IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 December 2023, accepted 15 December 2023, date of publication 18 December 2023,
date of current version 28 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3344321

TOPICAL REVIEW

Integrating Quantum and Satellites: A New Era of Connectivity

SHABNAM SODAGARI, (Senior Member, IEEE)
Department of Computer Engineering and Computer Science, California State University at Long Beach, Long Beach, CA 90840, USA
e-mail: shabnam@csulb.edu

ABSTRACT Quantum satellite networking is central to enabling quantum key distribution (QKD) and quantum-state transfer. Delving into the synergistic relations of quantum technology and satellite communications, we elucidate on continuous variable and discrete variable QKD schemes, and the strategic selection of satellite orbits for optimal QKD. The prospects and possibilities of the integration of software-defined networking into this paradigm showcases a fusion of traditional and quantum communication methods. In the context of continuous variable quantum systems, a comparative discussion on Gaussian and non-Gaussian paradigms is presented, emphasizing their distinct characteristics crucial for satellite-assisted quantum networks. Moreover, we underscore the role of quantum computing in bolstering the security of satellite information networks, emphasizing the importance of delay reduction for the connection of Internet of Things (IoT) devices to satellite networks. Lastly, we propose potential domains ripe for future exploration in this burgeoning field.

INDEX TERMS Quantum satellite networking, quantum key distribution (QKD), quantum-state transfer, continuous variable, discrete variable, satellite communication, satellite information networks, Gaussian, quantum computing, Internet of Things (IoT), quantum internet, quantum repeaters, entanglement swapping, quantum teleportation.

I. INTRODUCTION

Quantum satellite networking has the potential to revolutionize various industries, including autonomous vehicles, aircrafts, unmanned aerial vehicles (UAVs), secure communications, remote sensing, surveillance, and navigation. Satellites have a vital role in the realization of quantum Internet, since they can be used as quantum repeaters (e.g., to connect two terrestrial quantum computers) and for quantum key distribution (QKD), i.e., establishment of secure keys between two parties by leveraging the laws of quantum mechanics. Quantum satellite repeaters offer more coverage range and less attenuation compared to optical fibers and remove the need for terrestrial optical fiber repeaters. Quantum satellite relays leverage entanglement swapping to distribute entanglement from source to destination by transmission of photons entangled with the memories on neighboring nodes [1], [2]. This operation needs to be completed before quantum decoherence causes the quantum state of information to collapse to classical states. Additionally, quantum teleportation allows the transfer of quantum states between two remote locations using entangled particles.

The connection between satellite communications and quantum technology capitalizes on the inherent advantages of both fields. While satellites offer a reliable platform for QKD and secure key distribution, quantum cryptography reinforces the security and confidentiality of satellite communications. This symbiotic relationship creates a robust framework for future-proof, secure, and efficient global communication across diverse sectors, as shown in Fig. 1.

Since the nexus of satellite communications and quantum technology is essential for the realization of future global quantum internet, this paper investigates opportunities and challenges of this continuum.

The organization of this article, as depicted in Fig. 2, is thus as follows: Section II discusses the use of satellites as quantum relays, including continuous variable Gaussian and

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

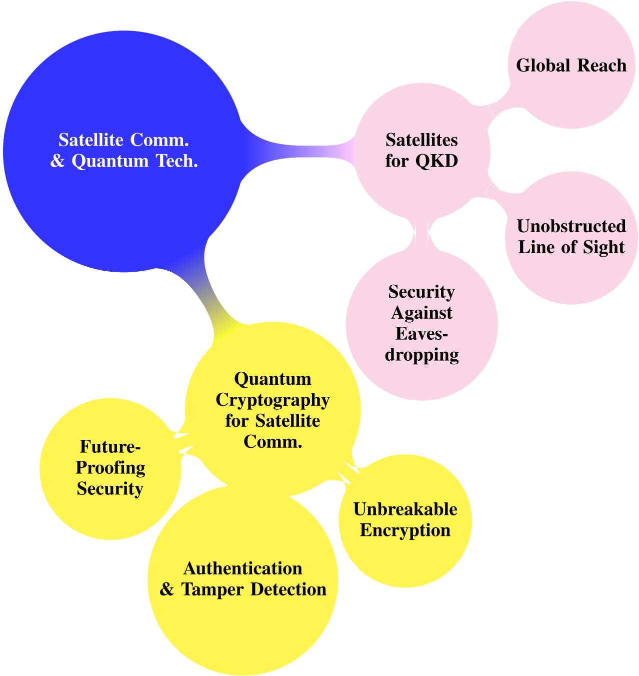
Satellite Comm. & Quantum Tech.
Satellites for QKD
Global Reach
Unobstructed Line of Sight
Security Against Eaves-dropping
Quantum Cryptography for Satellite Comm.
Future-Proofing Security
Unbreakable Encryption
Authentication & Tamper Detection

FIGURE 1. Symbiotic relations between satellite communications and quantum technology.

non-Gaussian quantum paradigms. Section III considers integration of software defined networking (SDN) in quantum satellite networking. Section IV discusses quantum-resistant cryptography for satellite information networks, while Section V contains emerging research directions. Finally, Section VI concludes the paper.

II. RELAY SATELLITES FOR QKD

Two possible umbrellas to categorize quantum communication include 1) prepare-and-measure; and 2) entanglement-based communication.

Prepare-and-measure schemes [3] involve a sender (Alice) preparing a quantum state, sending it through a quantum communication channel, and a receiver (Bob) subsequently measuring the state. In these schemes, single qubits are typically prepared and sent one at a time. These qubits could be in the form of polarized photons or other manageable quantum systems. Alice needs to prepare qubits in specific states, and Bob needs to perform measurements. There is no need for complex entanglement generation or distribution processes. These schemes can be quite robust to noise and losses, particularly if they use decoy-state protocols or other techniques to detect eavesdropping and enhance security.

Entanglement-based schemes [4], on the other hand, rely on the generation, distribution, and measurement of entangled quantum states. The generation of entangled states can be resource-intensive and challenging, requiring precise control and stabilization of quantum systems.

Once entangled states are generated, they need to be distributed to the parties involved, which can be lossy and inefficient, particularly over long distances. Entanglement distribution may require quantum satellite repeaters. Table 1 provides a comparison between prepare-and-measure vs. entanglement-based communication schemes.

Depending on the type of quantum states that are used to encode information, two schemes can be envisioned when using satellites for QKD: 1) Discrete variable QKD in which the encoder uses discrete variables of a quantum state and the decoder uses single photon detector; and 2) Continuous variable QKD [5] in which the encoder uses quadrature component of the light field and the decoder uses balanced homodyne (or heterodyne) detector.

Table 2 presents a comparison between continuous variable (CV) and discrete variable (DV) QKD schemes.

A. DISCRETE VARIABLE QUANTUM SYSTEMS

Discrete variable quantum schemes are a class of quantum communication protocols that utilize the properties of individual discrete quantum states, such as single photons, to establish secure cryptographic keys between two parties. These schemes primarily involve the transmission and measurement of qubits, which are the fundamental units of quantum information. The most common encoding bases for qubits in discrete variable QKD are typically the polarization and phase of single photons.

In a discrete variable QKD scheme, the sender (Alice) prepares qubits in different states, such as horizontal or vertical polarization, and sends them through a quantum channel to the receiver (Bob). Bob then measures these qubits using one of the predefined bases and records the measurement outcomes. The security of the key distribution is ensured by the principles of quantum mechanics, which dictate that any eavesdropping attempt on the quantum channel would disturb the states and be detectable by Alice and Bob.

The Micius satellite project leverages DV quantum concepts [6] for entangled photon pair distribution and teleportation for downlink and uplink transmissions. This technology uses single-photon detector. It facilitates satellite-based entanglement distribution to two ground stations almost 1200 kilometers apart [6].

Discrete variable QKD schemes pose challenges in terms of hardware complexity and practical implementation. Generating and manipulating single-photon states required for discrete variable QKD can be technically demanding and expensive. Achieving single-photon sources with high efficiency and low noise is a significant challenge, especially over long distances and in real-world conditions.

Due to the capabilities offered by CV quantum systems in information communication and the commercial deployment of CV quantum satellite networking being an open research area, next we discuss the CV quantum paradigm.

B. CONTINUOUS VARIABLE QUANTUM SYSTEMS

Continuous variable quantum schemes involve continuous properties of quantum states (quadrature amplitudes) and

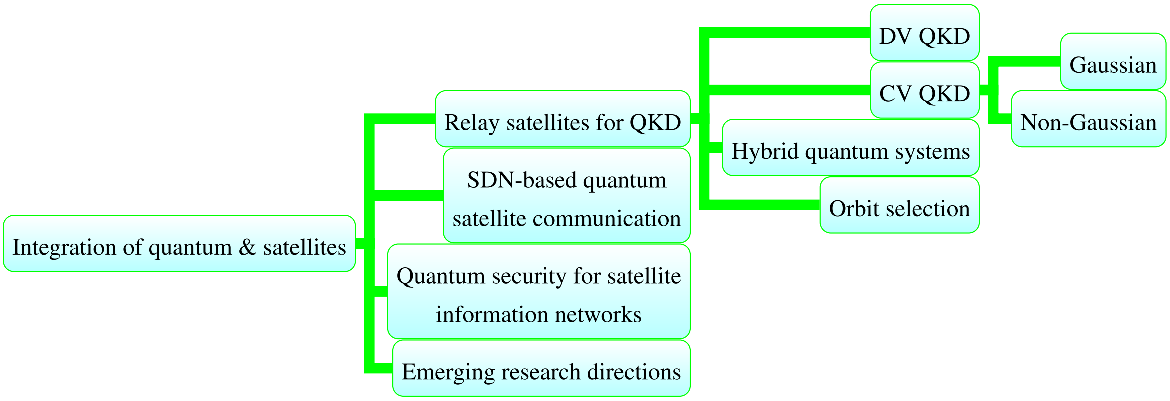
Integration of quantum & satellites
Relay satellites for QKD
SDN-based quantum satellite communication
Quantum security for satellite information networks
Emerging research directions
DV QKD
CV QKD
Hybrid quantum systems
Orbit selection
Gaussian
Non-Gaussian

FIGURE 2. Hierarchy of topics at the nexus of quantum and satellite technologies discussed in Sections II to V.

TABLE 1. Comparison of prepare-and-measure schemes and entanglement-based schemes.

Feature	Prepare-and-Measure Schemes	Entanglement-Based Schemes
Quantum States	Single qubits prepared and sent individually.	Generation and distribution of entangled states, which can be resource-intensive.
Operations	Simple preparation and measurement operations.	Requires complex operations for entanglement generation, distribution, and measurement.
Robustness	Robust to noise and losses, especially with decoy-state protocols.	Sensitive to losses; requires high-fidelity operations to maintain entanglement.
Key Rate	Typically achieves higher key rates.	Key rates can be lower due to complexities in entanglement processes.
Scalability	Easily scalable with less complex infrastructure.	Scaling up is challenging due to the need for high-fidelity entanglement and specialized equipment.
Flexibility	More flexible and easier to integrate with existing infrastructure.	Less flexible, requiring specialized conditions and equipment.

TABLE 2. Comparison of discrete variable and continuous variable QKD.

Feature	Discrete Variable QKD	Continuous Variable QKD
Encoding scheme	Polarization or phase of individual photons	Quadrature amplitudes of coherent states
Type of states used	Single-photon states	Multimode coherent states
Alphabet used	Binary (0 and 1)	Gaussian, non-Gaussian
Security against	Certain types of attacks, such as intercept-resend and side-channel attacks	Photon number splitting attacks
Hardware complexity	More complex and expensive to generate and manipulate single-photon states	Simpler and more efficient to generate coherent states
Source Requirements	Requires single-photon sources or weak coherent pulses with decoy states	Can use coherent light sources, which are readily available and less expensive
Error Correction	Uses discrete error correction codes, which are well-established	Requires continuous-variable error correction codes, which can be more complex
Performance	Slower data rate due to the use of single photon	Higher data rate
Quantum channel	Susceptible to channel loss, noise, and decoherence	More robust against channel loss and noise
Real-world implementations	Deployed in commercial systems (e.g., Micius)	Fewer commercial implementations

benefit from a higher dimensional Hilbert encoding space that can increase their robustness against noise. The quadrature amplitude refers to a property of the light field used for encoding information. In quantum optics, the light field is described in terms of its phase and amplitude. Continuous variable QKD leverages these properties to encode information. The quadrature amplitude refers to the amplitude of a particular component of the light field's phase space representation to provide a measure of how much the field's amplitude varies in a specific direction within a two-dimensional phase space. This variation in amplitude is used to encode information in continuous variable QKD systems. Furthermore, the quadrature components may be associated to the position and momentum of a harmonic oscillator [7]. Additionally, a Hilbert encoding space is a high-dimensional mathematical space where the continuous properties of quantum states, e.g., quadrature amplitudes are used to encode, transmit, and process information in a secure manner.

Due to atmospheric turbulence and beam wandering, quantum teleportation over ground to satellite channel (uplink) is more susceptible to noise compared with the satellite to ground channel (downlink) [6]. Nevertheless, continuous variable QKD may need the transmission of coherent states of different amplitudes. Coherent states are quantum states ideally emitted by a laser. These states serve as a basis for describing fields of all types. Coherent states are used to analyze photon statistics of arbitrary radiation fields in quantum mechanics [8]. To teleport a coherent state in the uplink channel, CV entanglement in the form of two-mode-squeezed vacuum state (modelled after the CV downlink channel) can be used as resource to enhance uplink teleportation [9].

Continuous variable QKD schemes are more robust against channel loss and noise because they rely on the statistics of continuous variables that can be measured with high efficiency. The use of coherent states in continuous variable QKD allows for the transmission of classical-like signals, and the Gaussian nature of these states enables error correction to be applied more effectively. This makes continuous variable QKD more suitable for practical implementations over longer distances and in the presence of certain types of noise and imperfections in the quantum channel.

The alphabet used for CV quantum information is either Gaussian or non-Gaussian, resulting in different features that are discussed below.

1) GAUSSIAN VS. NON-GAUSSIAN CV QUANTUM PARADIGMS

In the Gaussian CV quantum regime, quantum states are described by Gaussian distributions in phase space. These states are fully characterized by their first and second moments, such as mean values and covariance matrices. Gaussian operations are unitary transformations and linear-optical operations that preserve the Gaussian nature of quantum states. Examples include beam splitters, phase shifters, and squeezing operations. Measurements performed in the Gaussian CV quantum regime are described by Gaussian measurement operators. These measurements are generally homodyne detections, where the measurement outcomes are continuous variables. However, in the non-Gaussian CV quantum regime, quantum states are described by non-Gaussian distributions in phase space. These states require higher-order moments for their full characterization. Additionally, non-Gaussian operations are nonlinear operations that change the Gaussian nature of quantum states. Examples include photon subtraction, addition, and replacement operations [10]. Measurements performed in the non-Gaussian CV quantum regime are described by non-Gaussian measurement operators. These measurements involve higher-order correlations and can include photon counting or other non-Gaussian detection techniques. Table 3 presents a comparison of Gaussian and Non-Gaussian CV quantum CV systems. In CV quantum systems the distillation of Gaussian entanglement is impossible using only Gaussian operations, whereas the entanglement distillation of mixed non-Gaussian states does not need additional requirements. This feature and the robustness of non-Gaussian entanglement against decoherence make it a valuable choice for satellite-assisted quantum Internet [7].

Studies have examined CV-QKD protocols using Gaussian resources over atmospheric channels to understand how Gaussian quantum states behave when transmitted through high-loss atmospheric channels, which are vital for satellite-based communications. Non-Gaussian operations like photon subtraction or addition can lead to higher levels of entanglement, which is advantageous for QKD application of satellites. The conditions are different under atmospheric fading and fixed-attenuation channels between the satellite and ground stations, particularly in terms of quantum key generation rates. Non-Gaussian states could potentially enhance quantum key rates over fixed-attenuation channels compared to Gaussian states. However, this is not consistently the case in atmospheric fading channels. The true key rate provided for non-Gaussian states is still an area of investigation [11]. In terms of key generation rates, the Gaussian CV quantum scheme establishes rates over atmospheric channels in satellite networks, whereas the non-Gaussian scheme has potential for enhanced quantum key rates over fixed-attenuation channels compared to Gaussian states, but this is not consistently observed in atmospheric fading channels. The Gaussian scheme has proven applicability in satellite-based quantum networks for QKD between ground stations and LEO (low earth orbit) satellites. Nevertheless, research is still needed to fully characterize the use of non-Gaussian CV paradigm in satellite-based quantum networks. More specifically, the non-Gaussian paradigm is an emerging field of study, which requires understanding of its potential and limitations in practical applications, particularly in satellite-based quantum networks.

C. HYBRID DV AND CV QUANTUM TELEPORTATION

To advance quantum satellite communication hybrid teleportation protocols integrate DV and CV in quantum information [12], [13]. In satellite communication, this hybrid approach can interconnect terrestrial devices running on mixed technologies. Using a CV entangled state as the teleportation channel, this approach contrasts with directly distributing quantum entanglement from a satellite, where transmission loss directly affects the DV modes. By pre-distributing the CV channel from the satellite, different quantum states can be teleported, allowing the satellite loss to enter indirectly through the teleportation channel. Using

TABLE 3. Comparison of gaussian and non-gaussian cv quantum paradigms for satellite-assisted quantum internet.

Feature	Gaussian CV Quantum Paradigm	Non-Gaussian CV Quantum Paradigm
Quantum States	Described by Gaussian distributions in phase space	Described by non-Gaussian distributions in phase space, requiring higher-order moments for characterization
Operations	Gaussian operations preserve the Gaussian nature of states	Non-Gaussian operations are nonlinear and change the Gaussian nature of states
Measurements	Gaussian measurements described by Gaussian measurement operators, often using homodyne detections	Non-Gaussian measurements involve higher-order correlations and non-Gaussian measurement operators, such as photon counting
Entanglement	Gaussian entanglement is well understood, but distillation requires non-Gaussian operations	Non-Gaussian entanglement can be distilled without additional requirements
Robustness	Gaussian entanglement is more susceptible to decoherence	Non-Gaussian entanglement can exhibit increased robustness against decoherence

TABLE 4. Comparison of hybrid and non-hybrid methods in quantum communication.

Feature	Hybrid Method (Teleported DV Entanglement over CV Channel)	Non-Hybrid Method (Directly Distributed DV Entanglement)
Entanglement Quality	Higher quality of entanglement	Lower quality of entanglement compared to the hybrid method under similar conditions
Loss Tolerance	Higher tolerance to photonic loss; maintains higher logarithmic negativity, which indicates better entanglement quality under lossy conditions	Lower tolerance to photonic loss; logarithmic negativity (and thus entanglement quality) is significantly reduced compared to the hybrid method
Key Rates for Device-Independent QKD	No significant advantage over directly-distributed entanglement in terms of key rates	Similar key rate reduction to the hybrid method
Teleportation Channel	Utilizes an attenuated CV entanglement as a teleportation channel, which allows for the teleportation of DV states and offers flexibility in quantum information processing	Direct distribution without the intermediate step of teleportation, potentially less flexible in adapting to different quantum communication scenarios
Optimization	Involves a mathematical model considering transmission losses and a strategy for gain-tuning to optimize teleportation outcomes	Direct distribution might not have the same level of optimization flexibility in terms of adjusting to different loss scenarios

a CV channel to transfer one mode of a DV entangled state results in higher entanglement quality than directly distributing DV entanglement from the satellite. In the context of the teleportation of a hybrid entangled state over the CV channel results indicate that for the typical loss conditions of the Satellite-Earth channel, teleportation is more effective than direct distribution [12]. Table 4 presents a comparison between hybrid and non-hybrid solutions.

Another decisive factor for the realization of quantum Internet via satellites is the choice of orbits for the constellation.

D. ORBIT SELECTION FOR SATELLITE-ASSISTED QUANTUM RELAYS

Major design parameters for orbit selection to enable quantum satellite Internet are outlined in Fig. 3. For example, embodiments of this technology include leveraging satellites for QKD or for interconnecting a network of quantum computers. Here, the satellite helps expand the communication range compared with terrestrial fiber optics. Other example applications include ground to satellite quantum teleportation [14]. To minimize the attenuation with distance in satellite-assisted quantum networking, the orbits with closer distances to earth are reasonable. To this end, LEO satellites are a suitable choice [1]. Due to the mobility of LEO satellites in their orbit with respect to earth, ground stations can only access LEO satellites for a short period each day. This short time of coverage degrades QKD rates. In contrast, GEO (geosynchronous orbit) satellites have longer time and area of coverage. Nonetheless, the distance attenuation associated with GEO to ground stations is larger compared to that of LEO satellites.

As such, a hybrid of these two orbits can efficiently deliver quantum services to the ground [15]. More specifically, GEO satellites with direct links to both LEO satellites and ground stations can be used as a backup to boost quantum state transfer. However, GEO satellites have a higher probability of exposure to scattered sunlight noise than LEO constellations [6]. The scattered sunlight noise is a barrier against QKD and necessitates further investigation.

Optimal routing with the objective of minimizing the total flow on the hybrid GEO-LEO QKD network (or consuming the least secret keys) leans itself to a graph optimization problem. Key generation rates comprise the edge values of

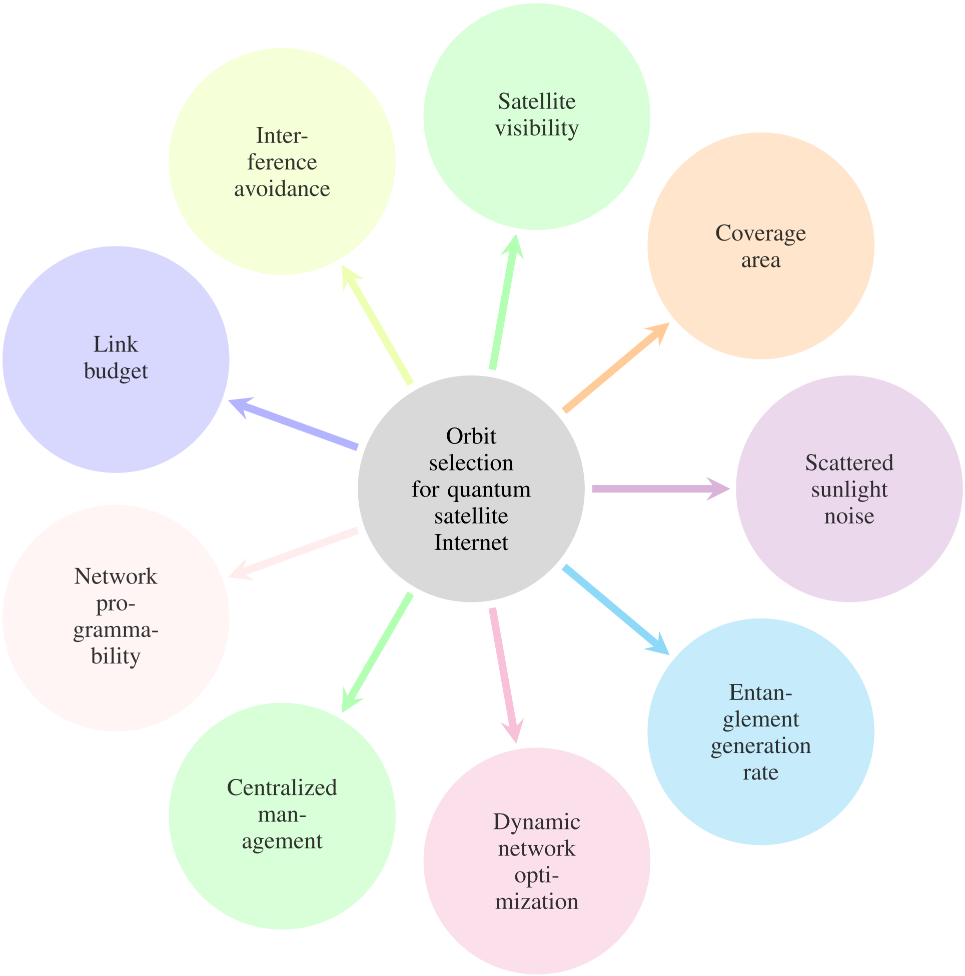
Orbit selection for quantum satellite Internet
Satellite visibility
Coverage area
Scattered sunlight noise
Entan-glement generation rate
Dynamic network opti-mization
Centralized man-agement
Network pro-gramma-bility
Link budget
Inter-ference avoidance

FIGURE 3. Design parameters for orbit selection in quantum satellite networking.

this weighted temporal graph, while its vertices are GEO and LEO satellite nodes (trusted-relays) as well as ground stations [16]. The temporal nature of the graph is due to the movement of LEO satellites and varying atmospheric conditions affecting secret key generation rates. To optimize routing and secret key flows in a centralized manner, for a pair of stations, the optimization problem can be formulated as a max-flow problem, solved using path-finding techniques. When multiple ground stations exchange keys with multiple others, the problem is modeled as a multi-commodity flow problem. Each edge in the graph has a maximum capacity, representing the amount of secret keys in the key pool associated with that link.

The flow of keys (for each commodity) is subject to constraints like link capacity, positive flow, and flow conservation. Flow conservation implies that for all nodes in the network (except the source and sink), the total incoming flow of key rate must equal the total outgoing flow.

The importance of routing and resource allocation leads us to the semi-centralized paradigm for managing quantum satellite information networks, which is the topic of the next section.

III. INTEGRATION OF SOFTWARE-DEFINED NETWORKING WITH QUANTUM SATELLITE COMMUNICATION

SDN provides a flexible and programmable way to manage and orchestrate the deployment of quantum satellite information networks [1], [17], [18], particularly for:

1) Controlling the generation of swapping operations to originate entanglement;
2) Dynamic routing optimization to increase entanglement generation rate and minimize swapping overhead by proper selection of quantum repeaters in the path; and
3) Adapting to satellite mobility and reliable handover.

Compared to pure distributed management, centralized strategy is shown to result in higher entanglement rates [18].

The routing decision is made based on network performance metrics such as overhead required to complete the entanglement generation, bandwidth utilization, latency, etc. [17]. The data plane of SDN-based quantum satellite architecture is composed of quantum satellite repeaters and ground stations, whereas the control plane may be directly integrated into the constellation, in addition to the terrestrial controller [1]. The terrestrial controller communicates with the satellites through the southbound APIs (application programming interfaces) to manage the best path [19]. The quantum repeaters on satellites are interconnected to each other through west and eastbound APIs. Enhancing the standard functionalities of a SDN controller, the ground station controller for quantum satellite communication uniquely integrates an entanglement management unit. This feature sets it apart from traditional classical SDN controllers. In other words, the controller builds a network state by querying databases containing adjacency matrices of the constellation. For linking two ground stations, the controller utilizes the northbound API to access a path evaluation module [19], then applies a path selection algorithm. The quantum repeaters on the satellites create and exchange entangled particles based on instructions from the controller through the southbound API. More specifically, delegating the role of a network control plane to a subset of satellites in the constellation (in addition to the ground controller) relieves the traffic burden on a single SDN controller and decreases delays and overhead for entanglement establishment [1]. Among the functionalities of the SDN control plane are time synchronization, calibration, management of Bell state measurements, network topology database, etc. [20].

Nevertheless, designing and deploying a SDN-based quantum satellite architecture is a complex endeavor that necessitates a meticulous consideration of the unique challenges posed by quantum communication and satellite networks. Quantum networks rely on the preservation of delicate quantum states, making low-latency communication imperative. The challenge lies in harmonizing the flexibility and resource efficiency offered by SDN with the real-time demands of quantum communication. Some examples include:

- Resource allocation and network efficiency: While SDN offers dynamic resource allocation, which can be advantageous for efficient utilization of available quantum channels, it must be optimized to cater to the specific requirements of quantum communication. Ensuring that the quantum channels receive the necessary resources while avoiding resource contention, especially during high-demand scenarios, poses a significant challenge, due to inherent complexities of satellite networks stemming from signal attenuation, varying distances, and dynamic connectivity.
- Security and vulnerabilities: SDN-based control planes are vulnerable to single point of failure attacks. To mitigate this vulnerability, strategies could involve designing a system capable of dynamic self-reconfiguration to sustain operations during adverse conditions, or decentralizing the control plane's functions across distributed nodes.
- Interoperability and standards: Achieving interoperability between quantum and classical components, developing consistent control protocols, and ensuring compatibility across different satellite systems demand a collaborative standardization effort among various stakeholders.

  The ETSI (European Telecommunications Standards Institute) QKD control interface for SDNs [21] defines management interfaces for integrating QKD into dis-aggregated network control plane architectures. It outlines workflows between an SDN-enabled QKD node and the SDN controller, focusing on resource discovery and system configurations. An SD-QKD node is an aggregation of one or more QKD modules that interface with an SDN controller. The connection allows for the dynamic and remote configuration of QKD systems to manage key associations between remote secure locations, either through a direct quantum channel or multi-hop repeaters (e.g., satellites). The modelling provides an abstracted view of the QKD domain, treating QKD systems within a secure location as interfaces of a network element - the SD-QKD node. This node can communicate with neighboring nodes and the central controller to create end-to-end services or key associations, either over a direct quantum channel or via a multi-hop link for a fully connected QKD network. Moreover, QKD key Association links are logical key associations between two remote SD-QKD nodes. There are two types: direct (physical) links, where a direct quantum channel generates keys, and virtual links, where keys are relayed through several SD-QKD nodes in a multi-hop manner. The standard specifies a set of base notifications for application interface and link management, along with a generic structure for integrating new events. This structure covers applications, links, and interfaces. Nevertheless, the standard does not directly involve satellite repeaters, necessitating new standardization efforts.

In the following section, we delve into the realm of quantum security for satellite networks. While quantum satellites address the long distance QKD aspect of securing data communication, the next section will explore how quantum computing can enhance security in satellite data transfer.

IV. QUANTUM SECURITY FOR SATELLITE NETWORKS

The channel between the ground station and the satellite is prone to eavesdropping and other attack types, e.g., man-in-the-middle, impersonation, and replay attacks. When several Internet of Things (IoT) devices try to connect to the satellite, access authentication imposes a large signaling overhead [22]. Accordingly, access authentication mechanisms with low latency are essential.

To this end, quantum-proof authentication schemes, such as lattice-based access authentication and ring learning with errors (RLWE) are alternatives to classical cryptography when user equipments seek direct connection to the satellite information network (SIN) [23]. Since the distances among satellite to ground network nodes already cause propagation delays, the authentication scheme must be designed with delay minimization in mind. To this end, strategies, such as pre-negotiation of the session key and lattice-based cryptography are suitable for resource-constrained IoT devices with limited power and processing capacity.

Lattice-based cryptography is based on the hardness of certain mathematical problems related to lattices. One example of such a problem is the Shortest Vector Problem (SVP), which asks to find the shortest non-zero vector in a given lattice. This quantum-proof lattice-based cryptography can be used for key exchange, digital signatures, and encryption.

RLWE, as a foundation for key exchange and encryption, is based on the hardness of finding the secret key from a set of noisy equations involving polynomials over a finite field or a polynomial ring. In this method Alice and Bob exchange a shared secret key by encoding it as a random polynomial with small coefficients over a finite field or a polynomial ring. The random polynomial is then multiplied by a public polynomial, which adds noise to the encoding. Alice and Bob exchange the noisy polynomials and use them to compute a shared secret key.

To detect various security vulnerabilities and flaws in either lattice-based or RLWE schemes, the Scyther verification tool and the Burrows-Abadi-Needham (BAN) logic are useful. BAN logic provides a formal framework to verify properties like authentication, confidentiality, and freshness. Moreover, Scyther is an automated tool that considers an adversary with unlimited computational power and the ability to intercept, modify, and replay messages by exhaustively exploring the state space of the scheme [24].

The main phases of access authentication aiming at delay minimization in quantum-resistant SINs, as in Fig. 4, are:

- Registration: device and satellite establish a shared key.
- Pre-negotiation: device and satellite verify each other's signatures and negotiate a session key.
- Authentication: device proves its identity to the satellite by solving a lattice or RLWE-based equation.
- Session key agreement: device and satellite use the shared key established during registration to derive a session key for secure communication.

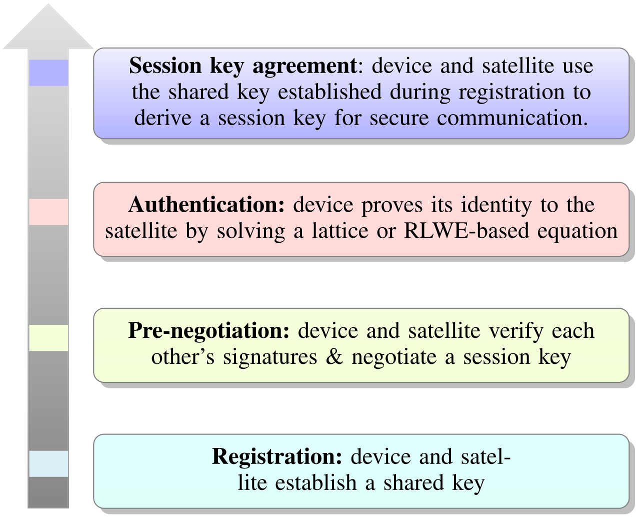
Session key agreement: device and satellite use the shared key established during registration to derive a session key for secure communication.
Authentication: device proves its identity to the satellite by solving a lattice or RLWE-based equation
Pre-negotiation: device and satellite verify each other's signatures & negotiate a session key
Registration: device and satellite establish a shared key

FIGURE 4. Major elements of quantum-proof authentication in SINs.

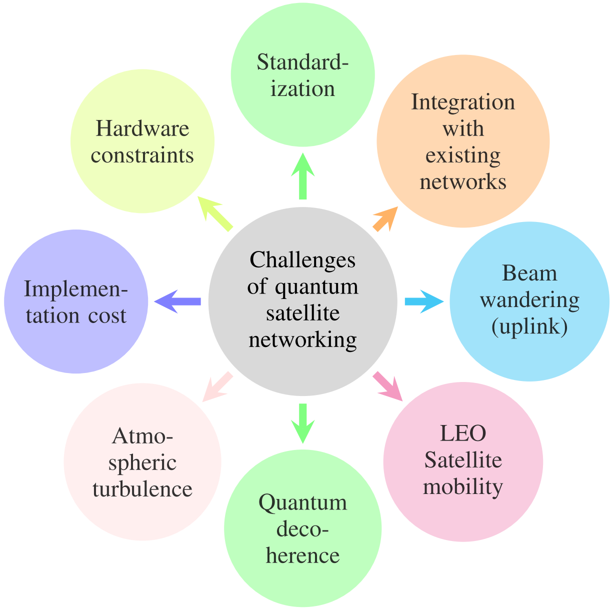

FIGURE 5. Challenges of global quantum satellite networking.

V. EMERGING RESEARCH DIRECTIONS

To achieve global quantum Internet, implementation of quantum satellite communication in real-world scenarios still faces challenges that need to be addressed through further research. This entails navigating a complex landscape of technical challenges, which requires innovative solutions to balance flexibility, latency, coherence preservation, security, and resource optimization. Addressing these challenges is essential to unlock the potential of quantum-assisted satellite communications as well as satellite-assisted quantum key distribution toward secure and efficient communication. As outlined in Fig. 5, some challenges include:

- Interoperability and integration of the quantum satellite network with existing heterogeneous ground networks: Existing ground networks are designed for scalability to handle large volumes of data. However, quantum satellite networks currently have limitations in terms of data rate and distance, making it challenging to scale these networks to meet the demands of existing ground network traffic. Accurate timing and synchronization are crucial for entanglement-based systems. Ensuring this level of precision in synchronization between ground and satellite systems is complex.
- Intelligent path selection and scheduling algorithms: The dynamic nature of satellite orbits results in a constantly changing network topology. This makes the task of path selection and scheduling extremely complex, as the algorithms must continuously adapt to the current configuration of the satellite constellation. Additionally, entangled states, are highly sensitive to environmental factors and can easily lose their quantum properties due to decoherence. Algorithms must account for signal

propagation delays and the relative motion of satellites and Earth. Additionally, satellites operate with limited power resources. Path selection and scheduling algorithms must be energy-efficient, minimizing the power consumption of onboard quantum and classical communication hardware.

- Entanglement swapping overhead reduction: The relative motion between satellites and Earth-based stations adds complexity to timing for successful entanglement swapping in light of cosmic radiation and temperature fluctuations in space. Quantum states, unlike classical signals, cannot be amplified due to no-cloning theorem. Therefore, signal attenuation over long distances, including through the Earth's atmosphere, is a challenge.
- Transfer of a higher alphabet of CV coherent states from the ground station to the satellite: A higher alphabet of CV coherent states implies more complex and high-dimensional quantum states. Managing these states requires more sophisticated control and error correction techniques, which can be challenging to implement in a dynamic network environment like SDN.
- Standardization of quantum internet protocol stack, especially in data link and network layers: Algorithms must consider regulatory constraints, such as spectrum allocation and orbital slots, which can impact path selection and scheduling decisions.
- Scalable and flexible allocation of the control plane role to selected satellites in the constellation: Satellite constellations operate in a highly dynamic environment, wherein satellite orbits, Earth's rotation, and atmospheric conditions constantly change the network topology. This requires the control plane to rapidly adapt to these changes, making scalable and flexible allocation difficult. Moreover, satellites typically have limited computing resources due to weight and power constraints. This limits the control plane functions that can be executed onboard to manage a large dynamic constellation.
- Reliable and close-packed hardware: Quantum communication systems involve complex hardware, including quantum sources, detectors, and processing units. Miniaturizing and integrating these components into a satellite's limited space without compromising their performance is technically challenging. Additionally, satellites operate in extreme temperatures, vacuum, and high levels of radiation. Components like optical systems must be designed to tolerate vibrations and mechanical stresses during the launch of satellites in orbit.

Tackling these challenges requires a multidisciplinary approach, combining quantum physics, satellite communication, computer science, and optimization methods, to develop robust and efficient algorithms for SDN-based quantum satellite communication. There is a need for regulatory and standardization efforts related to spectrum use, orbital slots, and coordination with other satellite operators and terrestrial networks, which the control plane must adhere to while managing the constellation. The benefit of overcoming these challenges includes enhanced overall security.

VI. CONCLUSION

The inherent connection between satellite communications and quantum technology is significant in shaping the future of secure and efficient global communication. This synergy arises from the unique capabilities of satellites to facilitate quantum key distribution and the application of quantum cryptography to enhance the security of satellite communications. The inherent properties of quantum mechanics can address the vulnerabilities in our current communication systems, especially when integrated with satellite infrastructures. The intricate balance between discrete and continuous variable QKD schemes offers varied potential in ensuring optimal secure communication. Furthermore, the choice of satellite orbits, LEO versus GEO, showcases the need for a hybrid approach to best serve quantum communication goals on a global scale. Access authentication, especially as we approach a world dominated by IoT devices, underscores the potential of quantum-cryptography schemes demonstrating the continued evolution in quantum-resistant security solutions. As industries such as autonomous vehicles, UAVs, and remote sensing increasingly rely on robust and secure communications, the symbiotic relationship between satellite communications and quantum technology is poised to play a pivotal role. This paper put forward the challenges and opportunities of discrete variable and continuous variable QKD, specially as relates to entanglement quality, loss tolerance, key rates, etc. Moreover, Gaussian and non-Gaussian quantum paradigms were compared in the context of satellite-assisted quantum Internet. Hybrid methods in which DV entanglement is teleported over CV channel offer higher quality of entanglement and loss tolerance compared to traditional non-hybrid methods that rely solely on directly distributed DV entanglement. Hence, they are a viable solution to the challenge of transmission loss, which is a critical issue in satellite-to-Earth quantum communication to interconnect terrestrial devices.

The challenges facing the implementation of quantum satellite communication, crucial for achieving a global quantum internet, were highlighted. These challenges are multifaceted, encompassing technical, operational, and regulatory aspects. Key issues include the integration of quantum satellite networks with existing terrestrial systems, the dynamic nature of satellite orbits demanding intelligent path selection and scheduling, the complexity of entanglement swapping, and the management of high-dimensional quantum states. Further, the standardization of quantum internet protocols, particularly in data link and network layers, and the scalable and flexible allocation of control plane roles in satellite constellations present additional hurdles. More precisely, existing standards fall short in addressing the unique requirements of satellite QKD networks, underscoring the need for dedicated efforts towards new standardization. Upon launching more satellite constellations with quantum capabilities in the future, the global quantum Internet will be on the horizon.

ACKNOWLEDGMENT

The author would like to thank anonymous reviewers for their help in improving the quality of this manuscript.

REFERENCES

[1] F. Chiti, R. Fantacci, R. Picchi, and L. Pierucci, "Mobile control plane design for quantum satellite backbones," *IEEE Netw.*, vol. 36, no. 1, pp. 91–97, Jan. 2022.

[2] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum internet—Applications, functionalities, enabling technologies, challenges, and research directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2218–2247, 4th Quart., 2021.

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020. [Online]. Available: https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[5] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, "Quantum key distribution using Gaussian modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003.

[6] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, "Micius quantum experiments in space," *Rev. Modern Phys.*, vol. 94, no. 3, Jul. 2022, Art. no. 035001.

[7] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.

[8] R. J. Glauber, "Coherent and incoherent states of the radiation field," *Phys. Rev.*, vol. 131, no. 6, pp. 2766–2788, Sep. 1963, doi: 10.1103/PhysRev.131.2766.

[9] E. Villaseñor, M. He, Z. Wang, R. Malaney, and M. Z. Win, "Enhanced uplink quantum communication with satellites via downlink channels," *IEEE Trans. Quantum Eng.*, vol. 2, pp. 1–18, 2021.

[10] T. J. Bartley and I. A. Walmsley, "Directly comparing entanglement-enhancing non-Gaussian operations," *New J. Phys.*, vol. 17, no. 2, Feb. 2015, Art. no. 023038.

[11] N. Hosseinidehaj and R. Malaney, "CV-QKD with Gaussian and non-Gaussian entangled states over satellite-based channels," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–7.

[12] H. Do, "Satellite-based quantum communications with hybrid protocols," M.S. thesis, School Elect. Eng. Telecommun., UNSW Sydney, Sydney, NSW, Australia, 2022.

[13] I. B. Djordjevic, "Hybrid CV–DV quantum communications and quantum networks," *IEEE Access*, vol. 10, pp. 23284–23292, 2022.

[14] J.-G. Ren, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70–73, Sep. 2017.

[15] D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, "Quantum key distribution over double-layer quantum satellite networks," *IEEE Access*, vol. 8, pp. 16087–16098, 2020.

[16] M. Grillo, A. A. Dowhuszko, M.-A. Khalighi, and J. Hämäläinen, "Resource allocation in a quantum key distribution network with LEO and GEO trusted-repeaters," in *Proc. 17th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Sep. 2021, pp. 1–6.

[17] Y. Wang, Y. Zhao, W. Chen, K. Dong, X. Yu, and J. Zhang, "Routing and key resource allocation in SDN-based quantum satellite networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 2016–2021.

[18] R. Picchi, F. Chiti, R. Fantacci, and L. Pierucci, "Towards quantum satellite internetworking: A software-defined networking perspective," *IEEE Access*, vol. 8, pp. 210370–210381, 2020.

[19] R. Picchi, "Architectures and protocols design for non-terrestrial quantum networks," Ph.D. dissertation, Univ. Florence, Florence, Italy, 2023.

[20] J. Chung, E. M. Eastman, G. S. Kanter, K. Kapoor, N. Lauk, C. H. Pena, R. K. Plunkett, N. Sinclair, J. M. Thomas, R. Valivarthi, S. Xie, R. Kettimuthu, P. Kumar, P. Spentzouris, and M. Spiropulu, "Design and implementation of the Illinois express quantum metropolitan area network," *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–20, 2022.

[21] *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks*, document ETSI GS QKD 015 V1.1.1, 2021.

[22] R. Ma, J. Cao, D. Feng, and H. Li, "LAA: Lattice-based access authentication scheme for IoT in space information networks," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2791–2805, Apr. 2020.

[23] J. Guo, Y. Du, X. Wu, and M. Li, "An anti-quantum authentication protocol for space information networks based on ring learning with errors," *J. Commun. Inf. Netw.*, vol. 6, no. 3, pp. 301–311, Sep. 2021.

[24] (2023). *The Scyther Tool*. [Online]. Available: https://people.cispa.io/cas.cremers/scyther/

SHABNAM SODAGARI (Senior Member, IEEE) received the Ph.D. degree from The Pennsylvania State University. She is currently a Faculty Member of computer engineering and computer science with California State University at Long Beach, Long Beach, CA, USA.