Quantum Superdense Coding-Based Secure Authentication for Military Metaverse

Esmot Ara Tuli, Mohtasin Golam, Jae-Min Lee, and Dong-Seong Kim
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(esmot, golam248, ljmpaul, and dskim)@kumoh.ac.kr

***Abstract*—Ensuring security in the metaverse is crucial, especially when considering its association with the military or defense system, where an exceptionally high level of security is imperative. This paper presents quantum superdense coding-based secure authentication (QSCSA) as a high-level security solution for the extremely sensitive military metaverse. By harnessing the principles of quantum mechanics, the system achieves a higher level of security, ensuring confidentiality and integrity within the military metaverse.**

***Index Terms*—Metaverse, metaverse authentication, superdense coding, quantum network.**

I. Introduction

The Metaverse signifies a fundamental change in how individuals engage with digital material, transitioning from passive consumption to active participation, transforming human connection, entertainment, and communication [1], [2]. The metaverse, originally used for civilian applications, is now undergoing special purposes for example, military-oriented development, referred to as the ”battle-verse” or ”military metaverse”. It investigates the advantages and strategies for focusing on metaverses, with a particular emphasis on the importance of comprehending the possible repercussions of compromising this virtual world [3].

In the real world, military purposes require a particularly high level of security compared to other areas. This is the same for the virtual world as well. The military metaverse is associated with sensitive activities that pose challenges in the real world. For instance, convening meetings with high-level decision-makers can be conducted within the military metaverse, offering a secure alternative of real-world meeting. In contrast, arranging meetings in the physical world between two parties from different parts of the world carries a high risk of information leakage to adversaries. Additionally, traditional communication methods, such as conversations over a hotline phone or through the conventional internet, lack adequate security and cannot guarantee the prevention of information dissemination into unauthorized hands. Additional activities within the military metaverse may include joint military drills in the metaverse, the sharing of defense technology, transactions related to weapons, and various other engagements.

Quantum computing emerges as a prominent and promising technology with applications in various sectors, including healthcare, medicine, drug development, chemical reaction simulation, artificial intelligence, security systems, supercomputing, and more. Leveraging principles from quantum physics, quantum computers exhibit unique features such as the impossibility of qubit cloning, entanglement, and superposition, which give quantum computers superiority over classical computers [4]. Even classical information security systems are vulnerable to powerful quantum computers. Despite excellent features, quantum computers have certain limitations. One major limitation is related to quantum hardware, which involves challenges in installation and maintenance due to the requirement of extremely low temperatures. Additionally, qubits have a limited lifespan, and long-distance transfer of qubits poses difficulties [5].

Given the limitations outlined in existing quantum computers, we propose the quantum superdense coding-based secure authentication (QSCSA) scheme, which has the potential for implementation although it has limitations in the current quantum computing system. Superdense coding shares similarities with teleportation, but it differs in that teleportation requires the transmission of qubits, while superdense coding enables the transmission of classical bits. Superdense coding facilitates the transmission of two classical bits using one qubit from each node at the cost of one entangled bit (e-bit) of entanglement.

II. Proposed System

Figure 1 presents the foundational model of the QSCSA concept. If User A wants to join the metaverse, send an authentication request to User B in a quantum channel via quantum satellite using superdense coding. Upon both parties' agreement, users can join the metaverse. Let, User A possess qubit A, and User B holds qubit B. The combination of these two qubits, denoted as (A, B), establishes the qubit state $|\phi^+>$. When User A intends to enter the metaverse for a meeting with User B, an authentication request using superdense coding is initiated by User A, transmitting a two-classic-bit (b_1, b_2) message through the quantum satellite.

The rationale behind incorporating a quantum satellite lies in the fact that quantum systems necessitate operating at temperatures near absolute zero (-459 degrees Fahrenheit), a condition achievable in space. This makes the implementation of quantum

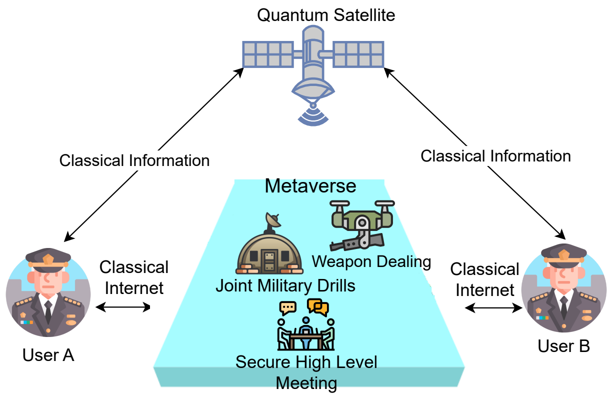

Fig. 1: Propose system model for QSCSA in the military metaverse.

systems in space feasible, consequently enabling millimeter-wave (mmWave) terahertz intra-satellite communication. The successful transfer of qubits from a satellite to the ground by China further demonstrates the potential for implementing quantum technology in communication [6]. However, after receiving an authentication request from User A to User B, User B measures the state of the qubit and gets the information that was sent by User A. User B can provide acceptance or denial feedback through the same process. It is essential to highlight that the authentication process may involve any classical biometric authentication or blockchain-based method. As the information traverses the quantum channel, it remains secure against both classical and quantum attacks, as well as man-in-the-middle attacks.

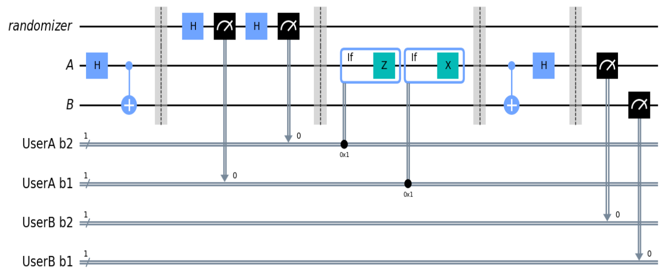

Fig. 2: Circuit Diagram of superdense coding. Here, b_1 and b_2 are classical bit produced by randomizer. A an B are quantum register. User A transmits two bits b_1 and b_2 to User B.

III. Implementation Description

The simulation of superdense coding is conducted on the IBM Quantum Computing platform, called Qiskit. Qiskit is well-documented and can be integrated with metaverse creation platforms such as Unity3D and Unreal Engine, facilitating the convenient execution and testing of metaverse simulations using quantum computers. In Figure 2, the circuit diagram of superdense coding is depicted. It illustrates the process where User A transmits any two random bits to User B. User A can send information as it is or shift it to one of the Bell states by using $1, X, ZorXZ$. Fig. 3 displays the measurement of qubit values, affirming the accurate reception of information by User B.

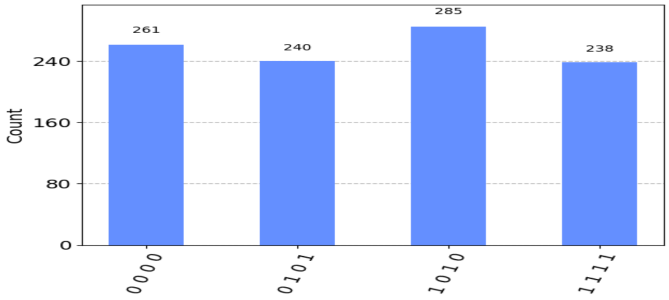

Fig. 3: Measurement of qubit.

IV. Conclusion

This paper proposes the superdense coding-based scheme QSCSA for secure authentication in the military metaverse. By leveraging principles from quantum superdense coding, the QSCSA framework enhances security in traditional authentication techniques for the metaverse. In future work, there is scope to implement sending multiple classical pieces of information using superdense code, which can allow the transmission of sensitive information over superdense code.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization programme through the Institute of IITP grant funded by the Korean government (MSIT) (IITP-2024-2020-0-01612, 50%) and by Priority Research Centres Programme through the NRF funded by the MEST (2018R1A6A1A03024003, 50%)

References

[1] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, “A survey on metaverse: Fundamentals, security, and privacy,” *IEEE Communications Surveys & Tutorials*, 2022.

[2] E. A. Tuli, A. Zainudin, M. J. A. Shanto, J. M. Lee, and D.-S. Kim, “Mediapipe-based real-time interactive avatar generation for metaverse,” , pp. 1370–1371, 2023.

[3] R. Solly and J. McArdle, “Unlocking the military potential of the metaverse,” 2022.

[4] A. Bayerstadler, G. Becquin, J. Binder, T. Botter, H. Ehm, T. Ehmer, M. Erdmann, N. Gaus, P. Harbach, M. Hess *et al.*, “Industry quantum computing applications,” *EPJ Quantum Technology*, vol. 8, no. 1, p. 25, 2021.

[5] F. Bova, A. Goldfarb, and R. G. Melko, “Commercial applications of quantum computing,” *EPJ quantum technology*, vol. 8, no. 1, p. 2, 2021.

[6] B. Li, Y. Cao, Y.-H. Li, W.-Q. Cai, W.-Y. Liu, J.-G. Ren, S.-K. Liao, H.-N. Wu, S.-L. Li, L. Li *et al.*, “Quantum state transfer over 1200 km assisted by prior distributed entanglement,” *Physical Review Letters*, vol. 128, no. 17, p. 170501, 2022.