2025 IMEKO TC-6 International Conference on
Metrology and Digital Transformation - **M4DConf 2025**
Benevento, Italy, September 3-5, 2025

Quantum Communications for Distributed Measurement Systems: Current Situation and Research Trends

Arman Neyestani, Ioan Tudosa, Luca De Vito, Fatemeh Khalesi†, Sergio Rapuano*

Department of Engineering, University of Sannio, Benevento, Italy
{neyestani, ioan.tudosa, devito, rapuano}@unisannio.it
† f.khalesi@studenti.unisannio.it

***Abstract* – This survey analyses how five key mechanisms—Quantum Key Distribution (QKD), Quantum Secure Direct Communication (QSDC), entanglement-enhanced sensing, Quantum Clock Synchronization (QCS), and quantum teleportation/entanglement swapping—map onto the core metrological attributes of accuracy, stability, sensitivity, synchronization, security, and traceability. The paper identifies the principal research gaps— in particular, scalable entanglement distribution, hybrid classical–quantum integration, and SI-traceable calibration of quantum devices—and the technical advances required to translate laboratory prototypes (e.g. QKD links, QSDC networks, entangled-clock arrays, and QCS demonstrators) into field deployable quantum-enabled metrology.**

Keywords: Quantum Metrology, QKD, Quantum Clock Synchronization, Distributed Sensing, Traceability

I. INTRODUCTION

Quantum communication technologies are emerging as transformative tools in the field of measurement and metrology. Modern Distributed Measurement Systems (DMSs) demand extreme accuracy, stability, and reliability, while also needing robust security and synchronization in distributed environments. Classical DMSs are based on fundamental limitations: noise limits the precision of sensor data and cyber threats endanger data integrity [1]. By incorporating quantum communication resources, these limitations can be overcome – quantum techniques enhance the achievable measurement accuracy and provide unconditional security guaranteed by physical laws [1]. Indeed, quantum entanglement and related phenomena enable measurement precisions beyond classical limits and fundamentally secure data transmission. Quantum communication, alongside quantum sensing and computing, is thus poised to elevate measurement systems to unprecedented performance levels. Recent advances illustrate the impact: quantum networks have been demonstrated to enable applications beyond the reach of classical networks, including provably secure communications, high-precision clock synchronization, and distributed quantum sensing [2]. This survey examines how various quantum communication mechanisms (e.g. quantum key distribution, entanglement-based networks, quantum clock synchronization, etc.) influence core metrological attributes of measurement systems. This survey reviews the current state-of-the-art and key case studies, analyzes comparative benefits and remaining challenges, and emerging research directions and standardization efforts. The overarching research question is how quantum communications can improve measurement systems' attributes (accuracy, stability, sensitivity, synchronization, security, and traceability) and what new capabilities or considerations they bring. By synthesizing recent findings, the aim is to provide researchers with a fresh perspective on integrating quantum communications into next-generation DMSs. This paper begins by recalling the well-known core metrological attributes of measurement systems, then examines in detail the impact of each quantum communication mechanism—supported by illustrative case studies—and concludes with a comparative analysis of remaining research gaps and a conclusion on future developments.

II. QUANTUM COMMUNICATION MECHANISMS AND THEIR IMPACT ON MEASUREMENT ATTRIBUTES

Measurement systems are judged by six interdependent attributes—accuracy, stability, sensitivity, synchronization, security, and traceability—that together define metrological quality and suitability [3, 4]. Quantum communication furnishes a complementary toolkit—QKD, QSDC, entanglement-based sensor networks, QCS, and quantum teleportation—that can elevate these attributes beyond classical limits: QKD and QSDC deliver information-theoretic security and maintain traceability, entanglement-enhanced sensing improves sensitivity and accuracy, QCS achieves picosecond-level timing alignment, and teleportation enables long-range transfer of quantum standards. The remainder of this paper reviews each mechanism, surveys representative demonstrations, and assesses the outstanding technical limitations to practical deployment.

*This work was supported by PNRR – Mission 4, Component 2, Investment 1.5 – ECS_00000024 – Rome Technopole – Call CODBAN_000378 – Spoke 3 – Project N. UR301-2023-000090 – "MES&QT: Distributed Measurement Systems based on Quantum Technologies for Secure Communications".

A. QKD and Secure Keying

QKD is a quantum communication protocol that enables two parties to generate a shared secret key with security based on the principles of quantum mechanics. By transmitting quantum states (such as polarized photons), QKD ensures that any eavesdropping attempt will be detectable due to unavoidable quantum disturbances. This guarantees information-theoretic security, making QKD particularly valuable for critical measurement infrastructures—such as power grids and aerospace systems—where secure data transmission is essential [5].

The primary impact of QKD on DMS attributes is a significant enhancement of the security of measurement data: QKD delivers provably secure encryption keys, protecting data confidentiality and integrity even against adversaries equipped with quantum computers. This, in turn, reinforces traceability and trust in remote measurements, as data authenticity can be verified throughout transmission. However, QKD does not improve attributes like accuracy or sensitivity, and its deployment introduces requirements for specialized hardware and integration with classical networks. Despite these challenges, QKD represents a potential solution for securing measurement data, already demonstrated in real-world fiber and satellite networks [6, 7].

B. Quantum Secure Direct Communication

Quantum Secure Direct Communication (QSDC) transmits confidential data via entangled quantum states—bypassing separate key exchange—and guarantees that eavesdropping yields only random noise. and inter-city links have reached 100 km, with free-space and satellite trials underway. QSDC significantly enhances the *security* attribute by delivering information-theoretic confidentiality and integrity and bolsters *traceability* by making tampering immediately detectable [8]. Its practical uptake is limited by low data rates, the complexity of reliable state discrimination, and the need for specialized hardware (entangled photon sources, quantum memories), but ongoing advances—and prospective satellite deployments—point to scalable, quantum-secure DMSs.

C. Entanglement-Based Distributed Sensing and Enhanced Sensitivity

Entanglement-based distributed sensing leverages quantum-correlated probe states to surpass classical precision limits—scaling as $1/N$, where N is the number of entangled probes (Heisenberg limit) rather than $1/\sqrt{N}$ Standard Quantum Limit (SQL) [1]—as exemplified by a four-node entangled atomic clock network achieving a 4.5 dB improvement in timing precision—equating to a $\tilde{2}.8\times$ reduction in phase variance—over independent clocks, and an 11.6 dB decrease in projection noise (nearly a fourfold reduction) while preserving high entanglement fidelity [9]. By sharing entangled probes across sensors, quantum correlations suppress noise to boost sensitivity and accuracy, align phases for sub-SQL synchronization, anchor remote devices to common SI standards, and secure data by limiting access to parties performing the required joint quantum measurement.Scaling beyond a few nodes is difficult because entanglement decays with channel loss and environmental noise, and high-order multipartite states are generated only probabilistically; chaining more resilient Bell-pair link (which is usually a two-node entanglement channel that, owing to its facile generation and swapping, underpins scalable teleportation, QKD, and distributed sensing at a minor sensitivity cost) can alleviate these issues, though at the expense of ultimate sensitivity [10, 11]—but ongoing advances in entangled photon sources, quantum memories, and standardized protocols suggest a forthcoming redefinition of metrological capabilities beyond classical bounds.

D. Quantum Clock Synchronization and Timing Links

Quantum clock synchronization (QCS) harnesses entangled photons to synchronize remote clocks with femtosecond to picosecond precision, immune to classical delay asymmetries and capable of detecting timing spoofing through broken quantum correlations [12]. Satellite-based QCS, demonstrated by the Micius mission, targets sub-100 fs alignment across global distances. These advances dramatically boost the synchronization attribute—enabling high-fringe-contrast interferometry, coherent multi-node sensing, and sub-picosecond event timestamping—and reinforce security, since any intercept or delay breaks entanglement and is immediately evident. Key challenges include photon loss and decoherence over extended links and scaling to multiple users; potential solutions involve wavelength-division multiplexing, quantum repeaters, and error-corrected quantum memories to extend range and network capacity.

E. Quantum Teleportation and Remote State Transfer

Quantum teleportation transfers an unknown quantum state to a distant node using pre-shared entanglement and two bits of classical information, with no residual copy at the source and immunity to eavesdropping on the teleported state. In metrology, this facilitates remote calibration by conveying quantum standards without physical transport, thereby enhancing traceability and *accuracy*. State fidelity quantifies the statistical overlap between the teleported and target quantum states, interpreted as the probability that the recovered qubit is correct [13]. A mean value of 0.80 over 1,200 km surpasses the 0.67 classical ceiling and approaches about the 0.91 achieved on a 64 km fibre link, demonstrating strong long-range performance. Heralding rate is the number of successful, signalled teleportation events per second; 32 events is unusually high for satellite experiments, which typically operate at hertz scale [14]. Teleporting a phase-encoded calibration tone over 64 km of fiber produced a phase deviation of only 0.3° ($\approx 5 \times 10^{-3}$ rad), corresponding to a $15\ \mathrm{mHz}$ uncertainty on a $10\ \mathrm{MHz}$ carrier. Chained entanglement swapping on Micius extended entanglement to 1,000 km at ap-

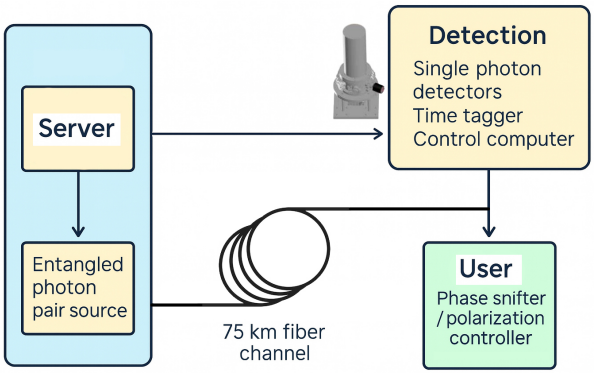

Fig. 1. Experimental setup flowchart of a single-user QCS protocol over a 75 km optical fiber link [2]

.

proximately $1\ \mathrm{s}^{-1}$ pair rates, boosting synchronization and sensitivity in networked sensors. Security is built in the classical feedforward bits, which reveal no state information without the entangled resource. in other hand, Bell-state measurement projects a two-qubit system onto the entangled basis [15]:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right).$$

where Φ labels the even-parity pair, Ψ labels the odd-parity pair, and is implemented by interfering two photons and detecting coincidences to identify the Bell state—an essential step for quantum teleportation. However, key challenges remain low success probabilities ($< 10^{-4}$ at continental scales), the need for quantum memories with millisecond coherence, and Bell-state measurement efficiencies below 80%. Progress in high-brightness sources, multiplexed memories, and loss-tolerant detection will be pivotal for teleportation-enabled metrology networks.

III. CASE STUDIES

To ground the discussion in practical terms, a selection of case studies is reviewed where quantum communication technologies have been implemented in measurement systems or testbeds. These examples highlight the affected performance attributes and report key metrics, demonstrating the current situation in this research area.

A. *Case Study 1: Quantum-Enhanced Clock Synchronization over 75 km Fiber*

In 2023, researchers demonstrated a multi-user quantum clock synchronization network linking a server and remote client over a 75 km optical fiber using entangled photons. In this experiment [2] as shown in Fig. 1, a polarization-entangled photon source at the server generated pairs of photons that were distributed to the remote user. By measuring arrival times of entangled photons (one traveling to the user and back, one measured locally), the clock offset between the user and server was determined with extremely high precision. The results were impressive: they achieved a measured clock time difference uncertainty of 4.45 ps, and a timing stability characterized by a TDEV of 426 fs after 4000s of averaging. For comparison, classical network time synchronization (e.g. Network Time Protocol (NTP) or Precision Time Protocol (PTP) over that distance) would be in the nanoseconds to microseconds range at best, and GPS typically offers nanoseconds precision under ideal conditions. This quantum method inherently avoided errors from asymmetric channel delays, since only one-way travel of quantum signals was used (with entangled timing correlations). Synchronization was directly improved to ps-level, vastly better than classical tech. This also improves accuracy for any measurements dependent on the clocks (e.g. time-of-flight measurements or comparing remote frequency standards). The scheme was secure against certain attacks (like delay manipulation), as noted by the authors, because any attempt to tamper would be evident in the correlation data [2]. The case study illustrates quantum communication enabling a new regime of synchronization useful for e.g. distributed radio telescopes, financial transaction timestamping, and fundamental constant measurements (where remote clocks need to be compared). It also showed scalability: the use of WDM (wavelength multiplexing) means multiple users could be synchronized off one entangled source, each getting their own wavelength channel.

B. *Case Study 2: Entangled Sensor Network for Distributed Quantum Sensing*

A notable experiment in 2020 (K. Malia et al.) [9] involved an entangled network of atomic clocks or sensors demonstrating improved measurement precision across nodes. In this setup, up to four atomic ensembles (acting as atomic clocks or interferometric sensors) were entangled via a shared quantum non-demolition measurement. The network was used to measure a common phase (or frequency) with enhanced precision. The reported gain was significant: the entangled network achieved a 4.5 dB better precision than a network with only local (separate) entanglement at each node, and about 11.6 dB better precision than a comparable classical network limited by independent quantum projection noise because phase noise maps directly onto fractional-frequency error, the result corresponds to tightening clock comparisons from the typical 10^{-12} level to the mid-10^{-13} range after a single second of averaging, with continued τ^{-1} Heisenberg scaling thereafter.. In other words, the entanglement between nodes gave a multi-fold reduction in measurement uncertainty beyond the usual $1/\sqrt{N}$ scaling, where N is the number of Nodes. The experiment demonstrated both atomic clock comparison and interferometric phase sensing, showing the generality of the approach. This directly relates to sensitivity/accuracy – it shows that distributing entanglement can improve the signal-to-noise ra-

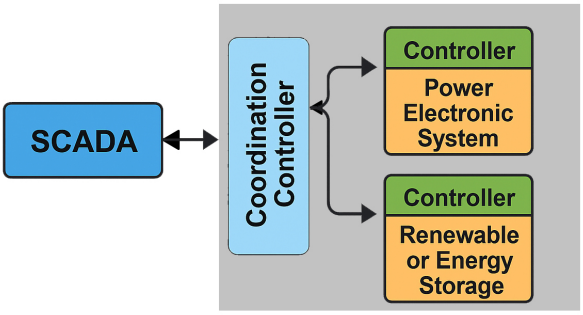

Fig. 2. A supervisory SCADA layer exchanges data with a central coordination controller, which issues commands to two local controllers—one governing the power-electronic interface and the other the renewable/energy-storage unit [17].

tio of measurements across a network. Each node individually has certain sensitivity, but together (when entangled), the network functions like a single larger sensor with lower noise. This has implications for, say, coordinating arrays of quantum sensors to detect tiny gravitational perturbations or comparing distant optical clock frequencies for geodesy (measuring gravitational redshift differences). By improving precision, it also strengthens traceability between standards: e.g., measuring frequency ratios to 18-digit accuracy as cited by the authors (beyond what was previously possible). The experiment did not focus on security, but if one can distribute entanglement for precision, one might also integrate QKD in parallel for secure classical channels among the sensor nodes (the Phys. Rev. A 2025 paper by Moore et al. indeed considered secure quantum-enhanced sensing protocols [16]). The challenge highlighted in this case was technical: entangling multiple macroscopic atomic systems and maintaining that entanglement was non-trivial and required careful collective measurements.

C. *Case Study 3: QKD-Secured Smart Grid Sensor Communications*

In 2022, a team from Oak Ridge National Lab and partners demonstrated the integration of Quantum Key Distribution into a smart grid communication network for securing measurement data [17]. They deployed a QKD system (entanglement-based QKD using a commercial Qubitekk unit) on a realistic utility fiber network between an electrical substation and a control center as shown in Fig. 2. The purpose was to authenticate and encrypt SCADA communications (telemetry from sensors like voltage/current meters and control signals to equipment) using the quantum-generated keys. The case study showed that QKD could operate alongside the utility's existing data traffic and continuously provide fresh secret keys for cryptographic use. They specifically implemented the QKD keys in the Message Queuing Telemetry Transport (MQTT) messaging protocol for machine-to-machine SCADA data, achieving quantum-enhanced authentication of commands and measurements. The feasibility was confirmed in a real-world environment (Chattanooga Electric Power Board (EPB) utility), not just a lab. The primary attribute in this case is security – the measurement system (power grid sensors and actuators) was secured against eavesdropping and tampering by virtue of QKD's unbreakable encryption keys. This improves the trustworthiness of grid measurements (voltage readings, frequency measurements, etc.), which is crucial for grid stability and safety. A power system operator can be confident that data has not been spoofed or altered in transit if it's protected by QKD-based authentication. Indirectly, this contributes to the stability and reliability of the measurement system (not the sensor reading itself, but the overall infrastructure), because a cyber attack attempting to falsify measurements can be thwarted. The experiment also underscores the importance of standards and interoperability – they had to use specific networking setups to integrate QKD, and they highlight challenges like key management, latency, and scalability for more nodes. Nevertheless, this case proved that quantum communication (QKD) can be added to critical measurement networks today to elevate security without harming the real-time operation (the key rate was sufficient for frequent re-keying of messages, and the classical control traffic coexisted with quantum signals on the same fiber via wavelength multiplexing). Even a modest QKD key rate of $\sim$1 kbps is ample: phasor measurement units (PMUs) transmit about 4 kbps of sensor data, so 1 kbps of fresh key material allows subsecond rotation of the AES key, well above the security requirements of North American Electric Reliability Corporation (NERC) and Critical Infrastructure Protection (CIP). Time alignment itself still relies on existing GPS or emerging quantum-synchronization links; QKD secures the data path but does not affect the timing budget. Thus, throughput is sufficient for remote smart-grid measurements, and synchronization performance remains unchanged while confidentiality and integrity are raised to information-theoretic levels.

D. *Case Study 4: Multi-User Quantum Secure Direct Communication Network*

Another illustrative example, though more futuristic, is the 15-user QSDC network demonstrated in China in 2021 [18]. While this was primarily a communication network experiment, one can envision its application in a measurement context for highly secure collaborative DMSs. In the demonstration, 15 users formed a fully connected network where any pair could directly exchange secret messages through entangled photon pairs and sum-frequency generation (a technique to perform Bell state measurements). They achieved >95% entanglement fidelity between any two users over 40 km fiber links and an information transmission rate above 1 kbit/second. From a metrology perspective, imagine these 15 nodes are distributed sensing

Mechanism	Key Attribute(s)	Notable Achievements	Limitations
QKD	Security, traceability	Utility fiber QKD secures SCADA; proven unconditional key security [17]	$\sim$100 km range; low key rate; needs single-photon hardware; standardization needed
QSDC	Security, authenticity	15-user, 40 km, >95% fidelity; direct quantum messaging [18]	Very low data rates; experimental; range limited; complex state management
Entanglement-Enhanced Sensing	Sensitivity, accuracy, (sync, security)	>11 dB precision gain in 4-node clock network [9]; quantum-secure metrology proposed [1, 16]	Entanglement fragile; small demos; quantum memory and specialized algorithms needed
QCS	Synchronization, timing accuracy, (security)	4.5 ps sync over 75 km fiber [2]; secure against delay attacks	Range/robustness limits; ultrafast detectors; not widely deployed; classical comm. still needed
Teleportation or Swapping	Enabler for sensitivity, sync, traceability	>1000 km entanglement via satellite; quantum internet backbone [13]	High loss; low success probability; quantum memory needed; complex coordination

Table 1. Compact summary of quantum communication mechanisms in measurement systems.

stations (for environmental monitoring, for example) that need to share data or aggregate results securely. QSDC would allow them to send not just keys but the measurement data itself in quantum form, with eavesdroppers gaining no information. Security is again the focus – data confidentiality and integrity across the network were guaranteed by physics. There is also a resilience benefit because QSDC doesn't rely on stored keys, the system is less vulnerable to key compromise or man-in-the-middle attacks (any attempt would break the entanglement and be noticed). The trade-off is the modest data rate. This network doesn't yet improve the accuracy or sensitivity of the measurements being shared, but it ensures the secure collaboration of multiple measuring units. This is relevant for distributed measurement projects (like an array of air quality sensors sending readings to each other and a central hub without fear of tampering, or distributed timekeeping where clocks exchange correction data securely). The case study also provided insight into scalability: the network used innovative multiplexing to connect many users without a trusted node. This hints at how future quantum networks might simultaneously cater to multiple functions – e.g., a single quantum network could handle QKD, QCS, and QSDC between many parties, serving as a multipurpose metrology backbone.

IV. DISCUSSION AND RESEARCH GAPS

Having examined various quantum communication mechanisms and their demonstrated impacts, a comparison of their relative advantages and a discussion of remaining research gaps is presented. Table 1 summarizes the core quantum communication mechanisms covered, the measurement attributes they principally improve, examples of achievements, and associated challenges or limitations.

From the table 1, no single quantum communication technology addresses all performance attributes, but each has a niche: For security and data integrity, QKD (and to a more experimental degree, QSDC) are the go-to solutions. They dramatically enhance the security attribute with proven theoretical security, something classical methods cannot match. However, they do not inherently improve measurement precision or accuracy – they ensure the trustworthiness of the measurement process rather than the quality of the raw measurement itself. Their deployment, therefore, is often a question of infrastructure and engineering (deploying fibers or satellites, handling keys) and aligning with industry standards, rather than altering the sensor physics.

For sensitivity, accuracy, and precision, entanglement-based approaches (quantum metrology, sensor networks) are unparalleled. They tackle the core physics of measurement by reducing noise floors and enabling correlated measurements. The potential here is transformative for high-end metrology (like clock networks, gravitational wave detection, etc.). The drawback is complexity – these improvements often require pristine laboratory conditions, careful state preparation, and low-noise environments. Real-world sensors (in industrial settings, for example) might find it hard to utilize these exotic states without more robust technology. There is also a diminishing returns vs complexity tradeoff: achieving a small additional precision gain might require exponentially more complex entangled states or error correction.

For synchronization, QCS is a clear quantum advantage solution. It directly outperforms classical synchronization in principle. If one's application needs timing beyond what GPS or fiber two-way can do, quantum is the way forward. But if classical synchronization is satisfies the design specifications, then QCS will be a tough sell. Right now, only very demanding applications (e.g. experimental tests of fundamental physics, or possibly future telecom networks at single-picosecond bit alignment) truly need what QCS offers. That being said, as other parts of technology advance (like analog-to-digital converter speeds, high-frequency trading, etc.), picosecond synchronization might become more relevant [19].

Interestingly, some attributes are interrelated, and quantum technologies can target them together. For instance, entanglement helps both sensitivity and synchronization (an entangled clock network yields better precision in time offset measurement, effectively synchronizing more accurately). Security can be layered on top of entanglement-

based sensing, meaning one can design a system that is simultaneously more precise and more secure than its classical counterpart. These multi-faceted quantum systems are very appealing but also highlight research gaps: integrating different quantum protocols together is complex. The Moore [16] work exemplifies this by mixing entangled and separable states to keep security in a large sensor network – essentially a hybrid approach to maintain both precision and security at scale. This is a new direction, blending QKD concepts with quantum sensing.

Despite rapid progress, key research gaps limit the broad impact of quantum communication on metrological attributes such as security, sensitivity, synchronization, and traceability [20]. Scaling quantum networks beyond current point-to-point or small multi-node demonstrations (e.g., QKD or QCS over tens of kilometers, entanglement-enhanced sensing in 2- 4 node labs) is hindered by the fragility of entanglement, resource demands, and a lack of operational quantum repeaters. Without advances in error-corrected quantum memory and efficient multi-node protocols, network-wide secure synchronization or entanglement-based precision remains unattainable. Integration with classical infrastructure also presents challenges: QKD devices must support existing IT standards and failover schemes, while QCS outputs require seamless interfacing with time distribution systems. Moreover, metrological calibration and standardization of quantum systems are underdeveloped—for instance, establishing SI-traceable standards for single-photon detectors or certifying quantum time transfer is ongoing, with efforts like ISO/IEC 23837-1 (2023) [21] and NIST-led detector standards [22]. Practicality remains an issue as many protocols need high photon rates or cryogenic components, and translating laboratory results (e.g., picosecond synchronization over 75 km fiber, $>$11 dB sensitivity gains in entangled clocks) into real-world, resource-efficient, telecom-compatible devices is not yet realized. Ultimately, widespread adoption will require research into application-specific benefits, hybrid quantum-classical solutions, and robust metrics to quantify and certify the measurement improvements enabled by quantum communication.

V. CONCLUSION

Quantum communication already can deliver concrete benefits: QKD and QSDC provide provably secure data channels that reinforce traceability; entanglement-based sensing demonstrably surpasses classical signal-to-noise ratios by double-digit decibels; and QCS realises picosecond-accurate timing links that eclipse GPS-class solutions. Yet these gains remain confined to point-to-point or few-node testbeds. The path to widespread adoption hinges on three advances: (i) scalable, resource-efficient entanglement distribution via quantum repeaters and multiplexed network protocols; (ii) seamless hybridisation with classical digital network and timing infrastructure, backed by emerging standards such as ISO/IEC 23837-1; and (iii) robust, SI-traceable calibration methods for single-photon sources, detectors, and quantum timing links. Addressing these challenges will enable an "internet of quantum sensors" in which security, synchronization, and sensitivity are elevated simultaneously, catalysing next-generation measurement capabilities across power grids, telecommunications, fundamental physics, and beyond.

REFERENCES

[1] M. T. Rahim, A. Khan, U. Khalid, J. u. Rehman, H. Jung, and H. Shin, "Quantum secure metrology for network sensing-based applications," *Scientific Reports*, vol. 13, no. 1, p. 11630, 2023.

[2] B.-Y. Tang, M. Tian, H. Chen, H. Han, H. Zhou, S.-C. Li, B. Xu, R.-F. Dong, B. Liu, and W.-R. Yu, "Demonstration of 75 km-fiber quantum clock synchronization in quantum entanglement distribution network," *EPJ Quantum Technology*, vol. 10, no. 1, pp. 1–10, 2023.

[3] A. Menditto, M. Patriarca, and B. Magnusson, "Understanding the meaning of accuracy, trueness and precision," *Accreditation and quality assurance*, vol. 12, pp. 45–47, 2007.

[4] D. Matsakis, J. Levine, and M. Lombardi, "Metrological and legal traceability of time signals," in *"Proceedings of the 49th annual precise time and time interval systems and applications meeting"*, pp. 59–71, 2018.

[5] W. Yan, X. Zheng, W. Wen, L. Lu, Y. Du, Y.-Q. Lu, S. Zhu, and X.-S. Ma, "A measurement-device-independent quantum key distribution network using optical frequency comb," *npj Quantum Information*, vol. 11, no. 1, p. 97, 2025.

[6] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of modern physics*, vol. 92, no. 2, p. 025002, 2020.

[7] A. Meda, A. Mura, S. Virzì, A. Avella, F. Levi, I. P. Degiovanni, A. Geraldi, M. Valeri, S. Di Bartolo, T. Catuogno, *et al.*, "Qkd protected fiber-based infrastructure for time dissemination," *Scientific Reports*, vol. 15, no. 1, p. 13419, 2025.

[8] H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, and J. Lu, "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," *Light: Science & Applications*, vol. 11, no. 1, p. 83, 2022.

[9] B. K. Malia, Y. Wu, J. Martínez-Rincón, and M. A. Kasevich, "Distributed quantum sensing with mode-entangled spin-squeezed atomic states," *Nature*, vol. 612, no. 7941, pp. 661–665, 2022.

[10] S.-R. Zhao, Y.-Z. Zhang, W.-Z. Liu, J.-Y. Guan, W. Zhang, C.-L. Li, B. Bai, M.-H. Li, Y. Liu, L. You, *et al.*, "Field demonstration of distributed quantum sensing without post-selection," *Physical Review X*, vol. 11, no. 3, p. 031009, 2021.

[11] Z. Zhang and Q. Zhuang, "Distributed quantum sensing," *Quantum Science and Technology*, vol. 6, no. 4, p. 043001, 2021.

[12] J. Shi and S. Shen, "A clock synchronization method based on quantum entanglement," *Scientific Reports*, vol. 12, no. 1, p. 10185, 2022.

[13] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, 2017.

[14] S. Shen, C. Yuan, Z. Zhang, H. Yu, R. Zhang, C. Yang, H. Li, Z. Wang, Y. Wang, G. Deng, *et al.*, "Hertz-rate metropolitan quantum teleportation," *Light: Science & Applications*, vol. 12, no. 1, p. 115, 2023.

[15] S. Welte, P. Thomas, L. Hartung, S. Daiss, S. Langenfeld, O. Morin, G. Rempe, and E. Distante, "A nondestructive bell-state measurement on two distant atomic qubits," *Nature Photonics*, vol. 15, no. 7, pp. 504–509, 2021.

[16] S. W. Moore and J. A. Dunningham, "Secure quantum-enhanced measurements on a network of sensors," *Physical Review A*, vol. 111, no. 1, p. 012616, 2025.

[17] M. Alshowkan, P. G. Evans, M. Starke, D. Earl, and N. A. Peters, "Authentication of smart grid communications using quantum key distribution," *Scientific Reports*, vol. 12, no. 1, p. 12731, 2022.

[18] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light: Science & Applications*, vol. 10, no. 1, p. 183, 2021.

[19] C. G. Song and Q. Y. Cai, "Excessive precision compromises accuracy even with unlimited resources due to the trade-off in quantum metrology," *npj Quantum Inf*, vol. 11, p. 115, July 2025.

[20] K. Azuma, S. E. Economou, D. Elkouss, and Others, "Quantum repeaters: From quantum networks to the quantum internet," *Reviews of Modern Physics*, vol. 95, p. 045006, Dec 2023.

[21] "Information security — security requirements, test and evaluation methods for quantum key distribution — part 1: Requirements," International Standard ISO/IEC 23837-1:2023(E), International Organization for Standardization and International Electrotechnical Commission, Aug 2023.

[22] J. C. Bienfang, T. Gerrits, P. S. Kuo, A. Migdall, S. Polyakov, and O. Slattery, "Single-photon sources and detectors dictionary," NIST Interagency/Internal Report NIST IR 8486, National Institute of Standards and Technology, Gaithersburg, MD, Sep 2023.