Privacy-preserving Mutual Authentication Protocol for Federated Learning in Intelligent Transportation Systems

Rohini Poolat Parameswarath
Department of ECE
National University of Singapore, Singapore
rohini.p@nus.edu.sg

Biplab Sikdar
Department of ECE
National University of Singapore, Singapore
bsikdar@nus.edu.sg

***Abstract*—Federated Learning (FL), which enables collaborative model training across distributed nodes, can play a significant role in Intelligent Transportation Systems (ITS). Intelligent vehicles can work collaboratively in FL networks to improve not just traffic flow but also road safety, environmental sustainability, and urban mobility. However, ensuring secure authentication among entities participating in the FL process remains a critical challenge. This paper proposes a privacy-preserving authentication protocol for FL in ITS, ensuring secure, efficient, and privacy-preserving participant verification. The proposed protocol leverages the concepts of privacy-preserving Decentralized Identifiers (DIDs) and Verifiable credentials (VCs) together with lightweight cryptographic operations. Experimental results demonstrate that the proposed protocol enhances the security and privacy protections of FL in ITS while maintaining efficient authentication compared to other existing protocols, making it a viable solution for real-world deployment in next-generation intelligent transportation systems. Additionally, its scalability makes it suitable for integration into large-scale vehicular environments.**

1. Introduction

Intelligent Transportation Systems (ITS) integrate advanced communication, sensing, and computing technologies to enhance the efficiency, safety, and sustainability of transportation networks [1]. ITS enable real-time data exchange among vehicles, roadside infrastructure, and traffic management centers, facilitating applications such as traffic control, collision avoidance, and autonomous driving [2]. ITS improve traffic flow, reduce traffic congestion, and enhance road safety and efficiency, ultimately contributing to a more intelligent and connected transportation ecosystem [3].

Federated Learning (FL) is a distributed machine learning (ML) approach that allows multiple nodes to collaboratively train a shared model without sharing actual datasets [4]. In ITS, FL can be leveraged to enhance real-time decision-making and predictive analytics while maintaining data privacy [5]. A Roadside Unit (RSU) is a device employed to enable communication between vehicles and the transportation infrastructure in ITS. The RSU can act as a communication hub and help with data processing. It can also act as an FL aggregator.

It has to be noted that FL is vulnerable to attacks since it involves a number of clients collaboratively training the model [6]. Hence, authentication is crucial in FL-based ITS to ensure that only legitimate and trusted vehicles participate in model training and updates. Without robust authentication mechanisms, adversaries can launch several attacks, inject malicious model updates, or compromise the integrity of the FL process through model poisoning and adversarial attacks. Secure authentication mechanisms are required to prevent unauthorized access, ensure accountability among participating vehicles, and safeguard the integrity of model aggregation. Also, the privacy of vehicles participating in FL must be protected. To ensure security and privacy for FL in ITS, we propose a privacy-preserving authentication protocol that enables an intelligent vehicle and the RSU to authenticate each other before participating in the FL process. The proposed protocol leverages the concepts of Decentralized Identifier (DID) and Verifiable Credential (VC). DID enables decentralized digital identity and has been standardized by the World Wide Web Consortium (W3C) DID working group [7]. A VC is a digital credential that can be cryptographically verified [8].

2. Proposed Scheme

2.1. System Model

In the system model, there are three major participants: the vehicle management system ($\mathcal{VMS}$), the intelligent vehicles ($\mathcal{IV}_i$ for $1, 2, \ldots, n$), and the road side units ($\mathcal{RSU}_i$ for $1, 2, \ldots, n$). The $\mathcal{VMS}$ is responsible for operating and maintaining the vehicles and storing information about vehicles. When the RSUs and the vehicles register with the $\mathcal{VMS}$, the $\mathcal{VMS}$ issues verifiable credentials to them. The $\mathcal{RSU}$s act as the FL aggregators. During FL training, the vehicles get the global model from the $\mathcal{RSU}$, train it locally with their local data, and send the locally trained models back to the $\mathcal{RSU}$ where they are aggregated and the global model is updated.

2.2. Proposed Authentication Protocol

The proposed protocol involves three phases: registration, mutual authentication, and model aggregation. The registration phase is required to be executed only once for each vehicle and RSU. We assume that the communication channels used in this phase are secure. However, mutual authentication is required for each iteration of model aggregation.

Registration Phase: In the registration phase, RSUs and vehicles register with the $\mathcal{VMS}$. Each registered entity receives a verifiable credential signed by the $\mathcal{VMS}$.

Mutual Authentication Phase: When $\mathcal{RSU}_i$ and $\mathcal{IV}_i$ want to authenticate each other, each party encrypts its credential with the other party's public key. Upon receiving the credential, the received party decrypts it with its private key and then verifies the decrypted credential using the public key of the $\mathcal{VMS}$. After successful credential verification, $\mathcal{RSU}_i$ and $\mathcal{IV}_i$ establish a session key.

Model Aggregation Phase: In this phase, $\mathcal{IV}_i$ trains the FL model locally using its data. Then, $\mathcal{IV}_i$ encrypts and sends the model update to $\mathcal{RSU}_i$ together with the current timestamp. $\mathcal{RSU}_i$ checks the received timestamp and ensures that it is not a replayed message and decrypts the model update. Similarly, $\mathcal{RSU}_i$ receives model updates from other vehicles as well and aggregates valid updates to improve the global FL model.

3. Evaluation

3.1. Security Properties

The proposed protocol ensures privacy of vehicles, protection from replay attacks, eavesdropping and Man-In-The-Middle attacks protection, mutual authentication, session key agreement, and protection against impersonation attacks.

3.2. Performance Analysis

Next, we compute the computation cost during the mutual authentication and model aggregation phases and perform a scalability analysis. In addition, we compare the computation cost with that of the protocols in three recent papers ([9], [10], and [11]). The simulations were carried out using Python. Figure 1 and Figure 2 illustrate the estimated computation costs and the computation costs at RSU/Server as a function of the number of vehicles, respectively. The analyses show that the computation cost of the proposed protocol is less than that of similar protocols, and the proposed protocol is highly scalable.

4. Conclusion

In this paper, we proposed a privacy-preserving mutual authentication protocol for the FL process in ITS. The proposed protocol ensures that only legitimate vehicles and legitimate RSUs participate in the FL process. The proposed protocol enables reliable identity verification, preserves privacy, and provides protection from several attacks by employing DID and VC. Our analyses demonstrate that the proposed protocol achieves secure authentication with low computation cost.

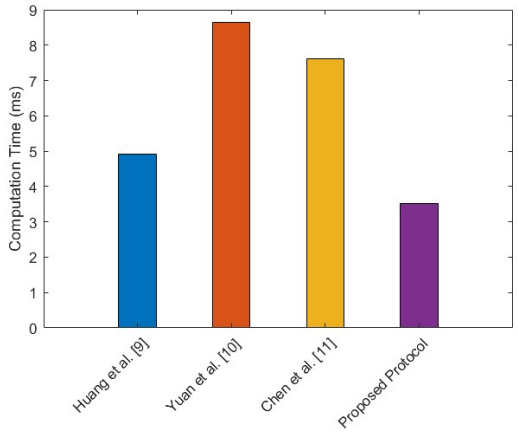

Figure 1. Comparison of computation cost.

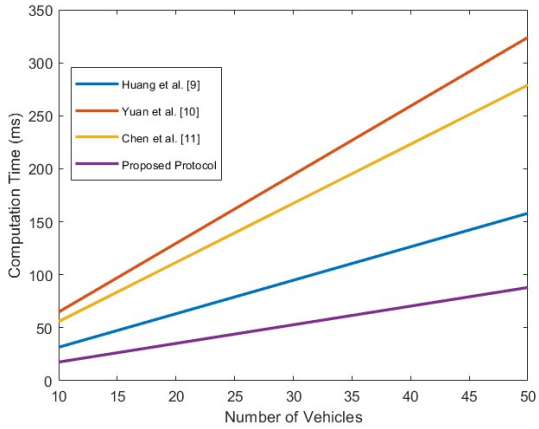

Figure 2. Computation cost at RSU/Server as a function of number of vehicles.

Acknowledgment

This research was supported by the National Research Foundation, Singapore and Infocomm Media Development Authority under its Future Communications Research Development Programme, under grant FCP-NUSRG-2022-019. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore and Infocomm Media Development Authority.

References

[1] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.

[2] T. Yuan, W. da Rocha Neto, C. E. Rothenberg, K. Obraczka, C. Barakat, and T. Turletti, "Machine learning for next-generation intelligent transportation systems: A survey," *Transactions on emerging telecommunications technologies*, vol. 33, no. 4, p. e4427, 2022.

[3] R. Jabbar, E. Dhib, A. B. Said, M. Krichen, N. Fetais, E. Zaidan, and K. Barkaoui, "Blockchain technology for intelligent transportation systems: A systematic literature review," *IEEE Access*, vol. 10, pp. 20 995–21 031, 2022.

[4] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[5] Y. Li, X. Tao, X. Zhang, J. Liu, and J. Xu, "Privacy-preserved federated learning for autonomous driving," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8423–8434, 2022.

[6] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Generation Computer Systems*, vol. 115, pp. 619–640, 2021.

[7] "Decentralized Identifiers (DIDs)," Online, https://www.w3.org/TR/did-core/, [Accessed: Aug 2024].

[8] "Verifiable Credentials Data Model 1.0," Online, https://www.w3.org/TR/vc-data-model/, [Accessed: Aug 2024].

[9] Y. Huang, G. Xu, Q. Wang, X. Song, and X. Wang, "Efficient and privacy-preserving authentication for federated learning in industrial internet of things data sharing application," *IEEE Internet of Things Journal*, pp. 1–1, 2024.

[10] X. Yuan, J. Liu, B. Wang, W. Wang, B. Wang, T. Li, X. Ma, and W. Pedrycz, "Fedcomm: A privacy-enhanced and efficient authentication protocol for federated learning in vehicular ad-hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 777–792, 2024.

[11] Y. Chen, Y. Su, M. Zhang, H. Chai, Y. Wei, and S. Yu, "Fedtor: An anonymous framework of federated learning in internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18 620–18 631, 2022.