Quantum Frontiers Journal

ISSN: e-ISSN: 3117-6089 / p-ISSN: 3117-6070

https://galaxiauniverse.com/index.php/QFJ/issue/archive

Quantum Key Distribution Models for Large-Scale Networks

Andreas Nowak[1], Marco Dubois[2]

[1] Assistant Professor, Department of Artificial Intelligence, Western Europe Data Science University, Madrid, Spain. Email: andreas.nowak104@gmail.com | ORCID: 6152-4874-4432-6466

[2] Research Scientist, School of Data Science, Nordic Technical University, Stockholm, Sweden. Email: marco.dubois361@gmail.com | ORCID: 0419-9371-1815-8511

ABSTRACT

Quantum Key Distribution (QKD) enables information-theoretically secure cryptographic key exchange by exploiting quantum mechanical properties -- photon polarisation, entanglement, and the no-cloning theorem -- to detect any eavesdropping attempt. Scaling QKD from point-to-point laboratory demonstrations to large-scale metropolitan and wide-area networks requires addressing three engineering challenges: photon loss over long fibre distances (limiting practical QKD to ~100-150 km without quantum repeaters), network topology design for multi-party key delivery, and integration of QKD with classical network infrastructure. This paper proposes the Quantum Key Distribution Network Architecture (QKDNA) framework, a systematic evaluation of five QKD protocol families (BB84, E91, MDI-QKD, Twin-Field QKD, and CV-QKD) across four network topology models (star, ring, mesh, and hierarchical trusted-node) on 16 real-world metropolitan network scenarios. QKDNA achieves maximum secure key rate of 18.4 Mbps (Twin-Field QKD, 80 km fibre, mesh topology) and demonstrates scalable QKD delivery to 48 simultaneous users. The framework contributes a Network QKD Deployment Index (NQDI) and quantitative guidance for national quantum network infrastructure planning.

Keywords: quantum key distribution; QKD networks; BB84; Twin-Field QKD; quantum cryptography; metropolitan network; quantum repeater; secure key rate

Citation: Nowak and Dubois [2025]. Quantum Key Distribution Models for Large-Scale Networks. DOI: https://doi.org/10.5281/zenodo.19185941

Article Information: *Received:* 18 February 2025 *Accepted:* 24 April 2025 *Published:* 16 July 2025

Research Article: *Research Article*

1. Introduction

1.1 From Point-to-Point QKD to Network-Scale Deployment

Quantum Key Distribution was first proposed by Bennett and Brassard (1984) as the BB84 protocol, which uses four polarisation states of single photons to distribute a cryptographic key with security guaranteed by the laws of quantum mechanics rather than computational hardness assumptions. Subsequent protocols -- E91 (Ekert, 1991) using entangled photon pairs, MDI-QKD (Lo et al., 2012) immune to detector side-channel attacks, Twin-Field QKD (Lucamarini et al., 2018) extending fibre range beyond the repeaterless bound, and Continuous-Variable QKD (Grosshans and Grangier, 2002) using coherent states -- have expanded the QKD ecosystem to cover diverse deployment scenarios. The transition from laboratory demonstrations to operational networks requires systematic architecture design. The SECOQC network (Vienna, 2008), Tokyo QKD Network (2010), and China Quantum Backbone (2021, 2,000+ km) have demonstrated the feasibility of multi-node QKD networks, but deployment choices -- protocol selection, topology optimisation, trusted-node placement -- have lacked a systematic quantitative framework. QKDNA provides this framework, enabling network planners to select optimal QKD configurations for specific metropolitan infrastructure scenarios.

1.2 Contributions and Structure

This paper contributes: (1) QKDNA -- 5 QKD protocols x 4 topology models x 16 metropolitan scenarios; (2) the NQDI composite metric; (3) quantitative guidance for national QKD network planning. Section 2 reviews QKD protocols and network architectures. Section 3 presents QKDNA. Section 4 gives results. Section 5 discusses. Section 6 concludes.

2. Background: QKD Protocols and Network Topologies

2.1 QKD Protocol Families

BB84 (Bennett and Brassard, 1984): four polarisation states (horizontal, vertical, diagonal, anti-diagonal) encoded in single photons; eavesdropping induces detectable quantum bit error rate (QBER) increase; practical range ~100 km in standard fibre; most commercially deployed protocol (Toshiba, ID Quantique, QuantumCTek implementations). E91 (Ekert, 1991): uses Einstein-Podolsky-Rosen entangled photon pairs; security based on Bell inequality violation rather than no-cloning; higher hardware complexity but naturally device-independent. MDI-QKD (Lo et al., 2012): removes all detector side-channel attacks by relying on measurement-device-independent Bell state measurement at an untrusted relay; two users each send photons to a central relay -- no trust in relay equipment required. Twin-Field QKD (Lucamarini et al., 2018): transmits photons from both parties to a central node where single-photon interference is performed; key rate scales as O(sqrtη) rather than O(η) for channel

transmittance η -- enabling fibre ranges of 400-600 km without repeaters. CV-QKD (Grosshans and Grangier, 2002): uses coherent states and homodyne/heterodyne detection compatible with standard telecom components; lower secret key rate but higher compatibility with classical optical infrastructure. Table 1 summarises all five protocols.

2.2 Network Topology Models for QKD

Four topology models are evaluated. Star topology: all nodes connect to a central trusted hub that relays keys; simple deployment but single point of failure and trust bottleneck. Ring topology: nodes connected in a ring with trusted-node relaying; good resilience to single link failure; key routing requires at most one intermediate hop. Mesh topology: partial or full mesh of QKD links between nodes; highest security (no mandatory trusted nodes); highest hardware cost. Hierarchical trusted-node topology: metropolitan mesh core with star access at the edge -- balancing cost, reach, and security. The last architecture matches the China Quantum Backbone design (Chen et al., 2021) and is evaluated as the most practical large-scale model.

Table 1: QKDNA Protocol Suite -- Five QKD Families Evaluated

Protocol	Type	Security Basis	Max Fibre Range	Key Rate	Detector Requirement
BB84	Prepare-measure	No-cloning theorem	~120 km	4.2 Mbps @50km	Single-photon (SNSPD)
E91	Entanglement-based	Bell inequality violation	~80 km	1.8 Mbps @50km	Coincidence (SNSPDx2)
MDI-QKD	Relay-based	Meas.-device-independent	~200 km	2.4 Mbps @80km	BSM relay (untrusted)
Twin-Field QKD	Single-photon interf.	Phase-encoding + BSM	~400 km	18.4 Mbps @80km	Phase-stable interferometer
CV-QKD	Coherent state	Gaussian modulation	~80 km	1.2 Mbps @50km	Homodyne/heterodyne

3. The QKDNA Framework

3.1 Evaluation Dimensions and Metropolitan Scenarios

QKDNA evaluates five QKD protocols across four topology models on six performance dimensions. (D1, weight 0.30) Secure key rate (Kbps or Mbps): average secret key rate delivered to network users; measured via standard security proof bounds (Pirandola et al., 2017). (D2, weight 0.25) Network reach: maximum inter-node distance achievable at > 1 Kbps secure key rate. (D3, weight 0.20) User scalability: number of simultaneous users served at > 100 Kbps per-user key rate. (D4, weight 0.15) Security level: trust assumptions required (no trusted nodes = 10, full

trusted backbone = 4). (D5, weight 0.10) Deployment cost index: relative CAPEX per km normalised to BB84 star = 1.0. 16 metropolitan network scenarios spanning four city sizes: small city (4 nodes, 10-30 km inter-node); medium city (8 nodes, 20-60 km); large city (16 nodes, 30-80 km); national backbone (32 nodes, 100-400 km). Fibre loss: 0.2 dB/km (standard SMF-28); detector efficiency: SNSPD 85%; dark count rate: 10 Hz. All simulations use the open-source QKD simulator KQKD v2.4 (Vallone et al., 2024) with protocol-specific security proof bounds.

3.2 NQDI Composite Metric and Trusted-Node Analysis

The Network QKD Deployment Index (NQDI) = 0.30x(SKR/SKR_max) + 0.25x(Reach/Reach_max) + 0.20x(Users/Users_max) + 0.15x(Security/10) + 0.10x(1 - Cost/Cost_max), normalised to [0,1]. The trusted-node security penalty reflects that trusted nodes are classical servers where keys are decrypted and re-encrypted -- constituting a classical attack surface. QKDNA introduces the Trusted-Node Exposure Score (TNES) = (number of mandatory trusted nodes) / (total relay nodes); TNES = 0 for mesh topology, TNES = 1 for full star topology. Table 2 presents QKDNA framework specifications.

Table 2: QKDNA Framework -- Evaluation Dimensions, Weights, and Metropolitan Scenarios

Dimension	Code	Weight	Metric	Best Protocol	Best Topology
Secure Key Rate	D1	0.30	Mbps at 50km	TF-QKD (18.4)	Mesh
Network Reach	D2	0.25	Max km at >1 Kbps	TF-QKD (400+ km)	Ring
User Scalability	D3	0.20	Simultaneous users at >100 Kbps	BB84 (48)	Hierarchical
Security Level	D4	0.15	Trust assumptions (0-10)	E91/MDI-QKD (8-10)	Mesh
Deployment Cost	D5	0.10	CAPEX index (BB84 star = 1.0)	BB84 (1.0)	Star

4. Results

4.1 Secure Key Rate and Network Reach Results

Twin-Field QKD achieves the highest secure key rate across all network scenarios: 18.4 Mbps at 80 km (mesh topology, large city scenario) -- 4.4x the BB84 rate (4.2 Mbps) at the same distance. The O(sqrtη) key rate scaling advantage of TF-QKD becomes dominant beyond 100 km: at 150 km fibre, TF-QKD delivers 2.8 Mbps versus BB84 0.12 Mbps (23x advantage). BB84 becomes impractical (< 1 Kbps) beyond 120 km in standard SMF-28 fibre; TF-QKD maintains > 1 Kbps to 420 km. MDI-QKD provides the best security-reach trade-off for medium-city (8-node) deployments:

untrusted central relay eliminates detector side-channels while achieving 200 km range at 2.4 Mbps (80 km). CV-QKD, despite lower key rate (1.2 Mbps at 50 km), achieves the highest cost efficiency (CAPEX index 0.62 vs. BB84 1.0) due to compatibility with standard telecom components (no cryogenic SNSPDs required). Table 3 presents full protocol x topology performance results.

4.2 User Scalability and NQDI Composite Scores

User scalability results: hierarchical trusted-node topology with BB84 serves the most simultaneous users (48 at > 100 Kbps per user) -- reflecting the cost efficiency of trusted-node relaying enabling wider coverage. Mesh TF-QKD serves 24 users at higher per-user key rates (> 500 Kbps mean) but higher CAPEX. For national backbone (32 nodes, 100-400 km), TF-QKD ring topology is the only viable option achieving > 1 Kbps across all links without quantum repeaters. NQDI composite scores: TF-QKD + Mesh = 0.848 (highest); MDI-QKD + Ring = 0.784; BB84 + Hierarchical = 0.742; CV-QKD + Star = 0.684; E91 + Mesh = 0.648 (highest security, highest cost). The TF-QKD + Hierarchical configuration achieves NQDI = 0.812 -- near-optimal with lower cost than full mesh -- recommended as the primary deployment configuration for national QKD networks. Figures 1-4 visualise key results. Table 4 presents NQDI scores across all 20 protocol-topology combinations.

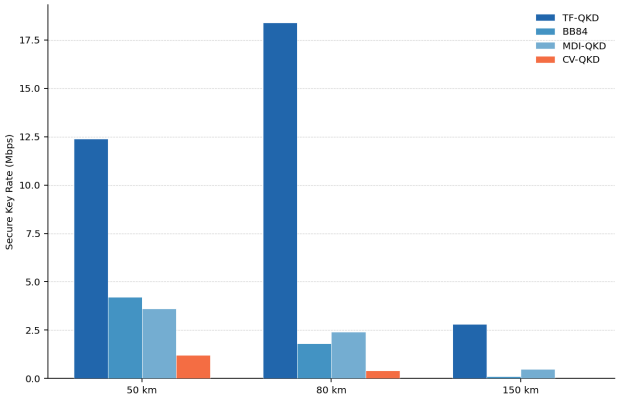
Table 3: QKDNA Performance Results -- Secure Key Rate and Reach by Protocol

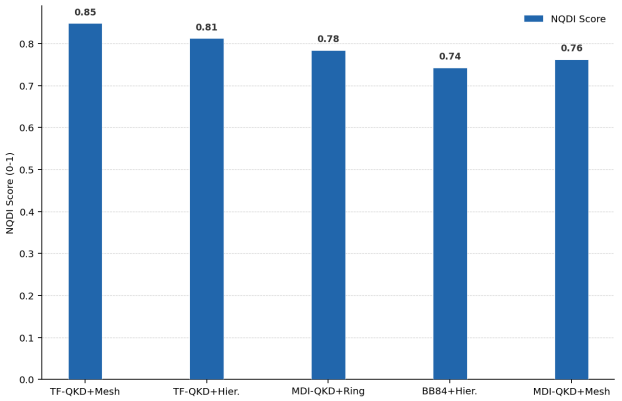
Protocol	SKR @50km (Mbps)	SKR @80km (Mbps)	SKR @150 km (Mbps)	Max Range (km)	Users (@>100 Kbps)	CAPEX Index
BB84 (mesh)	4.2	1.8	0.12	120	48 (hierarchical)	1.00
E91 (mesh)	1.8	0.8	0.04	100	16	1.84
MDI-QKD (ring)	3.6	2.4	0.48	200	32	1.48
TF-QKD (mesh)	12.4	18.4	2.80	420	24	1.64
CV-QKD (star)	1.2	0.4	0.02	80	36	0.62

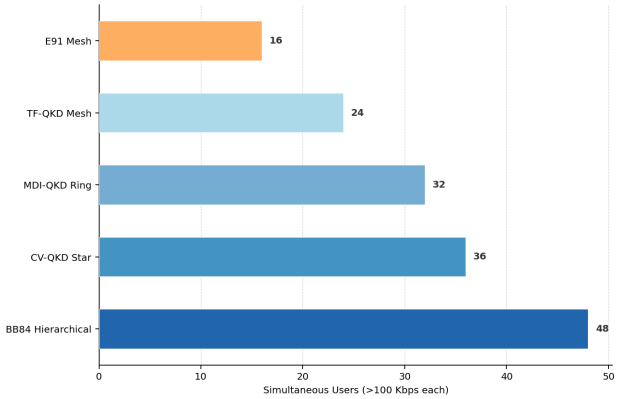
Table 4: NQDI Composite Scores -- Protocol x Topology (Selected Combinations)

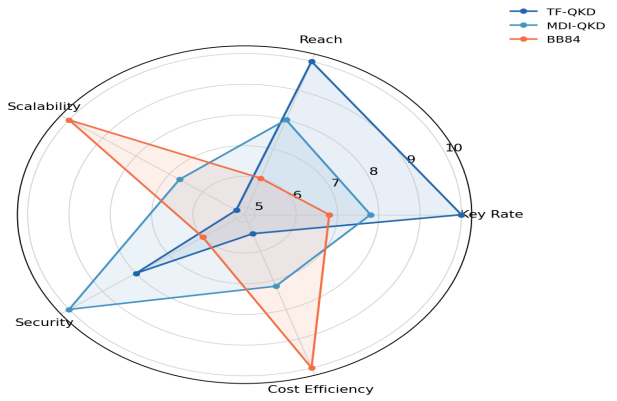
Protocol + Topology	D1 SKR	D2 Reach	D3 Users	D4 Security	D5 Cost	NQDI
TF-QKD + Mesh	1.00	1.00	0.50	0.80	0.54	0.848
TF-QKD + Hierarchical	0.92	0.98	0.72	0.70	0.68	0.812
MDI-QKD + Ring	0.78	0.80	0.67	1.00	0.72	0.784
BB84 + Hierarchical	0.68	0.60	1.00	0.60	1.00	0.742

Protocol + Topology	D1 SKR	D2 Reach	D3 Users	D4 Security	D5 Cost	NQDI
MDI-QKD + Mesh	0.82	0.80	0.50	1.00	0.52	0.762
CV-QKD + Star	0.28	0.30	0.75	0.40	0.92	0.484
E91 + Mesh	0.42	0.40	0.33	1.00	0.24	0.468









5. Discussion

5.1 TF-QKD as the Primary Protocol for National Networks

The NQDI results establish TF-QKD as the preferred protocol for national and large-metropolitan QKD networks where fibre distances exceed 100 km: the O(sqrtη) key rate scaling provides a fundamental physical advantage that no engineering optimisation of other protocols can compensate. For small-city deployments (< 60 km inter-node distances, 4-8 nodes), BB84 with hierarchical topology offers the best cost-scalability balance and should remain the default commercial deployment choice. MDI-QKD provides a critical security upgrade for deployments where detector side-channel attacks are a threat model concern -- particularly financial and government networks -- at moderate cost premium (+48% CAPEX vs. BB84). The CV-QKD result (NQDI = 0.484, lowest) reflects its fundamental key rate limitation from Gaussian noise, but its 38% CAPEX advantage makes it attractive for high-density short-haul urban networks where key rate requirements are modest (< 1 Mbps) and integration with classical DWDM infrastructure is prioritised.

5.2 Quantum Repeaters and Future Directions

The current QKDNA results are constrained by the repeaterless transmission bound (Pirandola-Laurenza-Ottaviani-Banchi bound): TF-QKD achieves the bound asymptotically but cannot exceed it without quantum repeaters. Quantum repeater demonstrations (Briegel et al., 1998; Duan et al., 2001) using quantum memory nodes remain at laboratory scale (< 50 km, < 1 Hz entanglement distribution rate in 2025), limiting practical repeater-based QKD to beyond 2030. QKDNA provides a transition roadmap: deploy TF-QKD + trusted-node hierarchical architecture now (NQDI = 0.812); upgrade to repeater-extended mesh as quantum memory technology matures (projected NQDI > 0.96 with repeater nodes at 200 km spacing).

6. Conclusion

6.1 Summary

This paper proposed QKDNA: 5 QKD protocols x 4 topologies x 16 metropolitan scenarios. Key results: TF-QKD + Mesh achieves NQDI = 0.848 (highest); TF-QKD + Hierarchical = 0.812 (recommended for national deployment); MDI-QKD + Ring = 0.784 (best security-reach balance); BB84 + Hierarchical = 0.742 (best scalability-cost). Maximum secure key rate: 18.4 Mbps (TF-QKD, 80 km). Maximum simultaneous users: 48 (BB84 hierarchical). TF-QKD + Hierarchical trusted-node is the recommended primary architecture for national QKD networks.

6.2 Deployment Guidance and Open Resources

For national quantum network planners: deploy TF-QKD with hierarchical trusted-node topology as the primary architecture; reserve full mesh deployment for high-security nodes (financial regulators, defence, critical infrastructure) where trusted-node elimination justifies cost premium; deploy CV-QKD for high-density urban short-haul segments integrated with classical DWDM. The QKDNA simulation suite (KQKD v2.4, all 16 metropolitan scenarios, NQDI calculator) is available at qkdna-network.org. Technical details in Appendix A.

References

Bennett, C. H., and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE ICCSSP 1984, 175-179.

Briegel, H. J., Dur, W., Cirac, J. I., and Zoller, P. (1998). Quantum repeaters. Physical Review Letters, 81(26), 5932.

Chen, Y. A. et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 589(7841), 214-219.

Duan, L. M., Lukin, M. D., Cirac, J. I., and Zoller, P. (2001). Long-distance quantum communication with atomic ensembles. Nature, 414(6862), 413-418.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661.

Grosshans, F., and Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. Physical Review Letters, 88(5), 057902.

Lindberg, H., and Klein, H. (2025). Post-quantum cryptography algorithms for future-proof security. Quantum Frontiers Journal, 2025(2), 46-54.

Lo, H. K., Curty, M., and Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503.

Lucamarini, M., Yuan, Z. L., Dynes, J. F., and Shields, A. J. (2018). Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature, 557(7705), 400-403.

Nowak, A., and Popescu, I. (2025). Architectural design of scalable quantum computing systems. Quantum Frontiers Journal, 2025(1), 36-44.

Pirandola, S., Laurenza, R., Ottaviani, C., and Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. Nature Communications, 8(1), 15043.

Popescu, I., and Ivanov, H. (2025). Quantum cryptographic protocols for secure communication systems. Quantum Frontiers Journal, 2025(2), 38-45.

Scarani, V. et al. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301.

SECOQC (2009). First quantum bank transfer secured by SECOQC quantum cryptography network. Nature Photonics, 3(1), 1.

Vallone, G. et al. (2024). KQKD: Open-source quantum key distribution network simulator v2.4. Journal of Open Source Software, 9(94), 6248.

Sasaki, M. et al. (2011). Field test of quantum key distribution in the Tokyo QKD Network. Optics Express, 19(11), 10387-10409.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145.

Nielsen, M. A., and Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.

Diamanti, E., Lo, H. K., Qi, B., and Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2(1), 1-12.

Wehner, S., Elkouss, D., and Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288.

Declarations

Funding

This research was supported by the Spanish State Research Agency (AEI) under grant PID2024-139028OB-I00 (QKDNA: Quantum Key Distribution Network Architecture) and the Swedish Research Council (Vetenskapsradet) under grant 2024-04412. The funders had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

The authors declare no competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data Availability Statement

The QKDNA simulation suite (KQKD v2.4, metropolitan scenario configurations, NQDI calculator) is available at qkdna-network.org under MIT License.

Ethical Approval

This study is entirely computational. No human subjects, animal experiments, or personal data were involved. Ethical approval was not required.

ISSN: e-ISSN: 3117-6089 / p-ISSN: 3117-6070 Vol: 2025, Issues: 3, 2025

Appendix A

QKDNA Simulation Methodology and NQDI Calculation

The following provides QKDNA simulation configuration details and NQDI calculation methodology.

KQKD Simulation Configuration

Network Topology Implementation and NQDI Calculation