going on within our main areas of concerns, this newsletter had been set up. The newsletter aims at inviting the authors of successful research projects and experts from all around the world with large vision about IoT-AHSN-related research activities to share their experience and knowledge by contributing in short news.

The twentieth issue of the IoT-AHSN TC Newsletter focuses on the theme "Physical Layer Security for Internet of Things". Specifically, this issue includes 1 news article: Enhancing Security of Federated Learning among IoT with IRS-Assisted Anti-Eavesdropper Approach. We thank the contributor for their efforts to help make the IoT-AHSN TC Newsletter a success. We hope that the methods/approaches presented in this issue could significantly benefit researchers and application developers who are interested in IoT and ad hoc/sensor networks.

Newsletter Co-Editors
Qiang Ye (Dalhousie University, Canada)
Moez Esseghir (University of Technology of Troyes, France)
Lu Lv (Xidian University, China)

TC OFFICERS AND NEWSLETTER EDITORS

TC Officers

Name	Affiliation	Email
Sharief Oteafy (Chair)	DePaul University, USA	soteafy@depaul.edu
Shuai Han (Vice Chair)	Harbin Institute of Technology, China	hanshuai@hit.edu.cn
Rodolfo Coutinho (Secretary)	Concordia University, Canada	coutinho@ece.concordia.ca

Newsletter Editors

Name	Affiliation	Email
Qiang Ye (Editor in Chief)	Dalhousie University, Canada	qye@cs.dal.ca
Moez Esseghir (Technical Editor)	University of Technology of Troyes, France	moez.esseghir@utt.fr
Lu Lv (Technical Editor)	Xidian University, China	lulv@xidian.edu.cn

Enhancing Security of Federated Learning among IoT with IRS-Assisted Anti-Eavesdropper Approach

Yingying Wu*, and Bomin Mao*†
*School of Cybersecurity, Northwestern Polytechnical University, Xi'an, Shaanxi, 710072, China
†E-mail: maobomin@nwpu.edu.cn

***Abstract*—Non-Orthogonal Multiple Access (NOMA) based Federated Learning (FL) can achieve the massive connectivity of Internet of Thing (IoT) devices, low latency, and pervasive intelligence in 6G networks. However, the parameters in model uploading phase can be intercepted by eavesdroppers, leading to security breaches. To tackle this issue, the Intelligent Reflecting Surface (IRS) assisted anti-eavesdropper approach is proposed in this paper, where a Deep Reinforcement Learning (DRL) based approach is utilized to solve the minimum secrecy rate problem. Performance is verified through simulation results.**

***Index Terms*—Non-Orthogonal Multiple Access (NOMA), Federated Learning (FL), Internet of Thing (IoT), anti-eavesdropper**

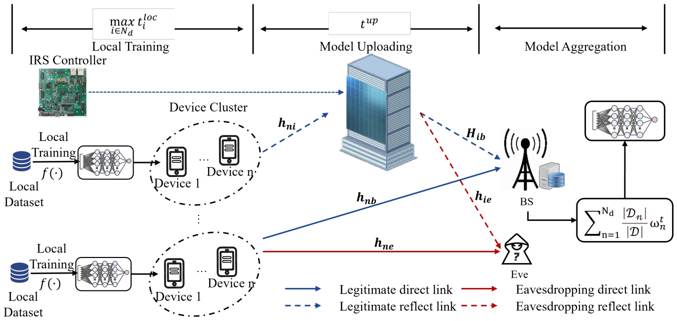

Fig. 1. System model for IRS-assisted FL

I. Introduction

6G is envisioned to enable diverse Internet of Things (IoT) device accessibility, ultra-low latency, as well as promising ubiquitous intelligence, while bringing out stringent privacy requirements. Federated Learning (FL), as a decentralized model training method, has been shown to be a promising enabler. It can facilitate the customization of AI services, empower real-time learning on edge devices, substantially reducing the communication latency. Additionally, it has been widely accepted as an efficient technique for protecting private information by keeping data localized for training. At the same time, Non-Orthogonal Multiple Access (NOMA) is adopted to relief the communication resource constraints for catering to multiple IoT devices access to swiftly build a reliable FL model among irregular local data distributions and heterogeneous data under 6G networks [1].

However, during model uploading phase, the model can be intercepted by Eavesdroppers (Eves), potentially leading to sensitive information leakage, which cannot be effectively mitigated on edge devices due to the resource constraint. Fortunately, an emerging advanced technology named Intelligent Reflecting Surface (IRS) can serve as a solution. IRS can reconfigure the wireless propagation environment to improve spectrum, energy efficiency [2] and impede the Eve. Since it mainly consists of passive reflecting elements, it proactively adjusts the wireless signal at a lower cost and in a more efficient full-duplex mode compared to other traditional relay methods [3]. With the IRS controller, each element can tune the amplitude and phase shift independently, thereby collaboratively changing the reflected signal propagation [3]. In this way, IRS can enhance the channel gain from information source to legitimate users and suppress the signal to Eves.

Traditional security methods primarily concentrate on the addition of jamming to signals. End devices [4] and Unmanned Aerial Vehicles (UAVs) [5] have been studied to serve as jammers to impede the Eves and secure the training process. However, the addition of jamming to the signal not only results in additional energy consumption for resource-constrained IoT devices, but also significantly degrades FL performance. While [6] tackles the covertness problem in Over-The-Air (OTA) communication-based FL, but OTA performs inflexibly in supporting diverse service requirements during FL aggregation. To address these issues, we explore the benefits of IRS to boost the security of NOMA-based FL, enabling the pervasive intelligence and massive connectivity of the upcoming 6G. Besides, the Deep Reinforcement Learning (DRL) based algorithm named Deep Deterministic Policy Gradient (DDPG) is utilized to solve the IRS optimization problem.

II. Problem Formulation

We consider an IRS-assisted NOMA-based FL system as shown in Fig. 1, including one BS with N_T antennas, N_d IoT devices with a single antenna, an Eve with a single antenna, and one IRS with N_I passive reflecting elements. The Eve is situated in the close proximity to the BS and intercept the parameters from devices to BS, while the IRS is utilized to prevent Eve from intercepting.

FL model: We consider Federated Averaging (FedAvg) algorithm as our FL model. In each iteration, N_d IoT devices participate in the local training. Device n collects and holds its data set of $\mathcal{D}_n = \{(\boldsymbol{x}_i, y_i)\}_{i=1}^{|\mathcal{D}_n|}$, where $(\boldsymbol{x}_i, y_i)$ is the i-th data pair of the device n, consisting of the input $\boldsymbol{x}_i$ and its label y_i. $|\mathcal{D}_n|$ denotes the cardinality of the data set $\mathcal{D}_n$.

In the FL training process, BS first initializes the model parameter $\boldsymbol{\omega}^0$ and distributes it to the participated IoT devices. Then in each iteration, local IoT devices perform local training via minimizing the local loss function: $F_n(\boldsymbol{\omega}) = \frac{1}{|\mathcal{D}_n|}\sum_{j=1}^{|\mathcal{D}_n|} f\left(\boldsymbol{x}_i, y_j; \boldsymbol{\omega}_j\right)$, where $f\left(\boldsymbol{x}_j, y_j; \boldsymbol{\omega}_j\right)$ is the loss of prediction on the local data pair $(\boldsymbol{x}_j, y_j)$ calculated with the model parameters $\boldsymbol{\omega}_j$. The parameter $\boldsymbol{\omega}$ is updated by executing Stochastic Gradient Descent (SGD) on the local loss function. Following that, BS performs the global training in the way that minimizing the global loss function: $f(\boldsymbol{\omega}) = \sum_{n=1}^{N_d} \frac{|\mathcal{D}_n|}{|\mathcal{D}|} F_n(\boldsymbol{\omega})$, where $|\mathcal{D}| = \sum_{n=1}^{N_d} |\mathcal{D}_n|$.

Communication model: The channel gains from device n to BS, Eve, and IRS are denoted as $\mathbf{h}_{nb} \in \mathbb{C}^{1\times N_\mathrm{T}}$, $\mathbf{h}_{ne} \in \mathbb{C}^{1\times 1}$, and $\mathbf{h}_{ni} \in \mathbb{C}^{1\times N_\mathrm{I}}$, while channels from IRS to the BS and Eve can be represented as $\mathbf{H}_{ib} \in \mathbb{C}^{N_\mathrm{I}\times N_\mathrm{T}}$, and $\mathbf{h}_{ie} \in \mathbb{C}^{N_\mathrm{I}\times 1}$. $\mathbb{C}$ denotes the complex matrices. Then the effective channels between device n and BS, as well as that between device n and Eve can be expressed as $\mathbf{h}_{nb}^{eff} = \mathbf{h}_{in}\,\mathrm{diag}(\Phi)\mathbf{H}_{ib} + \mathbf{h}_{nb}$ and $\mathbf{h}_{ne}^{eff} = \mathbf{h}_{in}\,\mathrm{diag}(\Phi)\mathbf{h}_{ie} + \mathbf{h}_{ne}$, respectively. IRS has the phase shift $\Phi = \left\{e^{j\phi_1}, \cdots, e^{j\phi_{N_\mathrm{I}}}\right\}^T \in \mathbb{C}^{N_\mathrm{I}\times 1}$, where $\phi \in [0, 2\pi]$. The ideal reflection of IRS is assumed, i.e., each element $\Phi_l = e^{j\phi_l}, l \in N_I$ satisfies $|\Phi_l| = 1$.

FL uploading phase is considered in this paper, therefore, in round t, the transmitted signals over the NOMA channel is the the trained local parameters w_n^t, which are encapsuled to transmit symbols s_n^t before the transmission. Besides, we make the normalization of aforementioned channels to mitigate potential numerical issues. The successive interference cancellation is adopted to decode the received channels where receiver starts by decoding the signal from the channel with the highest gain [7]. Assuming that the channel gain from device 1 to N_d gradually increases, then the transmission rates from device n to the BS, denoted as R_{nb}, and from device n to the Eve, denoted as R_{ne}, can be expressed as: $R_{nc} = B\log_2\left(1 + \frac{p_n\left|\mathbf{h}_{nc}^{eff}\right|^2}{\sum_{j=1}^{n-1} p_j\left|\mathbf{h}_{jc}^{eff}\right|^2 + 1}\right), c \in \{b, e\}$, where p_n is the n^{th} column vector of the matrix $\mathbf{P}$, the transmission power matrix at devices. We have the constraint that $\mathbf{P} \leq P_{Max}$, P_{Max} is the transmission power budget at devices. Therefore, the secrecy rate received at BS can be described as $R_{sn} = R_{nb} - R_{ne}$.

To mitigate the wire-tap channel from IoT devices to Eve and ensure the FL training security, we aim to maximize the minimum secrecy rate. The optimization problem is formulated as follows:

$$\begin{aligned} &\text{maximize} \;\; \min R_{sn} \\ \text{s.t.: } &\mathbf{P} \leq P_{Max}, \forall n \in \mathcal{N}_d, \\ &|\Phi_l| = 1, \forall l \in \mathcal{N}_\mathcal{I}. \end{aligned} \tag{1}$$

III. Proposed DDPG Algorithm and Simulation Results

We jointly optimize the devices' transmission power $\mathbf{P}$ and IRS phase shift Φ to maximize the minimum secrecy rate, as defined in problem (1). The DDPG which is a DRL-based algorithm with actor-critic structure is utilized to reach this. The devices' transmission power $\mathbf{P}$ and IRS phase shift Φ are seen as the action elements. They are updated iteratively through the interaction between the DDPG agent and the environment according to the predefined reward which is defined as the the minimum secrecy rate. To satisfy the constraint of $\mathbf{P} \leq P_{Max}$, we incorporate a normalization step in actor network: $\mathbf{P} = \frac{\mathbf{P}}{\sqrt{P_{Max}}}$. Similarly, to meet the constraint of $|\Phi_l| = 1, l \in N_I$, we normalize Φ_l using the same way. The value of Φ_l is complex number, so its real and imaginary parts should be calculated separately: $\Re(\Phi_l) = \frac{\Re(\Phi_l)}{\sqrt{\Re(\Phi_l)^2 + \Im(\Phi_l)^2}}, \Im(\Phi_l) = \frac{\Im(\Phi_l)}{\sqrt{\Re(\Phi_l)^2 + \Im(\Phi_l)^2}}$. Simulations show that the deployment of well-designed IRS in NOMA-based FL system can greatly impede the wire-tap channel from devices to Eve, securing the FL training process.

IV. Conclusion

This article investigates an IRS-assisted NOMA-based FL system, where Eves can overhear the model parameters sent from IoT devices to BS, and IRS is introduced to prevent Eve from intercepting. DDPG is adopted to optimize the devices' transmission power and IRS phase shift, thereby maximize the minimum secrecy rate. Simulation results demonstrate that the secrecy rate can be significantly improved via deploying the IRS with well-designed phase shift, which implies that the IRS can effectively degrade the wire-tap channel.

References

[1] T. H. T. Le, L. Cantos, S. R. Pandey, H. Shin, and Y. H. Kim, "Federated Learning with NOMA Assisted by Multiple Intelligent Reflecting Surfaces: Latency Minimizing Optimization and Auction," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11 558–11 574, 2023.

[2] Y. Zhu, B. Mao, and N. Kato, "On a novel high accuracy positioning with intelligent reflecting surface and unscented kalman filter for intelligent transportation systems in b5g," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 1, pp. 68–77, 2024.

[3] Y. Zhu, B. Mao, and N. Kato, "A Dynamic Task Scheduling Strategy for Multi-Access Edge Computing in IRS-Aided Vehicular Networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 4, pp. 1761–1771, 2022.

[4] T. Wang, Y. Li, Y. Wu, and T. Q. Quek, "Secrecy Driven Federated Learning via Cooperative Jamming: An Approach of Latency Minimization," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 4, pp. 1687–1703, Oct. 2022.

[5] P. Consul, I. Budhiraja, and D. Garg, "A hybrid secure resource allocation and trajectory optimization approach for mobile edge computing using federated learning based on web 3.0," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023.

[6] J. Zheng, H. Zhang, J. Kang, L. Gao, J. Ren, and D. Niyato, "Covert Federated Learning via Intelligent Reflecting Surfaces," *IEEE Transactions on Communications*, vol. 71, no. 8, pp. 4591–4604, 2023.

[7] W. Wang, W. Ni, H. Tian, and L. Song, "Intelligent Omni-Surface Enhanced Aerial Secure Offloading," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5007–5022, 2022.