




ORIGINAL RESEARCH

Quantum Key Distribution for V2I communications with software-defined networking

Alexandros Stavdas¹ | Evangelos Kosmatos¹ | Carsten Maple² |
 Emilio Hugues-Salas³ | Gregory Epiphaniou² | Daniel S. Fowler²  |
 Shadi A. Razak⁴ | Chris Matrakidis¹  | Hu Yuan⁵  | Andrew Lord³

¹OpenLightComm Ltd., Ipswich, UK

²WMG, University of Warwick, Coventry, UK

³British Telecom (BT), Research & Network Strategy Applied Research, Ipswich, UK

⁴Angoka, The Innovation Centre, Belfast, UK

⁵Kingston University, London, UK

Correspondence

Chris Matrakidis.

Email: cmatraki@openlightcomm.uk

Funding information

Innovate UK, Grant/Award Number: 45364

Abstract

The evolution of Connected and Autonomous Vehicles (CAVs) promises improvements in our travel experience and the potential to enhance road safety and reduce environmental impact. This will be utilising highly diverse traffic environments that enable several advanced mobility applications. A secure, efficient, reliable, and resilient communications infrastructure is required to support developments in these CAV systems. Next generation of telecommunication networks will seamlessly integrate terrestrial, satellite, and airborne networks into a single wireless system satisfying the requirements of trustworthy future transport systems. Given the increasing importance of CAVs, coupled with their attractiveness as a cyber-attack for threat agents (e.g., disruption of transportation systems by nation states), security is paramount. Future communications systems offer an opportunity to integrate Quantum Key Distribution (QKD) into vehicular environments, protecting against advances in quantum computation that render many of the classical algorithms that underpin Public Key Infrastructure obsolete. This paper proposes a method for the integration of QKD in V2I networks to enable secure data communication. Quantum Key Distribution is used in the end-to-end path of vehicle-to-infrastructure (V2I) networks. Furthermore, an overarching Software-Defined Network, with integrated QKD, is introduced. We have investigated the security performance of QKD in a V2I network over an urban environment.

KEYWORDS

cryptography protocols, public key cryptography, telecommunication security

1 | INTRODUCTION

The increasing commercialisation of quantum-derived technologies will see a future transition period. Quantum technology-based solutions will work alongside existing technologies or replace subsystems within current complex super systems. This commercialisation period was one of the reasons for the multi-partner, Innovate UK-funded, AirQKD project. The AirQKD project aims to strengthen the UK quantum-related expertise and capabilities, from quantum components to used cases [1]. The AirQKD project exploits a Free Space

Optical (FSO) Quantum Key Distribution (QKD) system, related control systems, and key management software, amongst other project successes. The project includes targeted used cases in telecommunications and V2I communications. In this project work, we examined how an FSO-QKD system forms part of a future urban V2I communications network located within a city infrastructure, that is, the role quantum-based technologies can play in V2I network links.

The rest of this paper is organised as follows: in Section 2, a background to V2I communications is provided; in Section 3, we identify the quantum technologies suitable for V2I

This is an open access article under the terms of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2023 The Authors. *IET Quantum Communication* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

communications; in Section 4, we detail the architectural steps for convergence between V2I and quantum networks with emphasis given on the necessary processes for security between building-to-building Base Stations (BS); Section 6 presents a standards compliant Software-Defined Network (SDN) overarching platform and key management for quantum secured V2I communications; finally, the conclusions from the work are provided.

2 | BACKGROUND TO VEHICULAR COMMUNICATIONS

The Vehicle-to-Everything (V2X) communications paradigm enables a variety of applications to enhance road safety, driving efficiency, and passenger infotainment. It offers the potential to radically change how we commute, the building of our cities, and how we live within them [2]. However, V2X has a diverse set of performance requirements in terms of latency, reliability, and data rates [3]. If these requirements are not met, safety-critical applications may fail to respond in potentially dangerous situations, jeopardising confidence and public trust in the application of V2X systems.

Dedicated Short-Range Communications (DSRC) solutions have been deployed for information exchange in the last drop between the network infrastructure and vehicles, the Vehicle-to-Infrastructure (V2I) element of V2X, in the quest for a robust and reliable communications infrastructure. A set of services and interfaces of V2X communications is defined by the IEEE 802.11p and IEEE 1609 standards for Wireless Access for Vehicular Environment. IEEE 802.11bd is the Next-Generation V2X (NGV) standard based on proven Wireless Local-Area Network technologies. Under these models, information exchange is made without a Basic Service Set, as is required in the traditional 802.11 standards. However, it has been recognised that DSRC suffers from significant drawbacks in dense and high-mobility environments because of limited coverage, low data rate, limited quality-of-service (QoS) guarantees, and unbounded channel access delay [4].

While the DSRC model has been used as a V2X communication model for a long time, it is being challenged by the emerging Cellular Vehicle-to-Everything (C-V2X). The third Generation Partnership Project (3GPP) initiative, in its release 14 specification, enhanced the cellular Long-Term Evolution standard for V2X services, that is, C-V2X [5]. Cellular communications are argued to provide broader coverage, support high mobility and density users, and lower latency. Release 14 is mainly focused on the delivery service of data related to road safety, such as Cooperative Awareness Messages, Basic Safety Messages, and Decentralised Environmental Notification Messages. In 2019, 3GPP introduced the release 15 specification of 5G New Radio (5G NR) C-V2X to support advanced V2X services such as vehicle platooning, advanced driver assistance, remote driving, and extended sensors [6].

The passing of the release 15 standards milestone allows organisations to capitalise on those standards as a base

platform for upcoming 6G Vehicle-to-Infrastructure (6G-V2I) systems. This is a convergence of fixed and mobile data transportation, integrating with a range of newer technologies, featuring versatile and efficient air interfaces and advanced resource allocation, decision-making, and computing schemes [7]. Whilst the constitution and meaning of 6G do vary [8], for example, it can be terahertz frequencies, photonics technologies, and even along the line of edge/fog computing (where computation is distributed throughout the system or at its periphery) and deployed Machine Learning techniques that will further enhance the efficiency of V2X communication units to achieve faster computation and better decisions. 6G could also be referred to the use of new photonics and quantum-based technologies to address future V2I challenges.

One key consideration that has not been sufficiently addressed in V2X communications is related to security in the context of a ubiquitous fixed wireless converged infrastructure [9]. For example, a malicious user may broadcast non-legitimate messages to other road users to disrupt the V2X communication system or obtain unauthorised private information of other road users. Public Key Infrastructure aims to ensure a trustworthy communication between entities in a V2X system. Yet, the implementation of Public Key Infrastructure can have a significant impact on the performance of this safety-critical infrastructure. For example, distributing and utilising data encryption keys may introduce latency issues. Latency is a particular concern for safety-related applications [10].

3 | THE PROSPECT OF QUANTUM TECHNOLOGIES FOR V2I

In the framework of V2I, quantum technologies are seen as a candidate to provide advanced security features readily integrated into communications infrastructure. Quantum technologies provide the means for inherent security as they cannot be cloned or accessed without tampering [11]. Depending upon how a quantum feature is used, several new quantum-based security technologies have emerged, leading towards QKD standardisation [12]. Some prominent quantum security application includes 'Mobile Secret Communications using QKD Network' [13], 'Secure Multi-Party Communication with QKD' [14], 'Method of Integrating QKD and IPsec' [15], and 'IPsec VPN Cipher Machines based on QKD' [16].

Another prominent example is a previous example developed by ANGOKA (one of the authors) regarding quantum-safe Device Identity and Authentication Units (DAU) and Device Private Networks (DPN) [17]. The highlighted technology comprises a method for secure symmetric key and Identity generation, authentication and secure communication between the plurality of entities in a network named Zero Trust Authentication Protocol (ZAP).

The DAU establishes an immutable root of trust and a cryptographic identity derived from the device hardware, software, and system configuration. While the DPN utilises zero-knowledge proof principles and distributed ledgers to

decentralise the identity and key management among a plurality of entities and establish secure communication channels by micro-segmenting the network infrastructure, and traditional communication channels.

DPNs and DAUs in conjunction with ZAP offer an opportunity to enhance and provide different grades of quantum-based security in V2I and other communication systems, see Figure 1.

Quantum Key Distribution supports information-theoretic security since the symmetric key distribution provided to the users is independent of the attacker's computational power. The eavesdropper is not working against the limits of computational assumptions or complex mathematical problems and models but is restricted by the laws of physics. The QKD system can secure V2I communications by detecting any malicious eavesdropping attempt, since a significant number of errors in the key data will occur whenever the eavesdropper (*Eve*) interferes with (listens to) the distribution of symmetric keys between the sender (*Alice*) and the receiver (*Bob*). This allows the detection of eavesdropping and results in a key being rejected, protecting the secrecy of any key that is agreed upon.

Among the candidate QKD technologies, Free-Space Optical (FSO) technologies have the potential to deliver high-grade, high-performance, and efficient security thanks to their high throughput data links, high-beam directivity, and energy efficiency. The potential of an FSO-based QKD system has attracted significant attention recently [18] thanks to the strict line-of-sight (LoS) and the enhanced spatial and temporal security of this technology that is leveraged to further limit *Eve's* capability to access the main channel. Most of the proposed hybrid schemes assume maximum transmission efficiency while *Eve* maintains physically bounded access to the channel (the wiretap model). These schemes offer the potential to enhance data transfers and layered cryptographic solutions for different applications, utilising quantum-safe technologies, and classical encryption [19].

When a system or its elements are not suitable for an optical QKD link, as with highly mobile vehicles, an alternative quantum-based device can be utilised, like the DAU. The AirQKD approach is to support the provisioning of secure key generation and authentication with a ZAP. The protocol utilises a hardware root of trust, such as a post-quantum secure Physical Unclonable Function (PUF) and other immutable system software and hardware characteristics to derive unique quantum-safe keys and identities [17]. DAUs are the realisation of ZAP in action, whereas DPNs are the microsegmentation of the DAUs-based network. In addition, the same hardware root of trust is used for a key amplification process that supports the QKD system.

4 | A CONVERGED FIXED-WIRELESS CONNECTIVITY PLATFORM FOR V2I

The converged connectivity infrastructure layout for AirQKD is schematically illustrated in Figures 2 and 3. The data network consists of BSs, located on the rooftops of buildings (points *E*

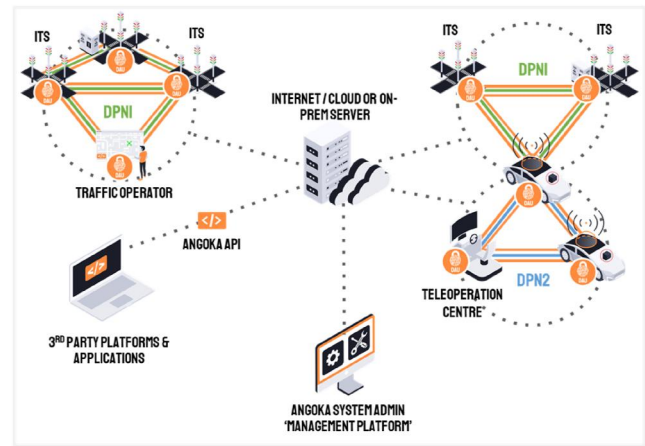


FIGURE 1 Device private networks secured with Zero Trust protocols are an alternative to certificate-based security.

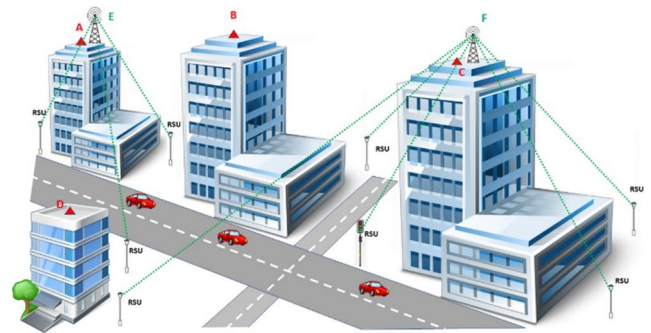


FIGURE 2 Physical Unclonable Function (PUF) secured connectivity between Road-Side Units (RSUs) and antenna (green dotted lines).

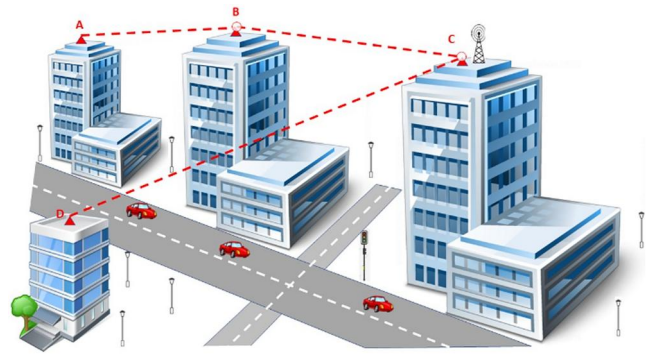


FIGURE 3 Free Space Optical (FSO) links for Quantum Key Distribution (QKD) key-relay between buildings (red broken lines).

and *F* in Figure 2), and Road-Side Units (RSUs) at the local vicinity of the corresponding BSs. The BSs are the Access Points that connect to the higher layer x-haul network for the backend infrastructure (not shown). Meanwhile, the RSUs are the APs for the vehicles. The RSUs are mounted to the existing street furniture, such as lampposts and traffic lights. Connectivity between the RSUs and the BSs is shown with green colour broken lines in Figure 2. Moreover, each vehicle is

equipped with an On-Board Unit (OBU) to exchange data with one or more RSUs as well as with other vehicles.

For the secured V2I communications, the converged connectivity platform consists of the following secured two-way communication paths:

1. To/from the vehicular OBUs and to/from the RSUs then to/from the BSs.
2. For the horizontal handover of data [20, 21] the path is to/from A , which is co-located with the BS at E , to/from the BS at C , which is co-located with the BS at F (see Figures 2 and 3). When establishing communications, the quantum key is relayed from A to B and from B to C .
3. For the onward vertical handover (not shown in Figure 2 or Figure 3), it is to/from a BSs and to/from an Edge Node (EN) on the infrastructure x-haul.

In AirQKD, we create a secure V2I communications infrastructure that results from combining cases 1 and 2. In case 1, data and keys follow the same physical path. The secure transportation of a key between a BS at a rooftop (points E and F in Figure 2) and the RSUs is made by means of a DAU, which is a semi-classical gateway that uses its hardware root of trust, such as the PUF to implement the ZAP [17]. A similar device is also used to facilitate the last drop from an RSU to the OBU, that is, to secure the vehicle link. The DAU supports, amongst others, the following functions:

- Identification (ID) generation
- Unit authentication
- Message authentication
- Message encryption

The associated processes for communication path 1 are shown in Figure 4. In the downstream direction, from the rooftop to the vehicle, the following takes place. A Data Application, requiring cryptographic security, instantiates to a server collocated with the BS and generates a session. The application calls the Application Programming Interface (API) of the BS DAU node (DAU-N), see Figure 4. DAU-N supports secure protocol connectivity within the network infrastructure based on ZAP. Zero Trust Authentication Protocol ensures security by providing enterprise-grade encryption mechanism to safeguard message integrity, authenticity, and confidentiality. The API passes a message to DAU, the DAU encrypts the message with a “fingerprint” of the BS and then, the message is sent over the data link. The RSU receives the encrypted message and passes it to the RSU’s DAU-N. The DAU-N decrypts the message and authenticates it using the fingerprint of the BS and passes it on to the DAU that supports the last drop to the vehicle (designated as DAU-V in Figure 4). The message is sent to the vehicle via the wireless link and, through another DAU-V and the corresponding API, the message reaches the application layer at the vehicle.

Ahead of transmitting the encrypted messages between DAU-N and DAU-V, the next phase in ZAP is to establish a secure communication tunnel within the communication

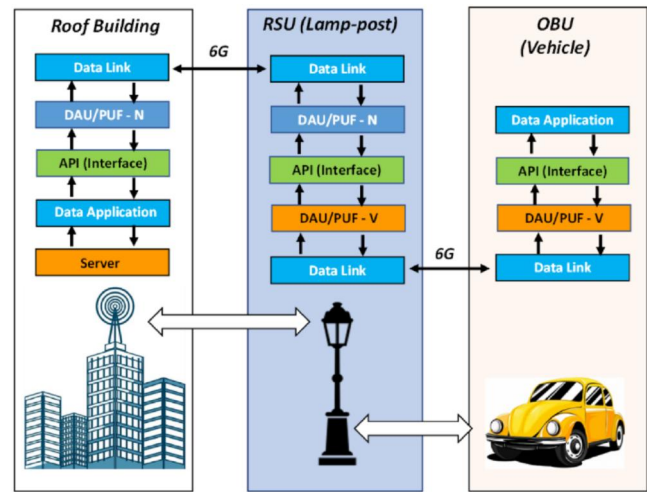


FIGURE 4 Processes and functions for secure message exchanges between rooftop Base Stations (BS) and vehicles based on Physical Unclonable Functions (PUFs).

channel known as DPN. The DPN is a security mesh architecture that allows DAUs to microsegment the system communication and create a mesh network of secure peer-to-peer communication networks among the DAUs. A DPN identity and session key is negotiated and derived from the DAUs' unique identities and keys. Subsequently, the DPN provides an additional security layer that safeguards and utilises the last-mile delivery of keys without exposing or using the distributed key.

To secure the horizontal handover of data between adjacent BSs, the quantum key relay scheme of Figure 3 is implemented, and data may follow a different path via the x-haul node for EN processing or further on to an Intelligent Transportation System control room. Bridging the geographically close buildings is by means of FSO-QKD point-to-point connections between rooftops. The generation of a quantum-derived key is implemented by exploiting BB84-based protocols [12].

However, FSO connections are prone to LoS limitations. Their performance is restricted by impairments related to free-space (atmospheric) propagation, for example, diffraction and scattering losses, stray light, and atmospheric turbulence. In addition, unwanted dark counts at the receiver detector limit the distance and the key rate achievable. Further, the Shannon capacity links the FSO reach, via the attainable Signal-to-Noise Ratio (SNR) and the Quantum Key Generation Rate (QKGR). The QKGR could be anything between 30 s and 24 h. Considering the AirQKD parameters the FSO distance target for the AirQKD project is in the order of 150–300m.

The high-level processes for secure data exchange using FSO point-to-point connections are schematically illustrated in Figure 5. An application that is hosted in servers (on-site or remotely) encrypts a “message” via a classic protocol, for example, Advanced Encryption Standard, and it requests a quantum key to secure this encryption. A quantum key is generated via the FSO link by means of the BB84 QKD

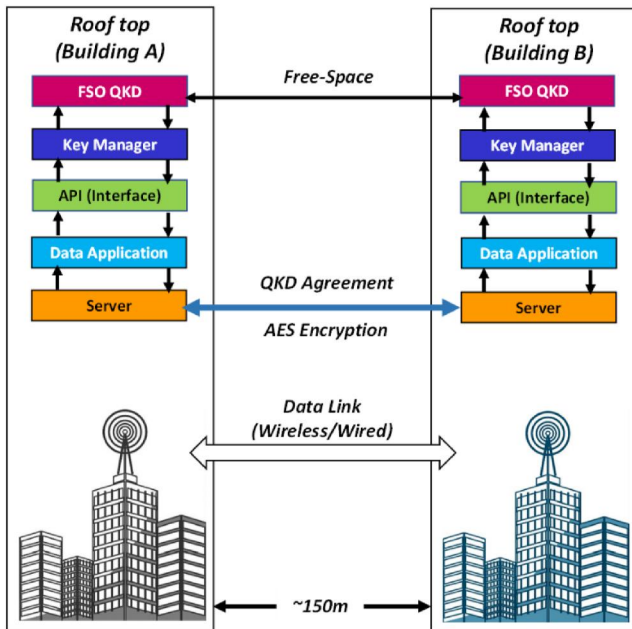


FIGURE 5 Processes and functions for secure message exchanges between rooftops based on FSO-QKD technology.

protocol. The quantum keys are agreed upon and processed by the Key Manager. These keys are used to secure the classic encryption and, hence, the messages exchanged between the two applications.

When the geographic distance is longer than the designated FSO-QKD reach, the secure relay is ensured by means of a daisy-chaining scheme [12] as in Figure 6. Therefore, for macro-cells located at $>300\text{m}$ apart, the quantum keys are relayed in a multi-hop fashion.

It is pointed out that in the most general case, the processes illustrated in Figures 4 and 5 are concurrently implemented for the secure handover of a session a vehicle has established when moving from the range of one BS at E to the range of the adjacent BS at F in Figure 2.

5 | FSO-QKD SECURITY ASPECTS

Shared secret generation using quantum mechanisms provides the appropriate security level for applications such as V2I. However, that entails that the FSO-QKD channel is always on and free from disturbances or errors in the quantum transmission line. Such errors can disrupt the distribution of the secret keys in certain parts of the environment and the key generation process overall [22]. To retain information-theoretic security, the QKD protocol invokes a Wegman–Carter message authentication code [23] with a pre-shared key that is transmitted at the end of the QKD protocol and authenticates messages up to that point. This reduces origin authentication to either Alice or Bob until both entities get hold of the secret key. This might also allow an adversary to obtain keys distributed using the same secret key used in

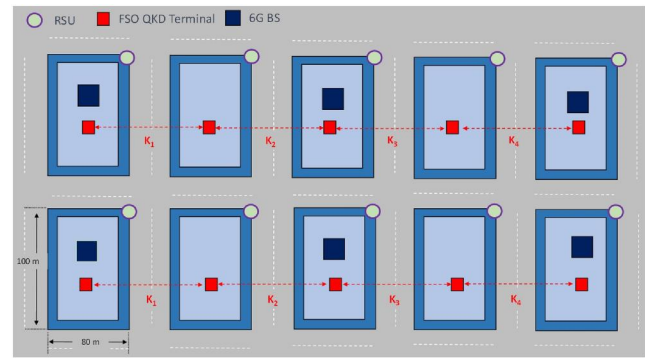


FIGURE 6 Key relay between rooftops using FSO-QKD links via “daisy-chaining”.

previous protocol rounds. Also, in standard BB84, classical information between Alice and Bob is communicated publicly after all bits have been exchanged. This can potentially yield information to Eve, reducing the protocol's resistance. The extent to which QKD channel disruption can contribute to man-in-the-middle (MITM) attacks of this nature is to be examined further.

With regards to key generation, preliminary QKD work over optical fibre in Ref. [24] shows that communication with illegitimate parties could be up to 10 min before detection for a single key generation round. For this case, the average time taken for a successful round of QKD with 10dB attenuation is approximately 20 min. If the QKD channel is down, this can lead to failed authentication or an inability to exchange keys with legitimate parties in the V2I environment. The generation of further keys might also be impaired, disrupting classical communication channels within the environment (for example through a key exhaustion attack). Mitigating this type of attack has been recorded in the public literature by deploying a post-quantum public-key algorithm to authenticate the next round of QKD.

For keys exchanged between entities, authentication per message will be required to ensure protection, while provision for secure authentication tags' re-use should be made to reduce the risk of decrypting messages that rely on the quantum keys. Also, the system's resilience dictates that a secret key recovery method is deployed to alleviate link failures in QKD. Trade-offs exist between secret key recovery sources and QKD wavelength in the platform due to disruption effects. This requires appropriate secret-key management, such as Quantum Key pools (QKP), to alleviate the low secret key rate [25].

QKPs are also used to recover secret keys due to disruption or link failures in the architecture. Making the architecture resilient allows for dynamic secret key recovery between each pair of adjacent nodes within the network. The number of keys stored at each QKP is associated with the limit distance of QKD and the nodes' security requirements. In Ref. [22], different operational scenarios for the QKPs have been identified as a function of wavelength consumption, the security requirements of node pairs, and QKD distance limits to ensure resilient key-service recovery.

6 | AN SOFTWARE-DEFINED NETWORK OVERARCHING PLATFORM FOR V2I COMMUNICATION

6.1 | Why Software-Defined Networking in V2I?

V2I communications leverage on heterogeneous wireless and fixed-line access technologies to enable high bandwidth, high density, and ultra-low latency communications. As such, SDN is proposed to enable the overall management and orchestration of network resources and QKD-related resources using a logically centralised network controller.

The main idea of SDN is to separate the forwarding data plane (data transmission) from the network control plane through APIs and software agents, providing an abstract view of the communications infrastructure and allowing the programmability of the network resources. This approach is further extended in our case to decouple the QKD-generated key communication path from the QKD control and management plane.

6.2 | An Software-Defined Network orchestrator architecture for a Quantum Key Distribution network infrastructure

Capitalising on the SDN framework allows the development of separate but interoperable orchestrators for the QKD and for the V2I infrastructures. In a schematic way, a separate orchestrator was developed to manage the processes illustrated in Figures 4 and 5. To jointly orchestrate data transportation and the two distinguished quantum technologies, an overarching hierarchical orchestrator is necessary that enables a global view of both the data and QKD networks, including the introduction of secondary controllers to fulfil specific data and QKD networking control and management tasks. In AirQKD, we solely concentrate on the task of end-to-end service provisioning for QKD-derived key generation exploiting FSO technology. Therefore, the SDN framework serves this purpose.

The end-to-end cryptographic service is made possible by means of coordinated actions and processes in four layers which are schematically shown in Figure 7. These layers are

- *Quantum Layer*: A pair of QKD transceivers generate symmetric keys. In each QKD transceiver module, a software middleware entity (driver) translates the quantum keys into a series of digital bit strings. Each QKD driver forwards the random bit strings to a Key Management Module (KMM) which is a digital entity that is developed in software too, and it is residing in the same QKD Trusted Node.
- *Key Management Layer*: This layer implements key management functionalities, such as the synchronisation and the reformatting of the bit strings and their subsequent storage within corresponding buffers. The KMM exposes interfaces to various cryptographic applications that aim to create a

secure data link by means of QKD symmetric keys. The KMM receives key requests from Secure Application Entities (SAEs), and it is responsible to acquire an adequate number of keys from the storage for these entities. A list of KMM functions is in the following Section 6.3.

- *QKD Control Layer*: This layer implemented the QKD control plane functions by means of the corresponding QKD Controllers. These functions include the connection set-up between KMMs to realise an end-to-end key delivery service, routing control for the key relay, control of QKD links and KMM links, session control for QKD services, as well as QoS and charging policy control.
- *Service Layer*: These are the cryptographic applications that request a particular encryption. The KMMs supply these SAEs with the necessary keys for implementing secure communication between the corresponding data links.

6.3 | The Key Management Layer Architecture

The proposed Key Management Layer Architecture is developed in compliance with the specifications that relevant standardisation bodies have issued [26–30]. In particular, the KMM supports the following functionalities:

- Key authentication.
- Key storage.
- Key protection.
- Key identification.
- Key provision to applications on request.
- Key replacement on request.
- Key destruction (based on decided key lifetime).
- Management of the key pool.
- Allocation of keys to applications based on the agreed QoS performance.
- Synchronisation with other KMM entities to allocate the correct keys to the applications.
- Key relay functionalities to support a multi-hop end-to-end key delivery scenario.

In particular, the last two functions, key synchronisation and key relay are two essential processes to perform the multi-hop end-to-end key delivery operation of Figure 2 via a cascade of steps as in Figure 5.

7 | CONCLUSION

Moving QKD systems from research into practical applications is important for the post-quantum future for secure communications. The AirQKD project has engineered an integrated V2I architecture consisting of a fixed wireless, converged connectivity platform made secure through a QKD system exploiting FSO technology. The architecture provides security and encryption efficiency for low-latency

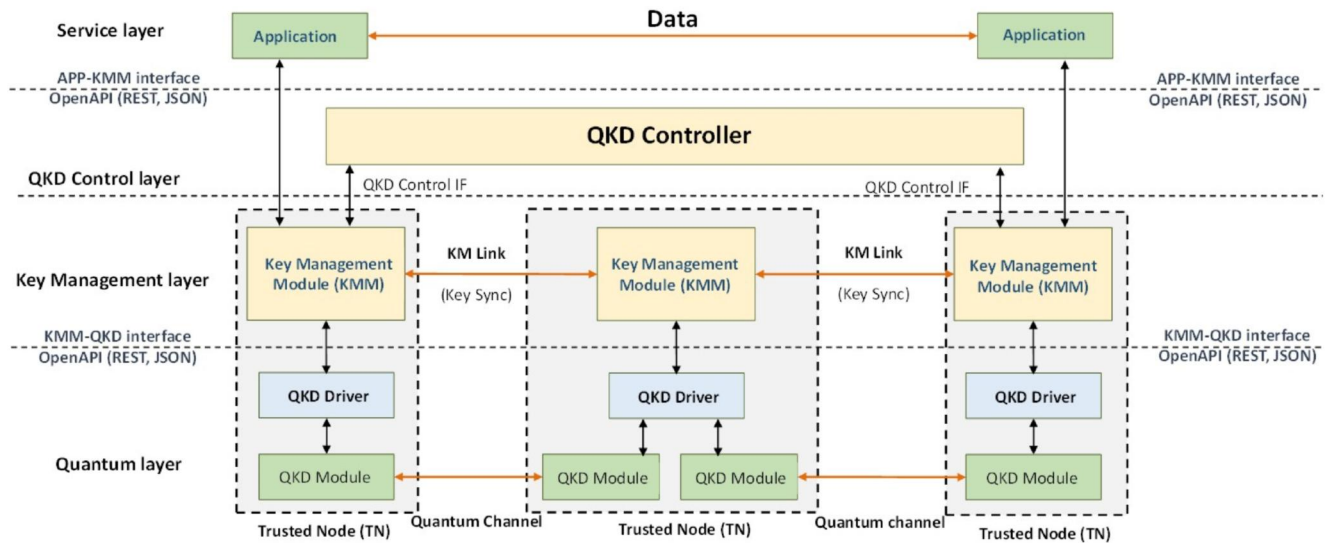


FIGURE 7 A schematic illustration of Software-Defined Network (SDN) architecture for the FSO-QKD key generation and relay.

performance. A high-level view of the architecture for the SDN-enabled control and management plane has been presented. This overarching SDN platform for V2I communications allows the orchestration of both the data transportation and the QKD system jointly. The foundations for mass commercialisation of FSO-QKD implementations have been laid. The experience of the AirQKD project has enabled much of the supporting hardware, software, and industrial services to be developed. The organisations involved aim to ensure that future communications can be secured with efficient symmetric key generation and usage systems.

AUTHOR CONTRIBUTIONS

Alexandros Stavdas: Conceptualisation; funding acquisition; investigation; methodology; project administration; writing – original draft; writing – review & editing. **Evangelos Kosmatos:** Conceptualisation; investigation; methodology; software; visualisation; writing – original draft; writing – review & editing. **Carsten Maple:** Conceptualisation; funding acquisition; methodology; project administration; writing – original draft; writing – review & editing. **Emilio Hugues-Salas:** Conceptualisation; investigation; methodology; visualisation; writing – original draft; writing – review & editing. **Gregory Epiphaniou:** Conceptualisation; investigation; methodology; writing – original draft; writing – review & editing. **Daniel S. Fowler:** Methodology; visualisation; writing – original draft; writing – review & editing. **Shadi A. Razak:** Conceptualisation; methodology; writing – original draft; writing – review & editing. **Chris Matrakidis:** Conceptualisation; methodology; software; writing – original draft; writing – review & editing. **Hu Yuan:** Methodology; writing – original draft; writing – review & editing. **Andrew Lord:** Funding acquisition; project administration; resources; supervision; writing – original draft; writing – review & editing.

ACKNOWLEDGEMENT

This work was supported by the Innovate UK project AirQKD (Ref.45364).

CONFLICT OF INTEREST STATEMENT

Andrew Lord is one of the guest editors of this special issue.

DATA AVAILABILITY STATEMENT

Data sharing not applicable – no new data generated.

ORCID

Daniel S. Fowler  <https://orcid.org/0000-0001-6730-2802>

Chris Matrakidis  <https://orcid.org/0000-0001-9302-5837>

Hu Yuan  <https://orcid.org/0000-0001-9833-5930>

REFERENCES

- Compound Semiconductor Applications Catapult: Project Snapshot AirQKD, (2020). <https://csa.catapult.org.uk/wp-content/uploads/2020/08/AirQKD.pdf>
- Stavdas, A.: 5G as a catalyst for a wider technological fusion that enables the fourth industrial revolution. In: Competitive Advantage in the Digital Economy (CADE 2021), pp. 39–49 (2021)
- Gyawali, S., et al.: Challenges and solutions for cellular based v2x communications. *IEEE Commun. Surv. Tutor.* 23(1), 222–255 (2020). <https://doi.org/10.1109/comst.2020.3029723>
- Zhao, L., et al.: Vehicular communications: standardization and open issues. *IEEE Commun. Stand. Mag.* 2(4), 74–80 (2018). <https://doi.org/10.1109/mcomstd.2018.1800027>
- Mannoni, V., et al.: A comparison of the v2x communication systems: its-g5 and c-v2x. In: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), pp. 1–5 (2019)
- Bagheri, H., et al.: 5g nrv2x: Towards Connected and Cooperative Autonomous Driving (2020). *arXiv preprint arXiv:200903638*
- Noor-A-Rahim, M., et al.: 6g for vehicle-to-everything (v2x) communications: enabling technologies, challenges, and opportunities. *Proc. IEEE* 110(6), 712–734 (2022). <https://doi.org/10.1109/jproc.2022.3173031>
- Jiang, W., et al.: The road towards 6g: a comprehensive survey. *IEEE Open J. Commun. Soc.* 2, 334–366 (2021). <https://doi.org/10.1109/ojcoms.2021.3057679>

9. Qiu, H., Qiu, M., Lu, R.: Secure v2x communication network based on intelligent pki and edge computing. *IEEE Netw.* 34(2), 172–178 (2019). <https://doi.org/10.1109/mnet.001.1900243>
10. Petit, J., Shladover, S.E.: Potential cyberattacks on automated vehicles. *IEEE Trans. Intell. Transport. Syst.* 16(2), 546–556 (2014). <https://doi.org/10.1109/tits.2014.2342271>
11. Tariq, F., et al.: A speculative study on 6g. *IEEE Wireless Commun.* 27(4), 118–125 (2020). <https://doi.org/10.1109/mwc.001.1900488>
12. Cao, Y., et al.: The evolution of quantum key distribution networks: on the road to the qinternet. *IEEE Commun. Surv. Tutor.* 24(2), 839–894 (2022). <https://doi.org/10.1109/comst.2022.3144219>
13. Zhao, Y., Liu, C.: Mobile Secret Communications Using Quantum Key Distribution Network (2020). <https://patentimages.storage.googleapis.com/c2/a2/8a/9ab440be60d309/US10560265.pdf>
14. Hughes, R.J., Nordholt, J.E., Peterson, C.G.: Secure Multi-Party Communication with Quantum Key Distribution Managed by Trusted Authority (2017). <https://patentimages.storage.googleapis.com/02/3f/ac/6b3da515685952/US9680640.pdf>
15. Berzanskis, A., et al.: Method of Integrating QKD and IPsec (2009). <https://patentimages.storage.googleapis.com/da/69/8c/7214a3c0aa42e7/US7602919.pdf>
16. Cha, Z., et al.: IPsec VPN Cipher Machines Based on Quantum Key Distribution (2018). <https://patentimages.storage.googleapis.com/d3/45/99/09493a95c384db/CN108173652A.pdf>
17. Andersson, Y., Papazoglou, K., Razak, S.: Symmetric Key Generation, Authentication and Communication between a Plurality of Entities in a Network (2020). <https://www.ipo.gov.uk/p-ipsum/Case/PublicationNumber/GB2589692>
18. Matsuda, K., et al.: Field demonstration of real-time 14 Tb/s 220 m FSO transmission with class 1 eye-safe 9-aperture transmitter. In: 2021 Optical Fiber Communications Conference and Exhibition (OFC), pp. 1–3, San Francisco (2021)
19. Paul, S., Guerin, E.: Hybrid opc ua: enabling post-quantum security for the industrial internet of things. In: 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, pp. 238–245 (2020)
20. Ndashimye, E., Sarkar, N.I., Ray, S.K.: A multi-criteria based handover algorithm for vehicle-to-infrastructure communications. *Comput. Network.* 185, 107652 (2021). <https://doi.org/10.1016/j.comnet.2020.107652>
21. Akhtar, A., et al.: Low latency scalable point cloud communication in vanets using v2i communication. In: ICC 2019 IEEE International Conference on Communications (ICC), pp. 1–7 (2019)
22. Wang, H., et al.: Resilient quantum key distribution (qkd)-integrated optical networks with secret-key recovery strategy. *IEEE Access* 7, 60079–60090 (2019). <https://doi.org/10.1109/access.2019.2915378>
23. Ghosh, S., Sarkar, P.: Variants of Wegman-Carter message authentication code supporting variable tag lengths. *Des. Codes Cryptogr.* 89(4), 709–736 (2021). <https://doi.org/10.1007/s10623-020-00840-w>
24. Price, A.B., Rarity, J.G., Erven, C.: A Quantum Key Distribution Protocol for Rapid Denial of Service Detection (2017)
25. Cao, Y., et al.: Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: a comparative study. *IEEE Trans. Netw. Serv. Manag.* 17(2), 946–957 (2020). <https://doi.org/10.1109/tnsm.2020.2964003>
26. The ITU Telecommunication Standardization Sector (ITU-T): Y.3800: Overview on Networks Supporting Quantum Key Distribution (2019)
27. ETSI Industry Specification Group (ISG) Quantum Key Distribution (QKD): ETSI GS QKD 004 V2.1.1 Quantum Key Distribution (QKD); Application Interface (2020)
28. ETSI Industry Specification Group (ISG) Quantum Key Distribution (QKD): ETSI GS QKD 014 V1.1.1 Quantum Key Distribution (QKD); Protocol and Data Format of REST-Based Key Delivery API (2019)
29. ETSI Industry Specification Group (ISG) Quantum Key Distribution (QKD): ETSI GS QKD 015 V1.1.1 Quantum Key Distribution (QKD); Control Interface for Software Defined Networks (2021)
30. The ITU Telecommunication Standardization Sector (ITU-T): Y.3803: Quantum Key Distribution Networks - Key Management (2020)

How to cite this article: Stavdas, A., et al.: Quantum Key Distribution for V2I communications with software-defined networking. *IET Quant. Comm.* 5(1), 38–45 (2024). <https://doi.org/10.1049/qtc2.12070>