Leveraging SDN Control for Time-Precise Quantum Position Verification

Anonymous Authors

***Abstract*—With ongoing improvements in quantum network hardware, the demand for practical applications continues to rise. Quantum Position Verification (QPV), which leverages geographic location as an authentication token, has been identified as a critical application. However, QPV faces significant challenges due to timing constraints introduced by real-world conditions. In this work, we investigate the c-QPV$^{f}_{\text{BB84}}$ protocol, examining how these timing constraints affect its reliability and security. To address these challenges, we propose precise timing requirements that ensure the successful execution of the protocol. Furthermore, we propose a possible approach to integrate Software-Defined Networking (SDN) control into quantum networks, introducing time calibration and synchronization phases to mitigate timing issues and improve the protocol's robustness under practical conditions. Our findings advance the development of secure and practical QPV protocols while showcasing the potential of programmable quantum control planes for scalable quantum networks.**

***Index Terms*—quantum network, quantum control plane, quantum network protocol**

I. Introduction

In an era of pervasive digital threats and an expanding reliance on secure communication, authentication has emerged as a cornerstone of cybersecurity. The authentication problem, at its core, seeks to verify the identity and integrity of entities within a network, ensuring that sensitive data is exchanged only with trusted parties [1].

One of the approaches to this problem is Position Verification (PV), which leverages a user's geographic location as an identification token. Such authentication is achieved by verifying the prover's ability to respond to time-constrained challenges issued by the verifier, based on the limits of classical signal propagation [2]. A pivotal application of PV is in banking, where it can authenticate a user's physical location during critical transactions, such as fund transfers or accessing vaults, ensuring that only individuals or devices in a specific, verifiable location can complete the operation. However, its reliance on classical information limits its resistance to eavesdropping, making it vulnerable to relay attacks and location spoofing. Such constraints can be addressed by introducing quantum communication, in which quantum information cannot be copied due to the no-cloning theorem [3]. This advancement leads to Quantum Position Verification (QPV) [4], a protocol that has gained recognition as a significant quantum network application and a step forward from quantum key distribution.

However, most discussions around the QPV are confined to perfect experimental setups, which may not apply to real-world scenarios. Successful deployment of the protocol on experimental platforms requires careful consideration of these real-world constraints, which can arise from device delays and environmental noise [5].

In this paper, we specify the timing constraints encountered during the experimental implementation of QPV. Specifically, we adopt the QPV-commitment protocol (c-QPV$^{f}_{BB84}$) [6], which introduces an additional commitment round based on the arrival of qubits. This additional round enhances the protocol's resistance to transmission losses between interacting parties, making it more robust for practical applications. Additionally, we analyze each timing constraint and propose corresponding timing requirements from both applicability and security perspectives.

To address these requirements without introducing costly hardware, we integrate Software-Defined Network (SDN) control into quantum networks. This programmable control plane provides the flexibility needed to implement the c-QPV$^{f}_{BB84}$ protocol effectively. We propose two key functionalities: **time calibration** and **time synchronization**. The time calibration process determines the necessary timing constraints and evaluates the experimental setup, while the time synchronization process ensures uniform delay for all interacting parties. Together, these SDN-based functionalities enhance the reliability and security of the protocol, enabling its implementation in real-world scenarios.

II. Background

A. QPV-commitment Protocol

One of the challenges in practical QPV is the photon loss within the quantum channel. A high loss rate between the verifiers and the prover can undermine security if the QPV protocol lacks loss tolerance. Notably, such protocols are vulnerable to entanglement-based attacks requiring only a single pre-shared EPR pair [7], or they demand a large-scale quantum computer at the prover along with computational assumptions [8]

To mitigate the impact of photon loss, a committing version [9] (or protocol with commitment) is introduced by adding a

small time delay $\delta > 0$ between the arrival time of the quantum information and the classical information at the prover. When the quantum information arrives at the prover (P), they are required to commit to either participate ($c = 1$) or not participate ($c = 0$) in the round. Here we define a round of c-QPV$^{f}_{BB84}$ protocol [5] (Definition. II.1).

Definition II.1 (QPV-commitment protocol)**.** Let $n \in \mathbb{N}$, and consider a $2n$-bit Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. A round of the QPV$^{\text{f}}_{\text{BB84}}$ protocol with commitment, denoted by c-QPV$^{\text{f}}_{\text{BB84}}$, is described as follows:

1) V_0 prepares the EPR pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends one qubit Q and $x \in \{0,1\}^n$ to P, and V_1 sends $y \in \{0,1\}^n$ to P such that x, y arrive a time $\delta > 0$ after Q at P. The classical information is required to travel at the speed of light, while the quantum information can be sent arbitrarily slowly.
2) If the prover receives Q, it immediately confirms that and broadcasts the commitment bit $c = 1$. Otherwise, the prover broadcasts $c = 0$.
3) If $c = 1$, P measures Q in the basis $f(x, y)$ as soon as (x, y) arrive and broadcasts his outcome a to V_0 and V_1. If the photon is lost in the time δ or during the measurement, he sends $\perp$.
4) The verifiers collect (c, a), and V_0 measures the qubit he kept in the basis $f(x, y)$, obtaining result v. If $c = 0$, they ignore the round. If $c = 1$, they check whether $a = v$. If c, a arrived at their appropriate times and $a = v$, they accept. They record 'photon loss' if they both receive $\perp$ on time. If any of the answers do not arrive on time or are different, the verifiers abort.

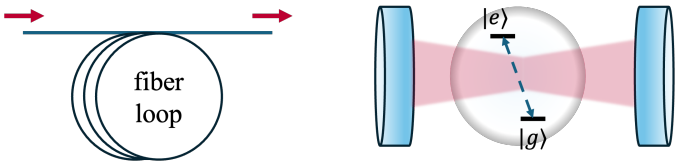
To fully convince the verifier, this protocol is repeated n times. However, the protocol is subject to inherent constraints, which lead to an error rate p_{err}. Let η be the successful message transmission efficiency over n attempts. By executing this protocol n times, an honest prover will broadcast $2n$ outcomes such that the probability of obtaining a correct answer is $\mathbb{P}(c) = \eta(1 - p_{err})$.

B. Quantum memory

Quantum memory [10] is a device that can reliably store and retrieve quantum states for a certain duration without significant loss of fidelity. It is one of the most important devices in large-scale quantum networks [11]. Quantum communication distance is limited to tens of kilometers due to losses in fibers, which exponentially degrades the degree of quantum correlations [12]. For this reason, quantum memory was proposed as part of the quantum repeater to extend the communication distance [13].

In the c-QPV$^{\text{f}}_{\text{BB84}}$ protocol, quantum memory plays a crucial role in maintaining the coherence of qubits during the time delay δ, allowing the prover to correctly measure the quantum state after the measurement basis has been determined. Any loss of fidelity or coherence during this storage period could result in incorrect measurement outcomes therefore affecting the protocol's accuracy.

In the past two decades, quantum memories with high fidelities, high efficiencies, long storage times, and promising multiplexing capabilities have been developed, especially at the single-photon level [14]. In its simplest form (see Fig. 1a), quantum memory relies on delay lines, such as fiber loops or mirror setups, to increase the propagation length of quantum optical signals [15]. However, this approach does not ensure high-fidelity storage. A more advanced alternative is atomic quantum memory [16], which is widely researched. This method involves coherently mapping quantum fluctuations from an optical field onto stationary excitations of atomic spins, enabling more reliable and robust storage, as shown in Fig. 1b.



(a) (b)

Figure 1: (a) A fiber loop serves as a simple quantum memory by delaying photon propagation. (b) An atom placed inside a low-loss optical resonator can significantly enhance light–atom interactions, enabling the reflection of a single photon off the cavity mirror to entangle the photon with the atomic spin [17].

Recent advancements in quantum memory have led to remarkable milestones. In a recent experiment, Ma *et al.* [18] employed the dynamical decoupling technique along with zero first-order Zeeman (ZEFOZ) transitions in Eu^{3+}-doped crystals, achieving a storage time of nearly one hour with a measurement fidelity of 96.4% for coherent laser pulses. Additionally, Hermands *et al.* [19] achieved quantum teleportation through an intermediate node utilizing nuclear spin quantum memory embedded in a nitrogen-vacancy (NV) center in diamond.

While current quantum memories are not yet fully optimized, integrating computer network control techniques can help streamline workflows and utilize these precious quantum memory resources [20].

III. Time sequence problem in c-QPV$^{f}_{BB84}$ Protocol

In most theoretical models, the c-QPV$^{f}_{BB84}$ protocol assumes that all processes occur instantaneously with perfect temporal resolution. However, achieving such precise timing conditions is practically challenging in experimental settings. As a result, inevitable time gaps emerge, which must be carefully considered during protocol implementation. These timing imperfections can arise from the inherent delays introduced by the protocol itself and constraints imposed by the physical platform. Consequently, messages may be intercepted by attackers within these time discrepancies [21]. This section delves into these regions and elaborates on their implications for protocol security.

A. Intersection Region

Consider executing the c-QPV$^{f}_{BB84}$ protocol in an x-dimensional space. To enable the prover to execute the protocol effectively, at least $x+1$ verifiers are required [22]. For each verifier V_i, we define a region R_i as the set of all points in space from which an entity can receive a message from V_i and send a response back to V_i within the allowed time window. This region can be expressed as:

$$R_i = \{\mathbf{p} \in \mathbb{R}^x : d(\mathbf{p}, V_i) \leq \frac{t_{\max}}{2} c\} \tag{1}$$

where $d(\mathbf{p}, V_i)$ is the Euclidean distance between the point $\mathbf{p}$ and the verifier V_i, c is the speed of light, and $t_{\max}$ represents the maximum allowable round-trip time. To make the protocol more practical, the allowable time window should account not only for the round-trip light travel time but also for additional data processing times required by the prover, such as light detection time and qubit measurement time.

Furthermore, for the prover to successfully receive all messages from the verifiers and respond within the required time constraints, the regions defined by these $x+1$ verifiers must overlap. This overlap forms a shared intersection region, denoted as:

$$\Omega = \bigcap_{i=1}^{x+1} R_i \tag{2}$$

where Ω represents the spatial region from which a prover can communicate with all verifiers simultaneously within the given time constraints.

Ideally, we want the intersection region to converge to a single point corresponding to the exact location of the prover. However, achieving such time precision is challenging in experimental implementations. To address these practical constraints, a natural solution is to introduce a more lenient time allowance to accommodate processing delays, such as photon detection and qubit measurement times. Although this relaxation makes the implementation of the protocol more feasible, it also increases the size of the intersection region Ω, where entities can communicate with all $x+1$ verifiers within the allowable time window.

Attackers can manipulate this overlap region to impersonate the legitimate prover. Consider attacks on a two-dimensional c-QPV$^{f}_{BB84}$ protocol in which three attackers are positioned on the connected fiber between the prover and the verifiers. They are able to intercept quantum and classical information from the verifiers, process it locally in a relatively short time (in particular: faster than the honest prover) and coordinate their responses to fool the protocol. Before the protocol commences, the attackers prepare a joint (entangled) quantum state ρ. Then attackers intercept the information sent from the nearest verifier. They copy the intercepted classical information and broadcast it to their fellow attackers. Simultaneously, they perform a unitary quantum operation on the intercepted qubit, retaining one quantum register locally while sending quantum messages to their fellow attackers. After one round of simultaneous communication, all attackers perform a positive operator-valued measure (POVM) to obtain a classical answer, which they send to their respective closest verifier.

The attackers adhere to a subjective mapping communication pattern [23]. The introduction of a generous time delay enables the attackers to complete their communication, thereby increasing the possibility of a successful attack.

B. Timing Specification

To better understand the composition of the region Ω and the time inconsistencies that may arise in a realistic scenario, we analyze the spacetime behavior of a c-QPV$^{f}_{BB84}$ protocol. For simplicity and clarity, we begin by considering a one-dimensional model with only an honest prover and no attackers.

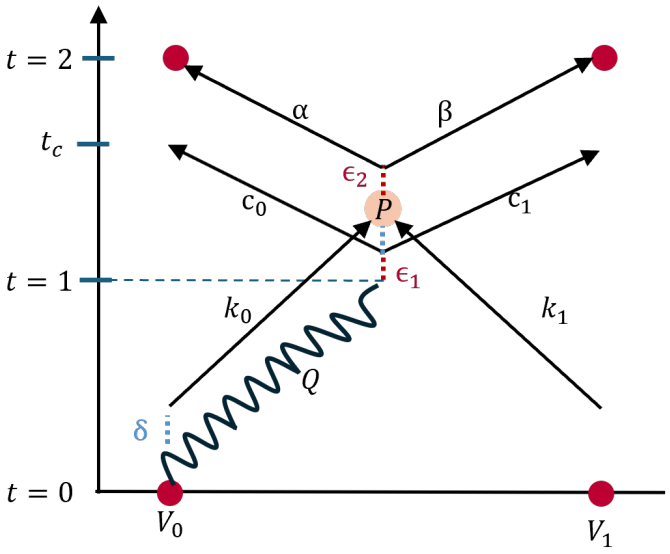


Figure 2: Spacetime geometry of the c-QPV$^{f}_{BB84}$ protocol in the one-dimensional case. The total time delay consists of three key components: the initial processing time ϵ_1 (red), the protocol's inherent time delay δ (blue), and the measurement time ϵ_2 (red).

When the qubit arrives at the prover's location, the first-time delay occurs due to additional processing required to handle the incoming qubit. This includes:

- Photon detection: The photodetector takes time to capture the incoming photon.
- Quantum memory storage: the qubit is stored in a memory device such as a looped fiber or a cavity for later use.
- Message initialization and broadcasting: The prover must initialize and commit as fast as possible.

These processes introduce an initial time delay, denoted as ϵ_1, representing the time from the qubit's arrival to the point when it is fully processed and ready for further operations. Following this initial processing, the qubit rests in the quantum

memory until the arrival of the classical challenge from the verifiers. The duration of this resting period is denoted as δ, and it depends on the timing constraints of the protocol and the performance of the quantum memory.

Once the challenge arrives, another sequence of operations introduces additional delays. The prover must decode the classical challenge to determine the measurement basis. Following this, the experimental setup must be adjusted to perform the required measurement. This involves aligning waveplates to match the desired basis, configuring a polarizing beam splitter to separate the qubit's components based on polarization, and activating single-photon detectors to measure the outcome. We denoted this time delay as ϵ_2, which accounts for the time required to decode the challenge and qubit measurement.

In total, the time at the prover's location can be characterized by three key components: the initial processing time (ϵ_1), the protocol's time gap (δ), and the measurement time (ϵ_2), as shown in Fig. 2. The first two combined affect the applicability of the protocol, and the last one brings security uncertainty.

C. Timing Requirements

The integrity of quantum position verification hinges crucially on the precise coordination of timing and spacetime positioning. These inherent time gaps reduce the security of the protocol. Therefore, it is essential to synchronize such that each commitment c_i arrives outside the light cone of other keys in spacetime. To formalize this relation, we utilize spacetime geometry, which is a set of all locations in both space and time. An event $C(x,t)$ occurs at space x and time t. Throughout our analysis, we assume a flat spacetime, characterized by $(t, x_1, x_2, ..., x_n)$ with $t, x_1, x_2, ..., x_n \in \mathbb{R}$. We define the *causal future* $C^+(x)$ of an event x as the set of all events (light cone) reachable from x, similarly, we define *causal past* as $C^-(x)$ as all events (light cone) in the past that can influence x.

Following such notation, this condition can be expressed as:

$$C^-(x_c, t_c) \bigcap C^+(x_k, t_k) = \varnothing \tag{3}$$

If this condition holds, then these two events are spacelike separated. This can also imply the time condition for qubit transmission, denoted as t_q:

$$t_q = t_c - \Delta t - \|C(x_c, t_c) - C(x_k, t_k)\|c \tag{4}$$

Where t_c is the time that commitment arrives, $\Delta t = \epsilon_1 + \delta$, $\|C(x_c, t_c) - C(x_k, t_k)\|$ is the Euclidean distance between two events.

Implementing the c-QPV$^f_{BB84}$ protocol requires addressing the two timing constraints above. First, the limited quantum memory lifetime poses a significant challenge. Current quantum memory devices cannot store photons for extended periods, which restricts the scale of the experiment. The second timing constraint arises from security requirements. To mitigate the risk of attacks, the commitment must be received outside the light cone of other keys' transmission. Consequently, it is essential to meticulously estimate and plan the timing of each process within the protocol to ensure the honest prover can successfully complete their tasks.

IV. Implementing c-QPV$^f_{BB84}$ protocol with programmable control plane

Meeting these timing requirements we introduced necessitates precise control over the quantum network, which can be prohibitively costly on physical platforms. As a more adaptable approach, we explore the integration of SDN (Software-Defined Networking) control into quantum networks and discuss how this control strategy enhances the practical implementation of the c-QPV$^f_{BB84}$ protocol in real-world scenarios.

A. Quantum SDN Network

A programmable control plane facilitates dynamic, software-defined management of network resources. Among various approaches, Software-Defined Network (SDN) control stands out as particularly effective due to its flexibility and robustness in network management. SDN control separates the network's control functions from the forwarding hardware, namely the SDN controller, enabling centralized and programmable management.

Qubits, the information carriers in quantum networks, are characterized by extremely short lifetimes and are difficult to monitor, which presents significant control challenges. Intuitively, integrating SDN can enhance the flexibility and efficiency of managing these networks. SDN control enables precise timing control, resource optimization, and scalability, making it ideal for meeting the strict requirements of quantum protocols [24]. Additionally, developing standardized protocols and interfaces is essential for seamlessly integrating quantum networks into existing communication infrastructures, ensuring better compatibility and functionality.

A simple illustration of implementing the c-QPV$^f_{BB84}$ protocol with SDN control is shown in Fig. 3. The process begins when a user submits an authentication request for a pre-authorized position through the Position Verification (PV) application. This request, transmitted to the SDN controller via the northbound interface, constitutes the first step.

Upon receiving the request, the SDN controller initiates a series of actions. In the second step, it identifies appropriate verifiers based on the current network topology and resource availability. Subsequently, it configures the routing paths and adjusts the timing parameters, including both the time calibration and synchronization phases.

After the configuration is complete, the controller sends a start command to the selected verifiers. In step 3, the verifiers execute the c-QPV$^f_{BB84}$ protocol, reporting the measurement outcomes and elapsed time back to the controller. The controller analyzes this data to validate the position claim and decides whether to accept or reject it. Finally, in step 4, the decision is communicated to the user via the northbound interface.

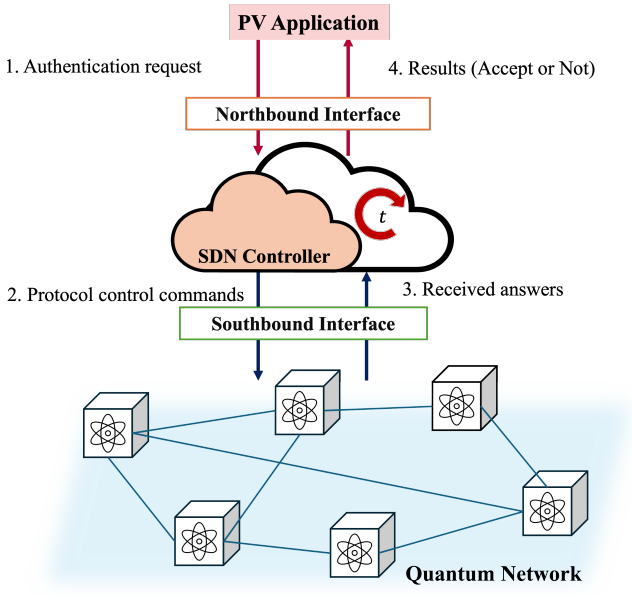


Figure 3: A simplified illustration of a quantum SDN network architecture. Similar to classical SDN, communication occurs through northbound and southbound interfaces. The northbound API connects the SDN controller to high-level applications, facilitating interaction between the controller and user-facing services. Conversely, the southbound API connects the controller to the underlying quantum network devices, enabling the configuration and management of quantum hardware.

B. Time Calibration Phase

The calibration phase improves the reliability of the protocol by accurately measuring elapsed time and mitigating time-related uncertainties caused by factors such as hardware delays and environmental noise.

The calibration process begins with the assumption that all quantum nodes in the network are homogeneous, ensuring consistent quantum operation times across nodes. Additionally, it is assumed that all designated verifiers are reliable. Once the nodes are selected as verifiers, the controller issues commands to each node to prepare a qubit and perform one round of a unitary quantum channel, corresponding to step 2. After this step, the verifiers report back with critical timing information, including the average quantum operation time and the maximum quantum memory storage time, denoted as δ_m.

Using these data, the controller evaluates whether the commitment under the current configuration is received after the measurement outcome, as outlined in Sec. III-C. If the timing meets the required criteria, the setup is approved for continuation. Otherwise, the controller can be programmed to restart the process or reject the request outright. Nonetheless, the controller retains all collected data for potential recalibration. The sequence diagram illustrating this calibration process is shown in Fig. 4. After this evaluation, the controller computes the operational window t_{max} (see Sec. III-C), which plays a key role in the subsequent stages of the protocol.

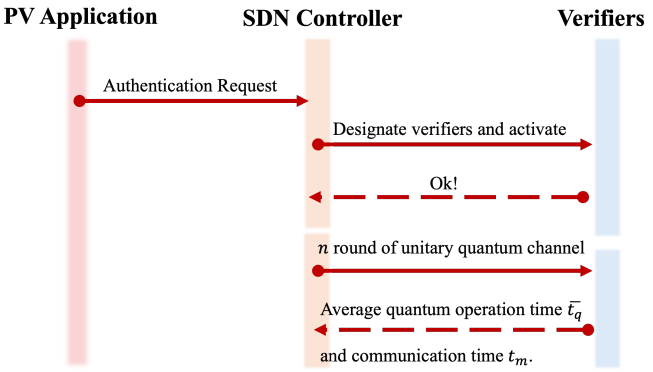


Figure 4: The sequence diagram of timing calibration using SDN control.

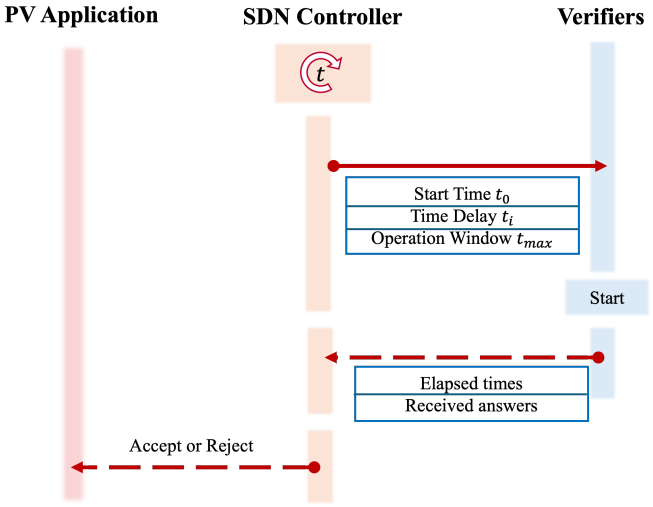


Figure 5: The sequence diagram of timing synchronization and following processes using SDN control.

C. Time Synchronization Phase

The time synchronization phase (see Fig. 5) is essential for the secure implementation of the c-QPV$^f_{BB84}$ protocol. Each verifier involved in the protocol must individually calculate the delay time while adhering to broader timing constraints. The SDN controller facilitates this process through its comprehensive network oversight and programmability.

Following the time calibration phase, the controller calculates the necessary time delays for each verifier V_i based on their respective distances d_i. The time delay t_i for each verifier is determined by the formula:

$$t_i = \max\left(\frac{t_{\max}}{2} - \frac{d_i}{c}, 0\right) \tag{5}$$

Once calculated, the timestamp for each verifier includes:

- **Start Time:** The precise moment when the verifier should begin its task.

- **Time Delay (t_i):** The calculated delay which ensures all actions are temporally aligned.
- **Operation Window ($t_{\max}$):** The maximum allowable round-trip time.

These timestamps are encoded into messages using a standardized format, typically as a JSON object or a similar structured data format, and then transmitted to each verifier via the SDN controller's southbound interface. This method effectively minimizes the impact of communication delays between the verifier and the controller.

Upon receiving the outcomes from the prover, each verifier sends all relevant outcomes and timing information back to the controller. If the information is consistent and unified, the controller marks this round of the protocol as 'Accept'. Otherwise, the controller marks it as 'Reject'.

V. Conclusion

In this work, we leveraged the c-QPV$^{f}_{\text{BB84}}$ protocol to investigate the impact of time constraints on both protocol reliability and security, and explored strategies to mitigate these constraints under real-world scenarios. We first analyzed the intersection region formed by the round-trip light travel distance from each verifier to the prover, highlighting its implications for protocol security. Furthermore, we identified three key time delays affecting the protocol: the initial processing time, the protocol's inherent delay, and the measurement time. Based on these findings, we proposed timing requirements that ensure an honest prover can successfully complete the protocol while maintaining security guarantees.

To enhance the protocol's feasibility, we showed a possible approach to embed SDN control into quantum networks, introducing two key functionalities: time calibration and time synchronization. The time calibration phase establishes the necessary timing constraints and evaluates the experimental setup, while the time synchronization phase ensures uniform delays for all interacting parties. Together, these SDN-based functionalities significantly improve the protocol's reliability and security, facilitating its implementation in realistic scenarios.

Despite these advancements, the protocol's efficiency remains constrained by the technological challenge of requiring high-fidelity quantum memories. Moreover, our current work operates under a worst-case assumption, where attackers can intercept all communications, including qubits. Future research should explore attack success probabilities and attacker behavior under partial interception conditions. Additionally, we plan to validate our methodology further using an experimental testbed.

As quantum network technologies continue to advance, our findings contribute to the development of practical quantum position verification protocols and programmable quantum control planes, paving the way for more secure and scalable quantum communication systems.

References

[1] J. Clark and J. Jacob, "A survey of authentication protocol literature," 1997.

[2] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions," *SIAM Journal on Computing*, vol. 43, no. 1, pp. 150–178, 2014.

[3] Z. Zhang, C. Papagianni, F. Speelman, and P. Grosso, "Towards complete quantum network stacks, a survey," *IEEE Network*, 2024.

[4] A. Bluhm, M. Christandl, and F. Speelman, "A single-qubit position verification protocol that is secure against multi-qubit attacks," *Nature Physics*, vol. 18, no. 6, pp. 623–626, 2022.

[5] L. Escolà-Farràs and F. Speelman, "Lossy-and-constrained extended non-local games with applications to cryptography: Bc, qkd and qpv," 2024. [Online]. Available: https://arxiv.org/abs/2405.13717

[6] R. Allerstorfer, A. Bluhm, H. Buhrman, M. Christandl, L. Escolà-Farràs, F. Speelman, and P. V. Lunel, "Making existing quantum position verification protocols secure against arbitrary transmission loss," *arXiv preprint arXiv:2312.12614*, 2023.

[7] C. C. W. Lim, F. Xu, G. Siopsis, E. Chitambar, P. G. Evans, and B. Qi, "Loss-tolerant quantum secure positioning with weak laser sources," *Physical Review A*, vol. 94, no. 3, p. 032315, 2016.

[8] J. Liu, Q. Liu, and L. Qian, "Beating classical impossibility of position verification," *arXiv preprint arXiv:2109.07517*, 2021.

[9] R. Allerstorfer, L. Escolà-Farràs, A. A. Ray, B. Skoric, and F. Speelman, "Continuous-variable quantum position verification secure against entangled attackers," *arXiv preprint arXiv:2404.14261*, 2024.

[10] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," *Nature photonics*, vol. 3, no. 12, pp. 706–714, 2009.

[11] R. Allerstorfer, H. Buhrman, F. Speelman, and P. V. Lunel, "On the role of quantum communication and loss in attacks on quantum position verification," *arXiv preprint arXiv:2208.04341*, 2022.

[12] K. Heshami, D. G. England, P. C. Humphreys, P. J. Bustard, V. M. Acosta, J. Nunn, and B. J. Sussman, "Quantum memories: emerging applications and recent advances," *Journal of modern optics*, vol. 63, no. 20, pp. 2005–2028, 2016.

[13] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018.

[14] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, "Experimental demonstration of quantum memory for light," *Nature*, vol. 432, no. 7016, pp. 482–486, 2004.

[15] Y. Lei, F. Kimiaee Asadi, T. Zhong, A. Kuzmich, C. Simon, and M. Hosseini, "Quantum optical memory for entanglement distribution," *Optica*, vol. 10, no. 11, pp. 1511–1528, 2023.

[16] X. Maitre, E. Hagley, G. Nogues, C. Wunderlich, P. Goy, M. Brune, J. Raimond, and S. Haroche, "Quantum memory with a single photon in a cavity," *Physical review letters*, vol. 79, no. 4, p. 769, 1997.

[17] A. Reiserer, N. Kalb, G. Rempe, and S. Ritter, "A quantum gate between a flying optical photon and a single trapped atom," *Nature*, vol. 508, no. 7495, pp. 237–240, 2014.

[18] Y. Ma, Y.-Z. Ma, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo, "One-hour coherent optical storage in an atomic frequency comb memory," *Nature communications*, vol. 12, no. 1, p. 2381, 2021.

[19] S. Hermans, M. Pompili, H. Beukers, S. Baier, J. Borregaard, and R. Hanson, "Qubit teleportation between non-neighbouring nodes in a quantum network," *Nature*, vol. 605, no. 7911, pp. 663–668, 2022.

[20] W. Kozlowski, F. A. Kuipers, R. Smets, and B. Turkovic, "Quip: A p4 quantum internet protocol prototyping framework," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 7, pp. 1936–1949, 2024.

[21] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[22] D. Unruh, "Quantum position verification in the random oracle model," in *Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II 34*. Springer, 2014, pp. 1–18.

[23] E. Culf and T. Vidick, "A monogamy-of-entanglement game for subspace coset states," *Quantum*, vol. 6, p. 791, 2022.

[24] V. Martín, A. Aguado, J. P. Brito, A. Sanz, P. Salas, D. R. López, V. López, A. Pastor-Perales, A. Poppe, and M. Peev, "Quantum aware sdn nodes in the madrid quantum network," in *2019 21st International Conference on Transparent Optical Networks (ICTON)*. IEEE, 2019, pp. 1–4.