ASEC 2024 Conference
The 5th International Electronic Conference on Applied Sciences
04–06 December 2024 | Online
MDPI

Application of quantum key distribution to protect data transmission from UAVs in geographic information systems for monitoring forest fires

Makhabbat Bakyt[1], Khuralay Moldamurat[1], Luigi La Spada[2], Sabyrzhan Atanov[1]
1 L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
2 School of Computing, Engineering and the Built Environment, Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, United Kingdom

INTRODUCTION & AIM

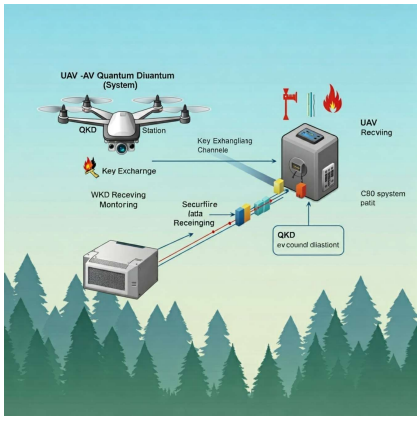
The increasing reliance on Unmanned Aerial Vehicles (UAVs) and AI in agrotechnical activities, particularly for tasks like forest fire monitoring and precision agriculture, necessitates robust data security measures. Traditional encryption methods are vulnerable to attacks from emerging quantum computing technologies. This study investigates the feasibility and effectiveness of Quantum Key Distribution (QKD) to secure data transmission in UAV-based Geographic Information Systems (GIS). The aim is to establish a secure communication channel between UAVs and ground stations, ensuring data integrity and confidentiality for critical agricultural monitoring applications.

METHOD

This research employs the BB84 protocol with polarization of weak coherent pulses for QKD. This protocol allows for the secure distribution of encryption keys between UAVs and ground stations. The study involves simulating the QKD process, taking into account the hardware requirements for both UAVs and ground stations, including compact lasers, polarization modulators, microlenses, polarization filters, and single-photon detectors. Furthermore, the simulation considers the practical constraints of UAV deployment, such as limited payload capacity, power restrictions, and the influence of atmospheric conditions on signal transmission.

RESULTS & DISCUSSION

Simulation results demonstrate that QKD can achieve key generation speeds sufficient for real-time secure data transmission in UAV-based GIS, even with the limitations imposed by UAV platforms. The study analyzes the impact of factors like atmospheric conditions (e.g., turbulence, scattering), geometric losses, and receiver characteristics on the communication range and stability of the QKD system. The findings indicate that the proposed QKD method significantly enhances the security of data transmission in agricultural monitoring applications, protecting sensitive information from potential cyber threats.



Secure Data Transmission from UAV to Ground Station via QKD

CONCLUSION

This study demonstrates the potential of Quantum Key Distribution (QKD) to address the critical need for secure data transmission in UAV-based GIS for agricultural monitoring. By leveraging the principles of quantum mechanics, QKD offers a robust solution to protect sensitive data from the threat of quantum computing attacks. The simulation results confirm the feasibility of achieving secure and real-time communication between UAVs and ground stations, even under the constraints of limited UAV resources and challenging environmental conditions. This research lays the groundwork for future practical implementations and the integration of QKD into existing agricultural monitoring systems, paving the way for enhanced security and efficiency in agrotechnical activities.

FUTURE WORK / REFERENCES

Future research will focus on:

- Practical Implementation: Moving from simulation to real-world testing and deployment of the QKD system on actual UAV platforms.
- System Optimization: Refining the QKD system design to further improve its performance and efficiency in UAV-specific scenarios, considering factors like weight, power consumption, and size constraints.
- Integration: Integrating QKD with existing communication systems and data transfer protocols used in agricultural applications to ensure seamless interoperability and compatibility.

This research aims to contribute to the development of a robust and secure support system for agrotechnical activities, enabling the effective use of advanced technologies like AI and UAVs to improve the efficiency and security of agricultural production.

1. Lai Q, Liu Y, Yang L. Remote sensing image encryption algorithm utilizing 2D Logistic memristive hyperchaotic map and SHA-512. Sci China Tech Sci, 2024, 67: 1553–1566, https://doi.org/10.1007/s11431-023-2584-y
2. Zhang Z, Teng L. Double-image coupling encryption algorithm based on TLCS and misplacement diffusion. Multimedia Tools and Applications, 2024. https://doi.org/10.1007/s11042-024-18432-4
3. Picciariello F, Vedovato F, Orsucci D, et al. Quantum-secured time transfer between precise timing facilities: a feld trial with simulated satellite links. GPS Solutions, 2024, 28: 48. https://doi.org/10.1007/s10291-023-01580-9 Lai Q, Liu Y, Yang L. Remote sensing image encryption algorithm utilizing 2D Logistic memristive hyperchaotic map and SHA-512. Sci China Tech Sci, 2024, 67: 1553–1566, https://doi.org/10.1007/s11431-023-2584-y
4. Guo Z, Feng D, Gong C, et al. A new image encryption scheme based on 3D Sine-adjusted-Logistic map and DNA coding. In: 2021 IEEE 24th International Conference on Computational Science and Engineering (CSE). 2021. p. 27-34.
5. Komma A, Gopathoti KK, Joga R, et al. FPGA Implementation of Arbiter PUFs for ideal Cryptographic Key Generation. In: 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE; 2021. p. 754-757.
6. Li J, Li X, Li C, et al. A Review of LEO Satellite Network Security Research. In: 2023 2nd International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI). IEEE; 2023. p. 496-501.
7. Wang H, Wen J, Liu J, Zhang H. ACKE: Asymmetric Computing Key Exchange Protocol for IoT Environments. IEEE Internet of Things Journal. 2023 Oct 15;10(20):18273-82.
8. Lee O, Vergoossen T. An updated analysis of satellite quantum-key distribution missions. Quantum Science and Technology. 2020 Jan 1;5(1):014003.
9. Chen B, Wu L, Zeadally S, He D. Dual-Server Public-Key Authenticated Encryption with Keyword Search. IEEE Transactions on Cloud Computing. 2022 Jan-Mar;10(1):322-33.