

Quantum Teleportation in Satellite Communications: Principles, Applications, and Operational Implications for Global Network Security

Dylan M. Charlton

United States Army

ABSTRACT

As satellite communications continue to be an integral part of global infrastructure, they face escalating cybersecurity threats and bandwidth limitations. Traditional cryptographic methods are increasingly vulnerable due to advancements in quantum computing. Quantum teleportation, leveraging quantum entanglement and quantum key distribution, offers a transformative approach to secure satellite communications. This paper lays out the foundational principles of quantum entanglement and quantum key distribution in order to allow for a complete understanding of quantum teleportation. Key experimental milestones for quantum teleportation in space environments are also discussed, such as the Chinese Micius satellite's achievements and Boeing's Q4S entanglement swapping mission. The benefits and possibilities of quantum teleportation, such as reduced signal attenuation, enhanced data integrity, and bandwidth optimization are analyzed alongside technical challenges and potential limitations like atmospheric interference and system vulnerabilities. These are brought up to showcase the potential of quantum teleportation to revolutionize satellite transmissions by enhancing secure satellite communications. Current implementations, future prospects, and challenges are laid out to highlight the role of quantum teleportation in national security, data sovereignty, and establishing secure communication networks on a global, and potentially interplanetary scale.

Keywords: Quantum Teleportation, Satellite Communication, Bandwidth Limitations, Secure Communications

Teletransportación cuántica en comunicaciones por satélite: principios, aplicaciones e implicaciones operativas para la seguridad de las redes globales

RESUMEN

A medida que las comunicaciones por satélite siguen siendo una parte integral de la infraestructura global, se enfrentan a crecientes amenazas de ciberseguridad y limitaciones de ancho de banda. Los métodos criptográficos tradicionales son cada vez más vulnerables debido a los avances en la computación cuántica. La teletransportación cuántica, que aprovecha el entrelazamiento cuántico y la distribución de claves cuánticas, ofrece un enfoque transformador para la seguridad de las comunicaciones por satélite. Este artículo expone los principios fundamentales del entrelazamiento cuántico y la distribución de claves cuánticas para permitir una comprensión completa de la teletransportación cuántica. También se analizan hitos experimentales clave para la teletransportación cuántica en entornos espaciales, como los logros del satélite chino Micius y la misión de intercambio de entrelazamiento Q4S de Boeing. Se analizan los beneficios y las posibilidades de la teletransportación cuántica, como la reducción de la atenuación de la señal, la mejora de la integridad de los datos y la optimización del ancho de banda, junto con los desafíos técnicos y las posibles limitaciones, como la interferencia atmosférica y las vulnerabilidades del sistema. Estos aspectos se presentan para demostrar el potencial de la teletransportación cuántica para revolucionar las transmisiones por satélite mediante la mejora de la seguridad de las comunicaciones por satélite. Se presentan las implementaciones actuales, las perspectivas futuras y los desafíos para destacar el papel de la teletransportación cuántica en la seguridad nacional, la soberanía de los datos y el establecimiento de redes de comunicación seguras a escala global y, potencialmente, interplanetaria.

Palabras clave: Teletransportación cuántica, Comunicación por satélite, Limitaciones de ancho de banda, Comunicaciones seguras

卫星通信中的量子隐形传态：原理、应用及对全球网络安全的运行影响

摘要

随着卫星通信日益成为全球基础设施不可或缺的一部分，其面临的网络安全威胁和带宽限制问题也愈发严峻。受量子计算技术进步的影响，传统加密方法的安全性正面临日益严峻的挑战。量子隐形传态技术利用量子纠缠和量子密钥分发原理，为实现安全的卫星通信提供了一种变革性的解决方案。本文阐述了量子纠缠与量子密钥分发的基本原理，旨在帮助读者全面理解量子隐形传态技术。文中还探讨了空间环境下量子隐形传态的关键实验里程碑，例如中国“墨子号”卫星取得的成就以及波音公司的Q4S纠缠交换任务。本文分析了量子隐形传态的优势与应用前景——如降低信号衰减、增强数据完整性及优化带宽利用率——同时也探讨了大气干扰和系统漏洞等技术挑战与潜在局限性。通过这些分析，本文展示了量子隐形传态在提升卫星通信安全性、进而彻底变革卫星传输模式方面的巨大潜力。最后，本文概述了该技术的当前应用现状、未来前景及面临的挑战，强调了量子隐形传态在维护国家安全、保障数据主权以及构建全球乃至行星际安全通信网络方面的重要作用。

关键词：量子隐形传态，卫星通信，带宽限制，安全通信

Introduction

In recent decades, humanity has become increasingly reliant on satellite communications for almost all forms of communication. Satellite communication is critical to a wide range of applications, and the successful operation of global networks. These applications include navigation systems, weather forecasting, military operations, and global broadcasting systems, all of which depend heavily on the integrity and security of satellite links. However, this reliance has led to an increas-

ingly dangerous cybersecurity threat, as well as limited bandwidth availability. The growing number of satellites and the increasing volume of data transmitted have strained existing bandwidth capacities, leading to potential bottlenecks and reduced efficiency in data transmission (Aygur et al., 2025). The proliferation of interconnected devices and the expansion of global communication networks have amplified the importance of secure and efficient satellite communication systems.

There have been a number of methods and techniques to mitigate

the possibility of eavesdropping and data interception in satellite communication, including cryptographic techniques. These traditional methods often involve complex encryption algorithms designed to protect data integrity and confidentiality during transmission (Kang et al., 2024). Nonetheless, even these techniques pose a risk for breaches given advancements being made in computational power and quantum computing (Baseri et al., 2024). Quantum computers, with their ability to process information at unprecedented speeds, threaten to render current encryption methods obsolete by efficiently solving problems that are currently difficult for classical computers. Traditional encryption methods are somewhat effective against current computational threats but are increasingly vulnerable to these emerging technologies that can potentially decrypt data that was once considered secure. For example, algorithms like Shor's algorithm can factor large prime numbers exponentially faster than classical algorithms, which are comprised of widely used encryption schemes such as Rivest-Shamir-Adleman (Khanal & Kaur, 2025).

The advent of quantum computing introduces a paradigm shift in data security, necessitating the development of novel communication protocols that can withstand quantum level threats. This shift has prompted researchers and organizations worldwide to explore quantum resistant cryptographic methods and to invest in quantum safe communication infrastructures (Baseri et al., 2024). In response to this, there is one communications method in its

infancy that shows a vast amount of promise. Quantum teleportation has proven to be a capable ultra secure method of making communication virtually impervious to hackers (Abbasi et al., 2024). Quantum teleportation enables the transfer of quantum states between distant parties without the need to transmit the actual particles, eliminating the risk of interception during transmission. This method leverages the principles of quantum entanglement to transmit information in a manner that is fundamentally secure against interception. Entangled particles exhibit correlations that are preserved regardless of the distance separating them, ensuring that any attempt to eavesdrop on the communication would be immediately detectable due to the disturbance it would cause in the quantum system (Khan et al., 2024).

Challenges of quantum teleportation include maintaining the coherence of quantum states over long distances and developing reliable quantum repeaters to extend the range of quantum communication. However, integrating quantum teleportation with satellite systems could not only enhance security but also improve the efficiency and reliability of data transmission across vast distances. Despite the challenges that come along with this technology, the benefits it produces will be invaluable when utilized alongside satellite communications. Satellites equipped with quantum communication capabilities can serve as nodes in a global quantum network, facilitating secure communication channels between ground stations separated by thousands

of kilometers (Khan et al., 2024). As research and development in this field continue to advance, the implementation of quantum teleportation in satellite communications stands to become a foundation for next generation secure communication infrastructure. This integration promises to usher in a new era of communication where data security is guaranteed by the fundamental laws of physics rather than computational complexity.

By enabling the instantaneous transfer of a quantum state, quantum teleportation can significantly reduce the latency associated with traditional communication methods, resulting in optimized bandwidth usage. Additionally, the combination of quantum teleportation and quantum key distribution can provide a robust framework for secure communication, where encryption keys are generated and distributed in a manner that is inherently secure against any form of interception or tampering. This change in thinking in communication technology holds the promise of not only enhancing the security of satellite communications but also transforming the very foundations of how information is transmitted and protected in the digital age. Quantum teleportation has the potential to revolutionize secure satellite data transmissions and free up essential bandwidth through the utilization of quantum entanglement and quantum key distribution, significantly reducing the attack surface for cybersecurity threats through its fundamentally physics-based security properties.

Literature Review

The body of work surrounding quantum teleportation in relation to satellite communications has expanded rapidly, centering mainly around four domains: foundational theory, experimental validation, security architecture, and emerging applications.

Theoretical foundations have been well established in recent years. Hu et al. (2023) survey progress in quantum teleportation across qubit modalities and transfer protocols, while Sidhu et al. (2021) map the full landscape of space quantum communications, highlighting challenges related to atmospheric interference, decoherence, and photon loss. Pirandola (2021) complements both articles by establishing fundamental performance bounds for satellite quantum systems, providing a theoretical ceiling against which real world implementations can be measured.

Experimental literature is anchored by the accomplishments of China's Micius satellite. Ren et al. (2017) documented the first successful ground to satellite quantum teleportation across more than 1,400 kilometers, a distance greater than what ground-based fiber systems can achieve. Lu et al. (2022) reviewed the full suite of Micius experiments, including the landmark intercontinental QKD link between China and Austria. Gonzalez-Raya et al. (2024) extended this work by modeling continuous variable entanglement distribution for future network architectures, while Ghalaii et al. (2023) ana-

lyzed QKD performance in the presence of bypass channels, adding essential nuance for real world deployment.

Research in quantum security has also grown in urgency alongside advances in quantum computing. Basseri et al. (2024) evaluate quantum safe protocols and identify residual vulnerabilities including side channel attacks, while Khanal and Kaur (2025) analyze how algorithms like Shor's threaten existing public-key cryptographic infrastructure. This provides the clearest case for why quantum native communications are not merely preferable, but necessary. Ain et al. (2025) offer a specific treatment of BB84 and E91 QKD protocols and their resilience against eavesdropping.

Work regarding emerging applications of quantum teleportation in satellite communications has begun moving beyond point to point security. Nande et al. (2024) examine quantum synchronization for satellite positioning, suggesting quantum payloads will serve dual functions across navigation and communications. De Forges de Parny et al. (2023) provide an operationally focused roadmap for satellite-based quantum networks bridging theoretical possibility and systems engineering, while Berera and Calderón-Figueroa (2022) address the viability of quantum communication across interplanetary distances.

Despite this wide range of research, significant gaps remain. Most published work addresses technical feasibility or cryptographic security in isolation. Far less attention has been given

to simultaneously optimizing security and bandwidth efficiency through quantum teleportation. Strategic, doctrinal, and policy dimensions are rarely treated as primary analytical concerns, and the governance frameworks needed to standardize interoperability across potential future international quantum networks remain underdeveloped relative to the engineering literature. These gaps can be addressed by treating security and bandwidth optimization as complementary priorities and situating findings within a strategic context directly relevant to national security and global communications architecture.

Principles of Quantum Teleportation

In order to effectively explain how quantum teleportation can enhance and secure satellite communications, it is important to first describe the principles and foundations of quantum teleportation itself. Stated plainly, quantum teleportation is the process in which the state of a particle (in this case a qubit) can be transferred from one user to another without sending the qubit directly through classical means (Hu et al., 2023). For context, this phenomenon is not about the physical transportation of matter, but rather the transmission of quantum information, preserving the integrity and security of the data involved. This distinction is important, as it highlights the fundamental difference between quantum teleportation in reality, and the concept of teleportation that exists only in science fiction.

The first step of quantum teleportation is for the two separate users to share a pair of entangled qubits. Quantum entanglement is the situation in which two or more qubits are linked in a way where the state of one qubit instantaneously influences the state of the other no matter how far they are from each other (Levin, 2024). These qubits will also remain entangled regardless of the distance between them (Levin, 2024). Therefore, once the state of one qubit is measured, the state of the other qubit is instantly defined as well (Pfaff et al., 2013). This non-local relationship defies classical intuitions and has been experimentally validated over distances exceeding 1,400 kilometers, demonstrating its robustness and possibilities for long range communication applications (Ren et al., 2017). This instantaneous correlation forms the backbone of quantum communication protocols, ensuring that any change in one qubit is reflected in its entangled partner, thereby enabling secure information transfer.

Now that the two users (A and B) each have one of the two entangled qubits, user A will be able to send the state of a third qubit to user B by performing a Bell state measurement (Levin, 2024). This measurement involves entangling the qubit whose state needs to be sent to user B, with user A's half of the entangled pair previously split up between users A and B (Levin, 2024). The Bell state measurement projects the combined state of the two qubits onto one of the four maximally entangled Bell states, effectively collapsing their joint state and entangling the third qubit's

information with user B's qubit (Chen et al., 2020).

This process is facilitated by specific quantum gates, such as a controlled-NOT gate or a Hadamard gate, which manipulate the qubits' states to achieve the desired entanglement and measurement outcomes (Wan et al., 2019). This instantly collapses user B's qubit into a related state based on the outcome of user A's Bell state measurement (Pfaff et al., 2013). It is important to note that while the quantum state transfer appears to be instantaneous, it does not violate causality due to the necessity of classical communication to complete the process. It is only the quantum state correlation that is instantaneous, not the communication itself. This requirement ensures that the overall process adheres to the fundamental principles of relativity, maintaining the causal structure of spacetime.

In order for the quantum state teleportation to be complete, user A must send two bits of classical information to user B through classical means of communication so user B can manipulate their qubit through a quantum operation, resulting in user B's qubit ending up in the same state as user A's (Hu et al., 2023). These two classical bits convey the result of the Bell state measurement and are essential for user B to apply the correct quantum gate operations, such as Pauli X or Z gates, to reconstruct the original quantum state accurately (Johansson & Larsson, 2019). Essentially, once user A entangles and measures the qubits, user B's qubit will be transformed into the same

state as the third qubit, the one user A wanted to send to user B originally, following the sharing of the measurement results (Levin, 2024).

This measurement ensures that the quantum state is faithfully transmitted without physically traversing the space between the users, a feature that is particularly advantageous for secure communications over vast distances. This capability is especially beneficial in satellite communications, where transmitting quantum information without relying on physical channels can mitigate losses and enhance security (Ghalaii et al., 2023). Therefore, the state of the qubit has been teleported from user A to user B without physically sending the qubit to user B.

Finally, the qubit whose state is being teleported from user A loses its quantum state during the process, meaning the quantum state no longer exists with user A, and only with user B (Hu et al., 2023). This highlights that this process is not a form of copying information from one user to another, but truly teleporting it to user B. This aspect is a direct consequence of the no-cloning theorem, which prohibits the creation of identical copies of an arbitrary unknown quantum state, reinforcing the security of the teleportation process (Abbasi et al., 2024).

It is also important to note that although the quantum state is instantaneously transferred between user A and B, this does not allow for faster than the speed of light communication. This is due to the need for two classical bits to be sent via classical communication

means in order for the state to be observed, and the process to be completed, as mentioned earlier. This limitation of quantum teleportation follows the no-communication theorem, which declares that quantum entanglement cannot be used to transmit information faster than light, preserving the principles of causality in physics (Khan et al., 2024). Understanding both the no-cloning and no-communication theorems is essential for developing secure quantum communication systems that leverage the advantages of quantum mechanics while adhering to the fundamental constraints imposed by the laws of physics.

Quantum Key Distribution Security

Currently, there are many methods utilized to secure satellite communications, including cryptography. However, with technological advancements, including those in quantum computing, these methods are more vulnerable than ever to breaches and hackers (Baseri et al., 2024). The advent of quantum computing threatens to render traditional encryption algorithms obsolete, as quantum algorithms like Shor's algorithm can efficiently factor large numbers, compromising Rivest-Shamir-Adleman encryption (Khanal & Kaur, 2025). Additionally, Grover's algorithm can accelerate brute force attacks on symmetric key cryptography by providing a quadratic speedup, effectively reducing the security of symmetric keys by half (Khanal & Kaur, 2025). This means that

a 128-bit symmetric key, which is currently considered secure, would offer only 64-bits of security against a quantum adversary, necessitating the use of longer keys to maintain security levels (Khanal & Kaur, 2025).

The implications of these quantum algorithms extend beyond theoretical concerns. They pose tangible threats to the confidentiality and integrity of sensitive data transmitted via satellite communications. As quantum computing technology progresses, the urgency to develop and implement quantum resistant cryptographic solutions becomes paramount to safeguard critical information infrastructures (Baseri et al., 2024).

One way quantum teleportation will be able to provide near unbreakable security for satellite communications is by being used alongside quantum key distribution. Quantum key distribution is a method of securing communication through the generation and distribution of encryption keys (Abbasi et al., 2024). Unlike classical key distribution methods, quantum key distribution utilizes the principles of quantum mechanics to ensure that any attempt at eavesdropping can be detected due to the disturbance it causes in the quantum system (Abbasi et al., 2024). On the contrary, current forms of encryption rely on mathematical algorithms which can be cracked through the aforementioned advancements in computing power (Baseri et al., 2024). This vulnerability highlights the need for cryptographic methods that are not solely dependent on computational complexity but are grounded in the fundamental laws of physics.

Quantum key distribution utilizes quantum mechanical systems to create and disperse cryptographic keys. Protocols such as BB84 and E91 have been developed to implement quantum key distribution, providing a framework for secure key exchange that is theoretically immune to quantum computer attacks (Ain et al., 2025). The BB84 protocol was introduced in 1984 and employs the polarization states of photons to encode key bits, ensuring that any eavesdropping attempt introduces detectable anomalies due to the disturbance of the quantum states (Ain et al., 2025). Similarly, the E91 protocol was introduced in 1991, which uses entangled photon pairs to establish secure keys, relying on the violation of Bell's inequalities to detect eavesdropping (Ain et al., 2025).

Currently, quantum key distribution can be utilized over classical forms of communication. However, as mentioned earlier, when paired with quantum teleportation, which could instantaneously send the states of the qubits being utilized to the end user, any interception attempt or effort to tamper with the communication would be detected (Abbasi et al., 2024). This ensures that the information about the quantum keys is exchanged securely, due to the fact that once a quantum state has been observed, it permanently collapses into that state, resulting in the destruction of its superposition (Hu et al., 2023). Essentially, if the quantum state were to be measured by anyone except the end user, the state would be destroyed. This fundamental property of quantum mechanics is known as the observer effect,

and it ensures that any eavesdropping attempt introduces detectable anomalies in the system (Polychronakos, 2024). To illustrate, if an adversary were to attempt to intercept the quantum key being sent via quantum teleportation for quantum key distribution, the end user would undoubtedly know that there was a breach.

This detection capability holds a significant advantage over classical cryptographic systems, where breaches may go unnoticed until after data has been compromised. This attests to the fact that utilizing quantum teleportation in conjunction with quantum key distribution creates communications that are nearly impervious to eavesdropping. The combination of quantum teleportation and quantum key distribution enhances the security of the communication channel, as quantum teleportation allows for the transfer of quantum states without transmitting the physical particles themselves, reducing the risk of interception. Furthermore, integrating these technologies into satellite communications can extend secure communication channels over vast distances, overcoming the limitations of terrestrial fiberoptic networks.

Application of Quantum Teleportation in Satellite Communication

With the foundational principles of quantum teleportation and quantum key distribution established, it is important to

address how they will impact and can be utilized for satellite communication. The intent behind using quantum teleportation in this manner is to address the existing constraints of ground-based communications related to transmission range, reduce the degradation of data over long distances, commonly referred to as line loss, and safeguard the information during the transfer process (Pirandola, 2021). Ground based quantum communication systems face significant challenges due to signal attenuation, noise, and free space path loss over long distances, which can degrade the fidelity of the transmitted quantum states (Dubey et al., 2024). These challenges are exacerbated by environmental factors like atmospheric turbulence and scattering, which can further disrupt quantum signals during transmission (Dubey et al., 2024).

Quantum teleportation has been tested and can be utilized in ground-based line of sight communication, as well as through fiber optic cables. However, when utilized in this way, especially through fiber optic means, photon losses increase exponentially with distance, which extremely limits the distance quantum teleportation can successfully occur due to the requirement of the classical bits that still need to be sent to the end user through classical means to complete the process (Gonzalez-Raya et al., 2024). This exponential loss of photons is primarily due to absorption and scattering in the optical fibers, which becomes prohibitive beyond certain distances (Chai et al., 2024).

The necessity of maintaining quantum coherence over long distances in fiber optics presents additional technical hurdles, such as the need for quantum repeaters (Abbasi et al., 2024). Currently, quantum teleportation has been demonstrated at a maximum distance of 100 kilometers through fiber optic cables, and 143 kilometers when utilizing free space from ground-to-ground stations (Gonzalez-Raya et al., 2024). These limitations necessitate the exploration of alternative methods to achieve long distance quantum communication.

However, when these signals are transmitted through the use of satellites, many of these limitations no longer apply. Quantum teleportation can occur over much longer distances by utilizing satellites and achieves significantly reduced signal attenuation due to the majority of the signal path traveling through the vacuum of space rather than the atmosphere (Gonzalez-Raya et al., 2024). The vacuum of space provides an ideal medium for photon transmission, minimizing losses and allowing for the establishment of global quantum communication networks (Dubey et al., 2024). This environment also significantly reduces the impact of decoherence and allows for the maintaining of entangled states over thousands of kilometers, which is essential for effective quantum teleportation (Khan et al., 2024).

Quantum teleportation has been achieved at a distance of 1,400 kilometers through the use of satellites (Ren et al., 2017). This milestone demonstrates

the feasibility of satellite-based quantum communication and has laid the groundwork for the development of a global quantum internet. Additionally, adaptive optics and error correction techniques can be employed to compensate for atmospheric disturbances to maintain the integrity of the quantum signals (Khan et al., 2024). Recent advancements in adaptive optics such as artificial intelligence powered turbulence forecasting tools and high-speed correction systems have shown promise in enhancing the stability and fidelity of quantum channels through the atmosphere (Mafu, 2024).

Satellite communications are crucial for nations to effectively conduct global security and defense, as well as respond promptly to emergencies and humanitarian crises (Lueschow & Pelaez, 2020). Quantum teleportation presents the opportunity to drastically advance the dependability and confidence placed in military satellite communications. A key threat that has emerged through the usage of satellite communication for security and defense is cybersecurity (Kang et al., 2024). Satellites are capable of passing a widespread quantity of secure data around the Earth that is critical to defensive and security operations. However, that information is vulnerable and can be retrieved by enemies through invasive procedures. To counter the growing security challenges posed by adversaries, it is necessary to implement quantum teleportation as a defensive measure.

A recent incident that showcases the urgency for more secure satellite

communications involves Russia's use of inspector satellites, like that of Kosmos-2558 (Maurin, 2023). Launched on August 1, 2022, Kosmos-2558 maneuvered into an orbit that closely matches that of USA 326, maintaining a separation of just 60 kilometers (McDowell, 2023). USA 326 is reported to carry a classified payload, and due to the close approach, Kosmos-2558 is suspected of conducting optical surveillance and possibly collecting data from it (Joint Functional Component Command for Integrated Missile Defense, 2024). This incident highlights the vulnerabilities inherent in current satellite communication systems and the pressing need for enhanced security measures. The integration of quantum teleportation into satellite communications could render espionage attempts like this ineffective, as any interception of quantum keys would be immediately detectable.

Quantum key distribution enables two distant parties to securely establish a cryptographic key, even if a third party is attempting to intercept the communication (Tedeschi et al., 2022). Yet when quantum teleportation is used to transfer the keys, even if an adversary manages to compromise the underlying cryptographic assumptions, the protocols remain effective and provide the capability to detect any potential eavesdropping on the communication link (Tedeschi et al., 2022). This dual layered security approach ensures that even if one layer is compromised, the overall integrity of the transmission remains intact. This establishes a form of communication resilience, rendering transmissions inaccessible to unautho-

rized eavesdroppers. This demonstrates that quantum teleportation in satellite communications serves as a vital defense against the continuously advancing landscape of cybersecurity threats. By leveraging the principles of quantum mechanics, these technologies offer a level of security that is fundamentally unattainable through classic means (Kang et al., 2024). Given that satellites like Kosmos-2558 may already have the capability to collect information from classified U.S. satellites, it is crucial to safeguard data using secure transmission channels.

By integrating quantum teleportation into current satellite communication systems, satellite operators could offer a level of security far beyond what is currently possible, protecting sensitive data from interception or tampering. The implementation of quantum teleportation can facilitate secure communication across the globe, which is particularly beneficial for coordinating international defense strategies and rapid response operations. This integration would not only enhance national security but also ensure the confidentiality of sensitive information across various sectors, including finance, healthcare, and critical infrastructure. As quantum technologies continue to improve, their adoption in satellite communications is poised to become a cornerstone of secure global information exchange.

Bandwidth Optimization

Another limitation in current satellite communication networks is that quantum teleportation

can mitigate is bandwidth constraints, and a congested electromagnetic spectrum. Currently, satellite communication networks utilize radio frequencies to transmit data. However, bandwidth, which is the amount of data that can be transferred over a network, is extremely limited in most of these frequencies (Secara & Hordiiuk, 2023). This results in an extremely crowded electromagnetic spectrum and interference of satellite communications. However, even in areas of the spectrum that have much more bandwidth than others, like the extremely high frequency portion, current security and encryption technology utilize so much of the bandwidth that the usable amount is still exceedingly small (Schodorf, 2000). The competition for bandwidth in the crowded radio frequency spectrum is a major challenge, especially when considering the continuous growth of communication networks.

Currently in the extremely high frequency portion of the electromagnetic spectrum, information is encrypted through advanced algorithms that generate a large amount of additional data that is required to ensure the security of the information (Schodorf, 2000). This data takes up a large amount of bandwidth in the electromagnetic spectrum, resulting in less usable bandwidth, even though extremely high frequency has such a wide frequency range. Additionally, due to potential degradation of the signal, error correction techniques such as forward error correction send additional redundant bits of information in order to correct for any lost data in the transmission process (Schodorf, 2000).

The data overhead for successfully encrypted extremely high frequency transmissions makes the extremely high frequency portion of the electromagnetic spectrum difficult to use due to the bandwidth limitations. Furthermore, the increasing demand for high-speed data transmission driven by applications such as high-definition video streaming, real time data analytics, and the proliferation of Internet of Things devices, exacerbates the strain on available bandwidth (Aygur et al., 2025). While traditional encryption methods are essential for securing data, they also introduce significant overhead, resulting in them consuming valuable bandwidth that could otherwise be allocated to actual data transmission (Abolade et al., 2021). This inefficiency becomes particularly problematic in scenarios where bandwidth is a scarce and valuable resource in satellite communications. Moreover, as the number of satellites in orbit increases, particularly in geostationary orbit, and with the deployment of large constellations for global internet coverage, the risk of frequency interference and signal congestion becomes more pronounced. This highlights the need for more efficient communication methods that can operate within the limited spectral resources available.

Quantum teleportation has the ability to limit the use of bandwidth for extremely high frequency satellite communications through its instantaneous transferring of qubits, and the use of quantum key distribution. Because quantum teleportation instantaneously transmits the quantum state correla-

tion from one particle to the other, this eliminates the need for the transfer of encrypted information over the electromagnetic spectrum, leading to a massive increase in data capacity for satellite communications, and an extreme drop in the amount of bandwidth being used for secure satellite communications (Hu et al., 2023). Essentially, cryptographic keys would not need to be sent through the electromagnetic spectrum along with the information due to quantum key distribution and quantum teleportation instantaneously transmitting the quantum keys to the end user. Keys would be sent securely without being sent as data, which would drastically reduce the amount of encryption related overhead for satellite communications in extremely high frequency bands. However, it should be noted that classical bits are still required to complete the teleportation process, so the reduction of data in the electromagnetic spectrum is significant, but not total.

By reducing the reliance on traditional encryption methods that require additional data transmission for key exchange and error correction, quantum teleportation and quantum key distribution can significantly enhance the efficiency of bandwidth utilization. This optimization not only improves the overall throughput of satellite communication systems but also enables the support of more simultaneous users and services without the need for additional spectrum allocation (de Forges de Parney et al., 2023). In addition, the implementation of quantum communication protocols can lead to the development of new network architectures

that are inherently more efficient. For example, the use of entangled photon pairs allows for the establishment of secure communication channels without the need for continuous key exchange, resulting in reducing the frequency of transmissions and conserving bandwidth (Joshi et al., 2020). Furthermore, advancements in quantum error correction techniques can minimize the need for redundant data transmission, further optimizing bandwidth usage (Khan et al., 2024).

The integration of quantum communication technologies into satellite systems can facilitate the development of more robust and scalable communication infrastructures. For example, as mentioned, the use of entangled photon pairs in quantum teleportation allows for the establishment of highly secure communication links that are less susceptible to interference and eavesdropping. This inherent security reduces the necessity for complex encryption algorithms and associated overhead, further conserving bandwidth (Joshi et al., 2020). Additionally, the adoption of quantum technologies can pave the way for innovative communication protocols that are inherently more efficient and secure, setting new standards for satellite communications (Baseri et al., 2024).

While the technology is still in its infancy, the proof of long-distance quantum teleportation showcases that quantum teleportation is a viable form of satellite communication that overcomes current traditional communication limitations. As research and

development in quantum communication continue to advance, it is anticipated that these technologies will become more accessible and cost effective, leading to their widespread adoption in satellite communication networks. This possible transition will not only enhance security and efficiency but will also potentially revolutionize the way data is transmitted across vast distances, marking a significant milestone in the evolution of global communications.

Real World Implementation

Researchers are actively exploring quantum communication technologies to counter threats like those mentioned earlier, focusing on satellite-to-ground quantum key distribution, the distribution of entangled particles, and quantum teleportation from the ground to satellites (Pirandola, 2021). The first successful quantum teleportation between two distant ground stations utilizing a satellite was the Chinese Micius satellite in 2017 (Ren et al., 2017). The Micius satellite was able to prove the capability of quantum teleportation and quantum key distribution through the use of a satellite over a long distance. The experiment successfully teleported quantum keys between two entangled qubits at two separate ground stations over 1,400 kilometers apart while utilizing a satellite (Ren et al., 2017). The distances that quantum teleportation achieved through the use of the Micius satellite were further than ever achievable through fiber optics or ground-based communication methods (Ren et al., 2017). This ground-

breaking experiment not only demonstrated the feasibility of long-distance quantum teleportation but also laid the foundation for a global scale quantum communication network.

The Micius satellite is officially one of China's Quantum Experiments at Space Scale projects. It utilized a low Earth orbit platform to minimize photon loss and decoherence, which are significant challenges in terrestrial quantum communication as mentioned earlier (Lu et al., 2022). By successfully conducting quantum teleportation over this vast distance, the experiment validated the potential of satellite-based quantum networks to overcome the limitations of ground-based systems. Furthermore, the Micius satellite facilitated the first intercontinental quantum secured communication by establishing a quantum key distribution link between China and Austria (Lu et al., 2022). This achievement showcases the satellite's capability to serve as a trusted quantum teleportation relay, enabling secure communication between distant locations on Earth, or even between Earth and distant space. The success of these experiments has also spurred international interests in developing similar quantum communication infrastructures, highlighting the strategic importance of quantum technologies in global cybersecurity and information assurance (Lu et al., 2022).

Following the vast achievements of the Micius satellites, Boeing has announced it will launch its Q4S satellite in 2026 to test quantum teleportation (Maasarani, 2024). Boeing hopes that

this satellite and the subsequent tests and experiments it will facilitate will help researchers understand how radiation and other effects in the harsh environment of space will affect quantum teleportation (Maasarani, 2024). This technology will not only revolutionize satellite communications but also create an extremely precise timing network to be utilized for positioning, navigation, and timing systems (Maasarani, 2024). While this diverges somewhat from satellite communications specifically, it does highlight how quantum teleportation will have vastly more capabilities than what it is currently being tested for, due to the technology being in its infancy.

Despite this, the Q4S mission does still represent a significant step forward in the practical implementation of quantum communication technologies. Boeing's initiative aims to demonstrate quantum entanglement swapping capabilities in orbit, a critical process for extending the range of quantum networks through the use of quantum repeaters (Boeing, 2025). By successfully performing entanglement swapping, the Q4S satellite could enable the establishment of long-distance entangled links between ground stations, effectively overcoming the distance limitations imposed by direct entanglement distribution.

The Q4S mission will also provide valuable insights into the performance of quantum systems in the space environment, where factors such as cosmic radiation, temperature fluctuations, and microgravity can impact

the stability and coherence of quantum states (Boeing, 2025). Understanding these effects is essential for the development of robust quantum communication systems capable of operating reliably in space. The data collected from the Q4S experiments will inform the design of future quantum satellites and ground stations, contributing to the maturity of quantum technologies for practical applications.

The advancements achieved through the Micius and Q4S missions have even broader implications beyond that of secure communication. The precise timing capabilities enabled by quantum technologies could enhance global navigation satellite systems, improve synchronization in financial networks, and support scientific research requiring high precision measurements (Nande et al., 2024). As quantum communication technologies continue to evolve, they hold the promise of transforming various sectors by providing unprecedented levels of security, accuracy, and efficiency.

Future Prospects

The integration of quantum teleportation and quantum key distribution into satellite communications has sparked a transformative era in secure global communications. Building upon the foundational achievements of the Micius satellite and the anticipated advancements from Boeing's Q4S mission, the trajectory of quantum communication is poised for significant growth. The successful demonstration of satellite-based

quantum teleportation has opened avenues for the development of a global quantum network (Gonzalez-Raya et al., 2024). This type of network would promise unparalleled security and utilize the principles of quantum mechanics to detect any eavesdropping attempts. The potential applications include precise timing systems, enhanced navigation, and advancements in quantum computing. The scalability of these quantum networks alone, which would be facilitated by satellite platforms, presents the opportunity to integrate quantum communication into existing infrastructures (Sidhu et al., 2021). This would enhance the resilience and security of all global communication systems (Khan et al., 2024).

Looking even further ahead, the successful integration of quantum communication technologies into satellite networks could also have profound implications for interplanetary communication. A global quantum network could serve as the backbone for extending secure communication channels to interplanetary missions, where traditional communication methods face significant latency and security challenges (Berera & Calderón-Figueroa, 2022). As space exploration missions venture further into the solar system, the need for secure and efficient communication becomes paramount. Quantum teleportation could provide a means of transmitting information across long interplanetary distances with enhanced security, overcoming the limitations of classical communication methods (Berera & Calderón-Figueroa, 2022).

An advancement of this magnitude would play a critical role in maintaining reliable communication links with spacecraft and habitats on other planets, ensuring the success and safety of future space missions. Moreover, establishing quantum communication links between Earth and other planetary bodies could pave the way for a Solar System wide quantum internet, enabling secure and efficient data exchange across interplanetary distances (Hippke, 2021). The successful implementation of quantum teleportation for interplanetary communication could revolutionize humanity's approach to space exploration, laying the groundwork for a truly interconnected Solar System.

If a global quantum communications network was ever adopted, standard protocols and regulatory frameworks would need to be established. Currently, due to the infancy of this technology, the lack of universally accepted standards hinders interoperability between different quantum systems and poses challenges for widespread deployment (Hossain, 2023). Collaborative efforts among international standardization bodies like the International Telecommunication Union (ITU) and the European Telecommunications Standards Institute (ETSI) would be critical to develop comprehensive guidelines that ensure compatibility, security, and reliability across quantum communication networks.

Extending these standards to encompass interplanetary communication would require unprecedented international cooperation and the devel-

opment of new policies to address the unique challenges posed by space environments. These challenges would include jurisdictional considerations and the coordination of quantum communication infrastructure across different planetary bodies. The path forward for the utilization of quantum teleportation in satellite communications would involve a concerted effort to address the technical, security, and regulatory challenges associated with satellite-based quantum communication. While advancements in photonic technologies, error correction methods, and satellite engineering will play pivotal roles in enhancing the performance and reliability of quantum networks, fostering international cooperation and investment will be instrumental in building a resilient and secure global quantum communication infrastructure (Khan et al., 2024). As research and development continue to progress, the vision of a quantum secure communication era becomes increasingly attainable, and it promises to redefine the landscape of global information exchange.

Technical Challenges

Despite its promising prospects, several technical hurdles regarding quantum communications and quantum teleportation must be overcome. Furthermore, in order to understand the full potential of these technologies, several critical challenges must be addressed. Firstly, atmospheric disturbances such as turbulence and background noise can play a larger factor in quantum communications than

they would for classic satellite communication capabilities (Gonzalez-Raya et al., 2024). These factors can degrade the quality of quantum signals transmitted between satellites and ground stations. For example, these disturbances can lead to events like beam wandering, wavefront distortion, and beam divergence, which collectively degrade the quality and fidelity of quantum signals transmitted through free space channels (Sidhu et al., 2021). Additionally, fluctuations in atmospheric conditions can cause scintillation effects, leading to temporal and spatial variations in signal intensity, impacting the reliability of quantum key distribution protocols (Pirandola, 2021). Maintaining precise alignment between rapidly moving satellite and ground-based receivers is another critical factor to consider in ensuring the integrity of quantum transmissions (Kang et al., 2024).

Additionally, the development of compact, robust, and space hardened quantum hardware remains a significant challenge. Quantum devices must withstand harsh space environments characterized by extreme temperatures, vacuum conditions, and elevated levels of radiation, all of which can adversely affect the performance of sensitive quantum components like single photon detectors and entangled photon sources (Sidhu et al., 2021). The excessive costs associated with launching and maintaining satellite-based quantum systems also pose economic constraints, requiring cost effective solutions and international collaboration. Deploying quantum satellites involves substantial financial investments, expenses that re-

late to research and development, manufacturing, launch services, and ground infrastructure (Rausser et al., 2023). Collaborative efforts among space faring nations and private entities will be necessary in order to share costs and expertise, resulting in the acceleration of advancements, and the eventual adoption of quantum communication technologies.

Even more importantly, while quantum communication does offer significant and inherent security advantages, it is not impervious to all threats. Potential vulnerabilities include side channel attacks, where information leakage occurs through unintended channels, and its reliance on trusted nodes, which could undermine the security of the entire network if compromised (Baseri et al., 2024). Side channel attacks exploit physical implementations of quantum systems, targeting aspects such as timing information, power consumption, or electromagnetic emissions to extract sensitive data without directly breaching the cryptographic algorithms (Baseri et al., 2024). It is also necessary to develop protocols that minimize trust assumptions, and to implement robust authentication mechanisms to fortify the security of quantum communication systems. This includes the integration of quantum resistant authentication schemes and the establishment of end-to-end security frameworks that do not rely on intermediary nodes, ultimately reducing the potential points of failure (Baseri et al., 2024).

In the context of interplanetary communication, additional challenges

such as cosmic radiation, signal attenuation over long distances, and the need for autonomous error correction mechanisms become even more pronounced, necessitating further research and innovation to ensure reliable quantum communication beyond Earth (Sidhu et al., 2021). Cosmic radiation can induce decoherence in quantum states, leading to errors in transmitted information. Signal attenuation over long distances requires the development of highly efficient quantum repeaters and error correction codes tailored for space applications (Sidhu et al., 2021). Moreover, the extremely long distances and communication delays that are inherent to interplanetary missions necessitate autonomous systems that are capable of performing error detection and correction without real time human intervention (Sidhu et al., 2021). This ensures the integrity and reliability of quantum communications in deep space environments.

Conclusion

Quantum teleportation is an extremely valuable technology that has the potential to revolutionize satellite communications due to its precision, security, and integrity. By leveraging the unique properties of quantum entanglement, quantum teleportation enables the transfer of quantum states between particles without the need for physical transmission, offering a paradigm shift in how information can be securely communicated over vast distances. In transferring the state of a qubit between entangled particles,

the possibility of fundamentally secure communications is made into a reality (Levin, 2024). This process ensures that any attempt at eavesdropping or interception can be immediately detected, because the act of measurement inherently alters the quantum state, alerting the communicating parties to security breaches.

Quantum teleportation in satellite communications overcomes many limitations in traditional communications and security. Traditional encryption methods are increasingly vulnerable to the advancements in quantum computing, which threaten to make current cryptographic techniques obsolete. With cybersecurity and communication eavesdropping becoming a major issue, the leveraging of quantum teleportation for quantum key distribution makes for ultra secure communication networks that are not possible through current secure communication methods (Baseri et al., 2024). The integration of quantum key distribution with quantum teleportation not only enhances security but also ensures that encryption keys are distributed in a manner that is fundamentally protected by the laws of quantum physics.

The teleportation of cryptographic keys over a long distance for quantum key distribution will also decrease the amount of data being sent over extremely high frequency satellite communication networks, which bypasses the bandwidth limitations that currently exist for satellite communication networks (Schodorf, 2000). By reducing the reliance on traditional data

transmission methods, quantum teleportation alleviates the congestion in the electromagnetic spectrum, optimizing bandwidth utilization and improving overall communication efficiency.

Regardless of the infancy of quantum teleportation technology, the Micius satellite has demonstrated the feasibility of its use in secure satellite communications, and Boeing has hopes of expanding and improving the technology through its Q4S satellite. The Micius satellite's successful experiments in quantum entanglement and teleportation over record breaking distances have laid the groundwork for future advancements in this field. Boeing aims to further explore the practical applications of quantum teleportation in space with Q4S, potentially leading to the development of a global quantum communication network (Boeing, 2025).

As humanity ventures further into space, the need for secure and efficient communication becomes paramount. Quantum teleportation offers a promising solution to the challenges of deep space communication, where traditional methods are hindered by latency and signal degradation. Quantum teleportation could play a crucial role in the establishment of interplanetary communication networks by enabling instantaneous and secure transmission of quantum states across vast distances. Quantum teleportation will transform the capabilities and security of satellite communication networks on a global, and ultimately, an interplanetary scale, supporting missions to the Moon, Mars, and beyond.

References

- Abbasi, Q. H., Weides, M., Li, C., & Imran, M. A. (2024). Dive into the quantum realm: Promise of quantum communication and what's next! *IEEE Communications Society Technology News*. <https://www.comsoc.org/publications/ctn/dive-quantum-realm-promise-quantum-communication-and-whats-next>
- Abolade, O., Okandeji, A., Oke, A., Osifeko, M., & Oyediji, A. (2021). Overhead effects of data encryption on TCP throughput across IPSEC secured network. *Scientific African*, 13, Article e00855. <https://doi.org/10.1016/j.sciaf.2021.e00855>
- Ain, N. U., Waqar, M., Bilal, A., Kim, A., Ali, H., Tariq, U. U., & Nadeem, M. S. (2025). A novel approach based on quantum key distribution using BB84 and E91 protocol for resilient encryption and eavesdropper detection. *IEEE Access*, 13, 32819–32833. <https://doi.org/10.1109/ACCESS.2025.3539178>
- Aygun, M., Kandeepan, S., Giorgetti, A., Al-Hourani, A., Arbon, E., & Bowyer, M. (2025). Narrowband interference mitigation techniques: A survey. *IEEE Communications Surveys & Tutorials*, 27(6), 3455–3482. <https://doi.org/10.1109/COMST.2025.3531428>
- Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. *Computers & Security*, 142, Article 103883. <https://doi.org/10.1016/j.cose.2024.103883>
- Berera, A., & Calderón-Figueroa, J. (2022). Viability of quantum communication across interstellar distances. *Physical Review D*, 105(12), Article 123033. <https://doi.org/10.1103/PhysRevD.105.123033>
- Boeing. (2025). Q4S. <https://www.boeing.com/space/quantum#introduction>
- Chai, N., Pao, C., & Chai, S. (2024). Quantum teleportation via optical communication channels. *Journal of Tecnologia Quantica*, 1(3), 146–158. <https://doi.org/10.70177/quantica.v1i3.1678>
- Chen, J., Li, D., Liu, M., & Yang, Y. (2020). Bidirectional quantum teleportation by using a four-qubit GHZ state and two Bell states. *IEEE Access*, 8, 20925–28933. <https://doi.org/10.1109/ACCESS.2020.2971973>
- de Forges de Parney, L., Alibart, O., Debaud, J., Gressani, S., Lagarrigue, A., Martin, A., Metrat, A., Schiavon, M., Troisi, T., Diamanti, E., Gélard, P., Kerstel, E., Tanzilli, S., & Van Den Bossche, M. (2023). Satellite-based quantum information net-

works: use cases, architecture, and roadmap. *Communications Physics*, 6, Article 12. <https://doi.org/10.1038/s42005-022-01123-7>

Dubey, U., Bhole, P., Dutta, A., Behera, D. P., Losu, V., Pandeeti, G. S. D., Metkar, A. R., Banerjee, A., & Pathak, A. (2024). A review on practical challenges of aerial quantum communication. *Physics Open*, 19, Article 100210. <https://doi.org/10.1016/j.physo.2024.100210>

Ghalaii, M., Bahrani, S., Liorni, C., Grasselli, F., Kampermann, H., Woollorton, L., Kumar, R., Pirandola, S., Spiller, T. P., Ling, A., Huttner, B., & Razavi, M. (2023). Satellite-based quantum key distribution in the presence of bypass channels. *PRX Quantum*, 4(4), Article 040320. <https://doi.org/10.1103/PRXQuantum.4.040320>

Gonzalez-Raya, T., Pirandola, S., & Sanz, M. (2024). Satellite-based entanglement distribution and quantum teleportation with continuous variables. *Communications Physics*, 7, Article 126. <https://doi.org/10.1038/s42005-024-01612-x>

Hippke, M. (2021). Searching for interstellar quantum communications. *The Astronomical Journal*, 162(1). <https://doi.org/10.3847/1538-3881/abf7b7>

Hossain, K. A. (2023). The potential and challenges of quantum technology in modern era. *Scientific Research Journal*, XI(VII), 41–49. <https://www.scirj.org/papers-0723/scirj-P0723953.pdf>

Hu, X., Guo, Y., Liu, B., Li, C., & Guo, G. (2023). Progress in quantum teleportation. *Nature Reviews Physics*, 5, 339–353. <https://doi.org/10.1038/s42254-023-00588-x>

Johansson, N., & Larsson, J. Å. (2019). Quantum simulation logic, oracles, and the quantum advantage. *Entropy (Basel, Switzerland)*, 21(8), Article 800. <https://doi.org/10.3390/e21080800>

Joint Functional Component Command for Integrated Missile Defense. (2024, February). *MD220: Joint Integrated Air and Missile Defense Course* [Military Course]. Joint Ballistic Missile Defense Training and Education Center, Fort Sill, OK, United States.

Joshi, S. K., Aktas, D., Wengerowsky, S., Lončarić, M., Neumann, S. P., Liu, B., Scheidl, T., Lorenzo, G. C., Samec, Ž., Kling, L., Qiu, A., Razavi, M., Stipčević, M., Rarity, J. G., & Ursin, R. (2020). A trusted node-free eight-user metropolitan quantum communication network. *Science Advances*, 6(36), Article eaba0959. <https://doi.org/10.1126/sciadv.aba0959>

Kang, M., Park, S., & Lee, Y. (2024). A survey on satellite communication system

security. *Sensors (Basel)*, 24(9), Article 2897. <https://doi.org/10.3390/s24092897>

Khan, M. A., Ghafoor, S., Zaidi, S. M. H., Khan, H., & Ahmad, A. (2024). From quantum communication fundamentals to decoherence mitigation strategies: Addressing global quantum network challenges and projected applications. *Heliyon*, 10(14), Article e34331. <https://doi.org/10.1016/j.heliyon.2024.e34331>

Khanal, A., & Kaur, N. (2025). *The role of quantum computing in enhancing encryption security: A review*. Punjabi University. <https://eprint.iacr.org/2025/706.pdf>

Levin, J. (Host). (2024, March 14). What is Quantum Teleportation? [Audio podcast episode]. In *The Joy of Why*. Quanta Magazine. <https://www.quantamagazine.org/what-is-quantum-teleportation-20240314/>

Lu, C., Cao, Y., Peng, C., & Pan, J. (2022). Micius quantum experiments in space. *Reviews of Modern Physics*, 94(3), Article 035001. <https://doi.org/10.1103/RevModPhys.94.035001>

Lueschow, H., & Pelaez, R. (2020). Satellite communication for security and defense. In K. U. Schrogl (Ed.), *Handbook of Space Security* (pp. 779–796). Springer, Cham. https://doi.org/10.1007/978-3-030-23210-8_107

Maasarani, Z. (2024). *Boeing pioneering quantum communications technology with in-space test satellite*. Boeing. <https://investors.boeing.com/investors/news/press-release-details/2024/Boeing-Pioneering-Quantum-Communications-Technology-with-In-Space-Test-Satellite/default.aspx>

Mafu, M. (2024). Advances in artificial intelligence and machine learning for quantum communication applications. *IET Quantum Communication*, 5(3), 202–231. <https://doi.org/10.1049/qtc2.12094>

Maurin, A. (2023). Russia's offensive Cosmostrategy. *Æther: A Journal of Strategic Airpower & Spacepower*, 2(1), 96–110. <https://www.jstor.org/stable/48714690>

McDowell, J. (2023). *Space Activities in 2022*. Johnathan's Space Report. <https://planet4589.org/space/papers/space22.pdf>

Nande, S. S., Tommaso Rossi, T., Habibie, M. I., Barhoumi, M., Palaparthi, K., Mansouri, W., Raju, A., Bassoli, R., Cianca, E., Fitzek, F. H. P., & De Sanctis, M. (2024). Satellite-based positioning enhanced by quantum synchronization. *Computer Networks*, 254, Article 110734. <https://doi.org/10.1016/j.comnet.2024.110734>

Pfaff, W., Taminiau, T. H., Robledo, L., Bernien, H., Markham, M., Twitchen, D.

J., & Hanson, R. (2013). Demonstration of entanglement-by-measurement of solid-state qubits. *Nature Physics*, 9, 29–33. <https://doi.org/10.1038/nphys2444>

Pirandola, S. (2021). Satellite quantum communications: Fundamental bounds and practical security. *Physical Review Research*, 3(2), Article 023130. <https://doi.org/10.1103/PhysRevResearch.3.023130>

Polychronakos, A. P. (2024). Quantum mechanical rules for observed observers and the consistency of quantum theory. *Nature Communications*, 15(1), Article 3023. <https://doi.org/10.1038/s41467-024-47170-2>

Rausser, G., Choi, E., & Bayen, A. (2023). Public-private partnerships in fostering outer space innovations. *Proceedings of the National Academy of Sciences of the United States of America*, 120(43), Article e2222013120. <https://doi.org/10.1073/pnas.2222013120>

Ren, J., Xu, P., Yong, H., Zhang, L., Liao, S., Yin, J., Liu, W., Cai, W., Yang, M., Li, L., Yang, K., Han, X., Yao, Y., Li, J., Wu, H., Wan, S., Liu, L., Liu, D., Kuang, Y., ... Pan, J. (2017). Ground-to-satellite quantum teleportation. *Nature*, 549, 70–73. <https://doi.org/10.1038/nature23675>

Schodorf, J. B. (2000). EHF satellite communications on the move: Baseband considerations. *Massachusetts Institute of Technology Lincoln Laboratory*, 1–54. <https://apps.dtic.mil/sti/pdfs/ADA373681.pdf>

Secara, I., & Hordiiuk, D. (2023). The importance of high-bandwidth low-latency network systems in the modern age. *Transactions on Engineering and Computing Sciences*, 11(1), 37–44. <https://doi.org/10.14738/tecs.111.13967>

Sidhu, J. S., Joshi, S. K., Gündoğan, M., Brougham, T., Lowndes, D., Mazzarella, L., Krutzik, M., Mohapatra, S., Dequal, D., Vallone, G., Villoresi, P., Ling, A., Jennewein, T., Mohageg, M., Rarity, J. G., Fuentes, I., Pirandola, S., & Oi, D. K. L. (2021). Advances in space quantum communications. *IET Quantum Communication*, 2(4), 182–217. <https://doi.org/10.1049/qtc2.12015>

Tedeschi, P., Sciancalepore, S., & Pietro, R. D. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. *Computer Networks*, 216, Article 109246. <https://doi.org/10.1016/j.comnet.2022.109246>

Wan, Y., Kienzler, D., Erickson, S. D., Mayer, K. H., Tan, T. R., Wu, J. J., Vasconcelos, H. M., Glancy, S., Knill, E., Wineland, D. J., Wilson, A. C., & Leibfried, D. (2019). Quantum gate teleportation between separated qubits in a trapped-ion processor. *Science*, 364(6443), 875–878. <https://doi.org/10.1126/science.aaw9415>