Quantum-Secured Intra-Twin Communication for Vehicular Digital Twin Networks

Awais Khan, Haejoon Jung, and Hyundong Shin
Department of Electronics and Information Convergence Engineering, Kyung Hee University, Korea
Email: hshin@khu.ac.kr

***Abstract*—A vehicular digital twin (VDT) network can effectively address the issues of autonomous vehicles by collecting and processing the vehicle's data on a digital twin. Nevertheless, security is a primary concern due to the sensitivity of the data. In this article, we propose a protocol to establish a secure communication channel between vehicle and its corresponding digital twin with the help of the communication service provider. The analysis of the proposed protocol shows that it is robust against attacks.**

I. Introduction

In the recent years, vehicular digital twin (VDT) network has become an emerging paradigm to address the issues of the autonomous vehicles and can provide better services to users [1]. The VDT is defined as the digital representation of the physical vehicle on the cloud, which synchronizes the vehicle sensitive data. By introducing the digital twin technique, vehicles upload their sensitive data on digital twin (process that data relying on cloud computing) via intra-twin communication. Autonomous vehicles data is considered sensitive and any modification in the data will lead to a disaster. Then, the security is a major concern in intra-twin communication. On the other hand, the security of all classical communication have their limits in the sense that they can never be unconditionally secure. To solve this problem, the properties of quantum physics and quantum information, in particular the no-cloning theorem [2] and monogamy of entanglement [3] is utilized to achieve high levels of security and privacy that are not possible using classical cryptography [4]–[7].

In this work, we propose the quantum-secured intra-twin communication for VDT networks. This protocols establish a secure channel between vehicle and its corresponding digital twin with the help of the communication service provider (CSP). The CSP in our protocol is semi-honest that means it is allowed to misbehave on its own without any outside help. We also show the robustness of the protocol against malicious CSP and outside adversary.

II. System Model

Our network model consist of vehicle, its corresponding digital twin at the cloud, and communication service provider (CSP) that can perform local operation and classical communication. All participants are connected via quantum and classical authenticated channel as described in Fig. 1. The vehicle uploads the real time sensing data to its private digital twin with the help of CSP, this type of communication is named as intra-twin communication. CSP is responsible for the resource management of intra-twin communication. It generates and distributes GHZ states

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle_{abc} + |111\rangle_{abc}\right) \tag{1}$$

among the participants via quantum channel. After distribution of the GHZ state, vehicle perform the verification to establish a secure connection with the digital twin. Vehicle and its corresponding digital twin work together in collaboration for verification procedure with CSP. Once the secure connection is establish vehicle encrypt his sensitive information with the following unitaries:

$$K_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{and} K_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

for encoding 0 and 1, respectively. After the encryption, sensing data is available only to the digital twin.

III. Proposed Protocol

In this section, we present the quantum-secured intra-twin communication protocol.

i) CSP prepares an N ordered GHZ state similar as in (1) and divides them into three sequence, $\mathcal{D}_a$, $\mathcal{D}_b$, and $\mathcal{D}_c$. The $\mathcal{D}_a$, $\mathcal{D}_b$, and $\mathcal{D}_c$ composed of all the a, b, and c photons in N ordered GHZ state, respectively.

ii) CSP sends the sequences $\mathcal{D}_b$ and $\mathcal{D}_c$ to vehicle and digital twin, respectively. The sequence $\mathcal{D}_a$ is held by the CSP.

iii) Vehicle choose randomly a subset α of the N GHZ states and basis either computational $\{|0\rangle, |1\rangle\}$ or Hadamard $\{|+\rangle, |-\rangle\}$ for security checking. The basis for each measurement and location of these α GHZ state are announced to each participants.

iv) All participant performs a measurement in the announced basis. CSP announced the measurement results first to Vehicle via classical authenticated channel, then digital twin follows. Vehicle complete the error rate analysis by comparing the results. If the error rate is zero, they will continue with the protocol otherwise they restart the protocol from the beginning.

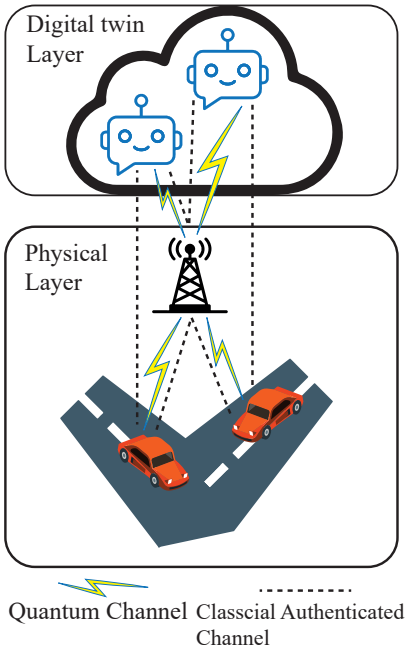

Fig. 1. System Model.

v) After the verification setup, they discard the qubits that are used for checking eavesdroppers. Vehicle choose a small subset β of the $(\mathrm{N}-\alpha)$ GHZ state to detect tampering of the data and encrypt his information on the remaining photons by applying unitaries K_0 or K_1.

vi) All participant performs a measurement in Hadamard basis. CSP and vehicle announced the results to digital twin. The digital twin calculates the result.

vii) Vehicle announced the location of β subset of GHZ state. The digital twin check if error rate is zero then data is not tempered otherwise they discard the data and restart the protocol.

IV. Security Analysis

Intra-twin communication is vulnerable against attack which can effect the safe operation of VDT. In this section, we analyze the security of the proposed protocol. We consider the security of intra-twin communication in two different scenarios:

1) The outside adversary attacks the protocol during the transmission of quantum resources or the CSP attacks the protocol during the preparation of the quantum states.

2) The CSP attacks the protocol by tampering with the data by announcing false measurement results or applying random unitaries.

In the first scenario, the sequences $\mathcal{D}_b$ and $\mathcal{D}_c$ are transmitted only once during the whole process of the protocol via quantum channel. Therefore, this is the only chance for CSP or outside adversary to carry out their attacks. This means that adversaries have to perform active attacks (e.g. intercept and resend attack or man in the middle attack etc.) to get the private information. CSP can perform the attack by preparing false state other than GHZ state to capture the data. While the outside adversary can perform the attack during the transmission of the GHZ state from CSP to vehicle and the digital twin. However, any misadventure by outsider adversary or CSP will introduced errors and the state will no longer in (1). The state will be in GHZ state, if and only if it satisfy both of the following conditions: 1) when all participant measure their qubits in computational basis and measurement outcomes are same, and 2) when measurements are performed in the Hadamard basis by all the participants and sum of the measurement outcomes are 0 modulo 2. So, both of these attack will be detected during the verification setup (iii & iv) of the GHZ state.

In the second scenario, the CSP can perform the attack by applying unitaries or announcing false measurement results. This attack can modify the data send by the vehicle to its corresponding digital twin. However, any manipulating of the data will be detected during the last three steps of the protocol.

V. Conclusion

We have proposed a quantum-secured intra-twin communication protocol for vehicular digital twin networks. The proposed protocol established a secure connection between the vehicle and its corresponding digital twin with the help of CSP. Furthermore, the security analysis is provided to show its robustness against the malicious CSP and outside adversary.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1A2C2007037) and the MSIT (Ministry of Science and ICT) ITRC (Information Technology Research Center) support program (IITP-2021-0-02046) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

References

[1] C. He, T. H. Luan, R. Lu, Z. Su, and M. Dong, "Security and privacy in vehicular digital twin networks: Challenges and solutions," *IEEE Wirel. Commun.*, pp. 1–8, 2022.

[2] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, "Quantum cloning," *Rev. Mod. Phys.*, vol. 77, no. 4, p. 1225, Nov. 2005.

[3] A. Khan, J. ur Rehman, K. Wang, and H. Shin, "Unified monogamy relations of multipartite entanglement," *Sci. Rep.*, vol. 9, no. 1, p. 16419, Nov. 2019.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[5] A. Khan, J. ur Rehman, and H. Shin, "Quantum anonymous notification for network-based applications," *Quantum Inf. Process.*, vol. 20, no. 12, p. 397, Nov. 2021.

[6] A. Khan, U. Khalid, J. ur Rehman, K. Lee, and H. Shin, "Quantum anonymous collision detection for quantum networks," *EPJ Quantum Technol.*, vol. 8, Dec. 2021.

[7] A. Khan, U. Khalid, J. ur Rehman, and H. Shin, "Quantum anonymous private information retrieval for distributed networks," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4026–4037, 2022.