

IET Quantum Communication

Special issue Call for Papers

**Be Seen. Be Cited.
Submit your work to a new
IET special issue**

Connect with researchers and experts in your field and share knowledge.

Be part of the latest research trends, faster.



[Read more](#)



The Institution of
Engineering and Technology

INDUSTRY ARTICLE

Analysis of outage performance in a 6G-V2X communications system utilising free-space optical quantum key distribution

Hu Yuan¹  | Daniel S. Fowler²  | Carsten Maple² | Gregory Epiphaniou²

¹School of Computer Science and Mathematics, Kingston University, London, UK

²WMG, University of Warwick, Coventry, UK

Correspondence

Daniel S. Fowler.

Email: dan.fowler@warwick.ac.uk

Funding information

Innovate UK, Grant/Award Number: 45364

Abstract

Quantum-based technologies will provide system engineers with new capabilities for securing data communications. The UK AirQKD project has implemented a Free-Space Optical Quantum Key Distribution (QKD) system to enable the continuous generation of symmetric encryption keys. One of the use cases for the generated keys is to secure Vehicle-to-Everything (V2X) communications. V2X applications would benefit from the certificate-free security provided by QKD for a post-quantum society. How FSO-QKD could integrate into a V2X architecture is examined. An overview of V2X is provided with the role that FSO-QKD could secure V2X data though some obstacles exist. One of the issues with 6G communications is the potential line-of-sight (LOS) considerations between the V2X devices. The modelling required for LOS is examined to analyse the outage performance of the building to infrastructure links in the 6G architecture. The results from the model show that further work is required if 6G LOS communications are going to be relied upon for future safety-critical V2X applications.

KEYWORDS

cryptology protocols, quantum cryptography, telecommunication security

1 | INTRODUCTION

Quantum and photonics-based technology will play a role in the next sixth generation, that is, 6G, of communications, whether that is quantum: computing, communications, random number generation (QRNG), timing, or secure key generation and distribution, that is, Quantum Key Distribution (QKD) [1]. The Innovation UK-funded AirQKD multi-partner project addressed the future challenges in commercialising quantum Free-Space Optical (FSO) communication technologies within the UK. An overview of Optical Wireless Communication (OWC), which includes FSO, can be found in ref. [2].

Society will see a transitional period where elements within complex communications infrastructures will be replaced with quantum-based versions to step up system capability. There will be improvements in data capacity, latency, and security [3]. The AirQKD project has constructed a system for FSO-QKD and associated supporting technologies from semiconductors to applications. The AirQKD FSO-QKD project has allowed

its contributors to raise their Technology Readiness Level for UK-derived quantum communications-related components, software, and systems.

One of the application scenarios developed for the new AirQKD FSO-QKD system is its use in securing Vehicle-to-Everything (V2X) communications (see Figure 1). In this work, we examine FSO-QKD within a 6G-V2X architecture. 6G-V2X will benefit from the improved capacities and security provided by OWC systems [4]. Further, we consider how future deployment of an FSO-QKD system for urban 6G-V2X systems must consider Line-of-Sight (LOS) issues. The LOS challenge is part of the distribution issues of secure keys from the QKD system to the V2X infrastructure. LOS has been previously modelled around buildings [5] and to the vehicle [6] for classical radio frequency (RF) communications, here we considered LOS for building-based communication Access Points (APs) for OWC links. For a V2X system, the aim is to minimise the non-line-of-sight (NLOS) issues and to provide the optimal density of devices required to provide

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.



FIGURE 1 Vehicle-to-Everything data communications could benefit from quantum-based technologies to improve bandwidth and latency.

reliable key distribution. Furthermore, when NLOS occurs, we test an algorithm to enable an LOS device to relay a key to an NLOS device.

The rest of this work is as follows: in Section 2, we discuss some of the current technologies being used for V2X systems, and Section 3 discusses how quantum-based technologies could enhance the security of V2X technology. In Section 4, the architecture for a V2X system with FSO-QKD is described. Section 5 has a model that can be used to look at LOS issues in future 6G-V2X systems. We propose a peer-assisted QKD in Section 6 to see if it improves LOS issues. The results from the modelling are discussed in Section 7 before concluding in Section 8.

2 | BACKGROUND TO 6G V2X TECHNOLOGIES

The V2X concept covers all connected vehicle communication scenarios, where the X in V2X can represent infrastructure (V2I), vehicles (V2V), pedestrians (V2P), and networks (V2N) [7]. The V2X system enables localised and wide area messaging for traffic incidents and communication with a central Data Centre (DC) for advanced Intelligent Transportation System (ITS) requirements. V2X can be an enabler for a variety of applications to enhance road safety, driving efficiency, and passenger infotainment and offers the potential to change the way we commute [8]. However, the complex and demanding V2X environment illustrated by Figure 1 demands high performance in areas related to reliability, latency, bandwidth, and security, and handling high urban device density [7, 9]. If the V2X technical requirements cannot be met with high assurance, then safety-critical applications may not be deployed. This would jeopardise confidence and public trust in the use of Connected and Automated Mobility (CAM) transport systems [10].

The development towards robust and reliable V2X communication infrastructure has been based on Dedicated

Short-Range Communications (DSRC) solutions, utilising the Wireless Access for Vehicular Environment (WAVE) standards IEEE 802.11p and IEEE 1609 [11]. This has relied on the deployment of dedicated devices called Road Side Units (RSUs) within the urban infrastructure and On-Board Units (OBUs) within vehicles. The OBUs exchange data with other OBUs and with RSUs that act as APs for the vehicles. Road Side Units can be attached to existing street furniture, such as lamp-posts and traffic lights, or separate poles. They have a local Wi-Fi connection for maintenance or travel time applications.

The RSUs and OBUs transmit at 5.9 GHz to provide low latency for high-speed events, for example, for crash avoidance applications, and for relaying data related to road safety. There are several types of standardised V2X messages used as required by V2X applications; examples include [12]:

- CAM – Cooperative Awareness Messages, for vehicle status and capabilities.
- DENM – Decentralised Environmental Notification Messages, for road profiles, zones, and hazards.
- CPM – Collective Perception Messages, for object and obstacles detection.
- MAPEM – Map Message, for geographic information.
- SPATEM – Signal phase and Timing Message, for the state for signals at intersections.
- IVIM – In-Vehicle Information Message, to relay electronic sign indications to vehicles.

In 2019, the third-Generation Partnership Project (3GPP), the body responsible for cellular communication standards, enhanced support for vehicular services. The 5G New Radio (5G NR) standards have support for Cellular-Vehicle-to-Everything (C-V2X) [13]. This can utilise the cellular connection built into vehicles and a slice of the widely installed 4G/5G telecommunication infrastructure. The design of C-V2X is aimed at adding other V2X features, for example, vehicle platooning, advanced driver assistance, cooperative driving, remote (teleoperation) driving, and more powerful sensors [14]. C-V2X will compete with the Next Generation V2X (NGV) WAVE standard, IEEE 802.11bd.

Despite many V2X trials, the widespread roll-out of V2X applications has not occurred. This is due to both technical and commercial challenges [9, 15–17], they include:

- DSRC is seen to have limitations in cities because of limited coverage, low data rate, limited quality-of-service (QoS) guarantees, and access delays.
- A high RSU density is needed to support high throughput urban and inter-urban traffic and the associated data processing requirements.
- Again, high RSU density is required to reduce or eliminate LOS issues.
- The need to keep data communications resilient and secure during a long operating life cycle.
- Equipment purchase costs, installation and maintenance costs, insufficient return on investment or cost benefits.

- The verification of systems operating at large scales within city-wide environments.

The implementation of C-V2X is seen as a way to address some of the challenges. However, the lack of V2X adoption is why the United States Federal Communications Commission reduced the amount of 5.9 GHz spectrum available to V2X devices [18]. If current communication technologies are unable to meet the performance requirements to support the Internet of Vehicles, then engineers will look at the capabilities of 6G communication technologies [19] with quantum technologies having a future role. We define the emerging quantum-based communication technologies as being within the 6G label, which is being applied to several technologies [20], including those based around photonics, terahertz frequencies, advanced Artificial Intelligence software, as well as the utilisation of quantum properties from new devices, for example, FSO-based systems, QRNGs, and Physical Unclonable Functions (PUFs).

3 | QUANTUM-BASED TECHNOLOGIES FOR V2X SECURITY CHALLENGES

In the AirQKD project, the V2X security challenge was one of the aspects addressed by quantum-based technologies. The resilience and security of future super-systems, as with a city-wide V2X network, are important [21]. Nation-state threat actors, cyber terrorists, hacktivist groups, and cyber criminals could seek to cause widespread disruption, whether by transmitting illegitimate V2X messages to disorientate real or autonomous drivers, locating infrastructure targets to distribute ransomware, or harvesting private data.

In the V2X standards, certificate-based Public Key Infrastructure (PKI) has been specified to ensure trustworthy communication. However, the implementation of PKI can have an impact on performance. For example, distributing, redistributing, and using encryption keys may introduce latency issues, a particular concern for safety-related applications [22]. Further, PKI security loses its strength as the number of nodes in a system increases and the system has to be managed over a long life cycle. Furthermore, PKI is seen as weak in a post-quantum environment. This provides an argument for the use of provably secure quantum-based symmetric key generation systems and their inherent security. They are highly resistant to cloning and tampering [23]. Two such systems included in the AirQKD project are QKD [24], specifically FSO-QKD, and PUFs [25].

Free-Space Optical and FSO-QKD have traits that are beneficial for high-performance secure communications [26, 27]:

- high throughput data;
- accurate beam targeting;
- energy efficiency;
- spatial and temporal security, including the strict LOS requirements;

- information-theoretic (unconditional) security (symmetric keys are independent of the computational power);
- distance coverage without physical cabling;
- integration into existing communications systems.

There are disadvantages with FSO communications due to variable atmospheric conditions and LOS blocking. However, FSO, and particularly FSO-QKD, can have a part to play in future communications systems. Instead of relying on post-quantum weak PKI, a continuous source of strong keys can be provided. During the generation of keys between two parties, Alice and Bob, an eavesdropper, Eve, will be detected based on the physical properties of FSO-QKD. The errors in the key data will occur when Eve listens to the FSO channel between Alice and Bob [28]. This allows the detection of Eve and the suspect keys reject, protecting the key agreement protocol [29].

A fixed point-to-point FSO-QKD system is not suitable for mobile vehicles, and the technology has a long way to go before it is of a size and cost suitable for mass deployment. Further, there are occasions when the FSO beam is functioning below the operational level (through atmospheric or other interference). This requires another quantum-based source of keys to maintain data security. The AirQKD approach utilises a quantum-enhanced Hardware Security Module (HSM) that provides a key amplification process for the QKD and utilises a PUF and associated key distribution algorithm [30]. The HSM interfaces to relevant devices within the V2X system. The patented PUF and key amplification protocol supports the FSO-QKD system and generates secondary keys for V2X devices.

Alongside the development of QKD systems and PUFs, other alternative security approaches that will enter the quantum transitional period include Quantum Resistant Algorithms (QRA) [31] or Post Quantum Cryptographic codes (PQC) [32] with standardisation efforts in progress [33]. These potential alternatives to QKD, or working alongside QKD, are not part of the AirQKD project. However, a future possibility of systems that integrate QKD and QRA can be viewed as feasible [34], predicated on the assumption that the new mathematical QRAs will not be broken by future quantum computers.

The AirQKD project V2X scenario was limited to the Vehicle-to-Infrastructure (V2I) network. It is an example of a transitional system, where the V2I system devices operate with security provided by quantum-based elements, namely FSO-QKD and PUFs.

4 | OVERVIEW OF THE AirQKD 6G V2I ARCHITECTURE

The illustration in Figure 2 is the AirQKD transitional 6G V2I infrastructure. Building on the V2X background in Section 2, the RSUs are typically powered over an Ethernet connection, that is, using Power-over-Ethernet (PoE), which can be used for communications with the ITS system. The RSU has a backhaul data connection to and from the city-wide ITS

networks and their DCs, via fixed (e.g., fibre-optic, copper) or wireless (5G/Wi-Fi) technologies. Future RSUs could implement optical connections with sufficient advancement in optical transmitter/receiver engineering, miniaturisation, and cost reduction. In this work, we are only considering wireless/optical connectivity. The RSUs communicate with a microcell Base Station (BS) or Wi-Fi/optical AP located on a rooftop of nearby buildings (the dashed blue line in Figure 2). The data flowing to or from the AP and DC is routed through typical telecommunication infrastructure, for example, via an Optical Network Unit for a fibre network backhaul, that is located in the vicinity of the building (connection is shown as a solid blue line in Figure 2).

The DC infrastructure provides connectivity to city and cloud services and the processing and storage resources for V2X. Therefore, RSUs are able to connect vehicles to the cloud, to core network computing resources, and allow access to local traffic mapping and V2X messaging functions. A secure V2X system will include vehicle authentication and ITS service registration facilities. The use of the project's FSO-QKD enables the continuous generation of secure keys for the encryption of system data. The rooftop-mounted transmitters, T_X , and receivers, R_X , can be separated by 300 m (the dashed red line in Figure 2). The generated keys, K_X , are daisy-chain relayed [24] throughout the system utilising an AirQKD-developed Key Management (KM) software system. The KM has a store of keys and exposes an Application Programming Interface for use by system devices to store and request keys.

As mentioned in Section 3, the AirQKD approach to key resilience is to use an enhanced HSM. The HSM has a post-quantum secure PUF [30] and uses it to support key provisioning with a key amplification process. This enables system devices to operate securely when the FSO-QKD system is not fully operational. The HSM module interfaces with the KM via the APs and other system elements, enabling the secure passing of amplified quantum keys to the endpoint devices. This process adds resilience to the key generation and distribution protocol.

The system aspects of reliability, security, and LOS, noted in Sections 2 and 3, are important [35] in a mixed RF/FSO architecture. Ensuring reliable key distribution requires investigating the suitable placement of RSUs for LOS to the APs.

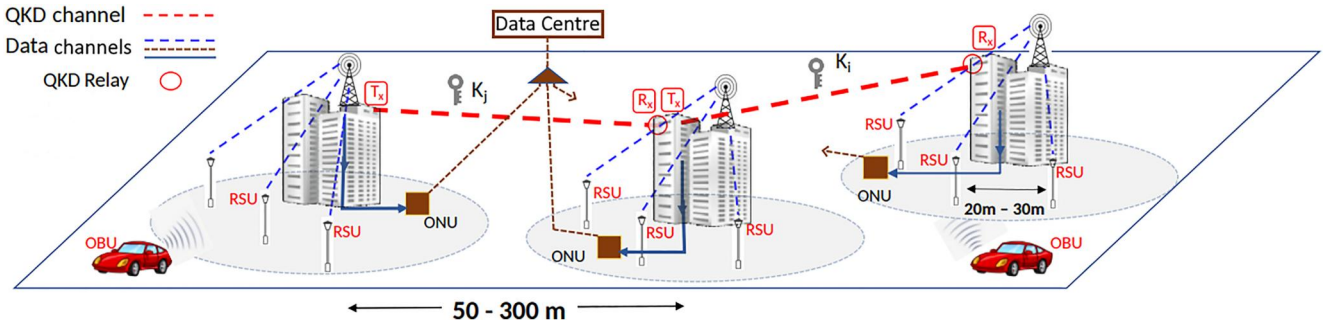


FIGURE 2 Overview of the AirQKD scenario architecture.

5 | SYSTEM MODEL FOR LOS V2X DEVICE PLACEMENT

The optimal placement of devices within the V2X infrastructure is not only for the reliability of both communications and security. It is a consideration in installation and system costs. All these reasons motivated the modelling of the LOS placement of RSUs. In this case, we consider direct LOS to maximise both wireless and (future) optical communication links. The issue is illustrated in Figure 3; a microcell BS will have NLOS to a V2X device (e.g., an RSU) if another building or obstacle is of sufficient height to block the transmission path.

5.1 | Road Side Units distribution

For any set of Euclidean space \mathcal{B} , $\mathcal{B} \subset \mathbb{R}^d$, \mathbb{R}^d is a d -dimensional Euclidean space. $N(\mathcal{B})$ is the number of points in the set \mathcal{B} , the number $N(\mathcal{B})$ has a Poisson distribution with the density Λ of a space set of \mathcal{B} . Therefore, the probability of the number of random points in the set \mathcal{B} is [36],

$$\mathbb{P}(N(\mathcal{B}) = k) = \exp\left(-\int_{\mathcal{B}} \Lambda(x) dx\right) \frac{\left(\int_{\mathcal{B}} \Lambda(x) dx\right)^k}{k!} \quad (1)$$

For a 2D Poisson process, $\int_{\mathcal{B}} \Lambda(x) dx = A\Lambda$, where A is the area of the 2D space \mathcal{B} .

Therefore, the probability of the number of random points in the 2D set \mathcal{B} is:

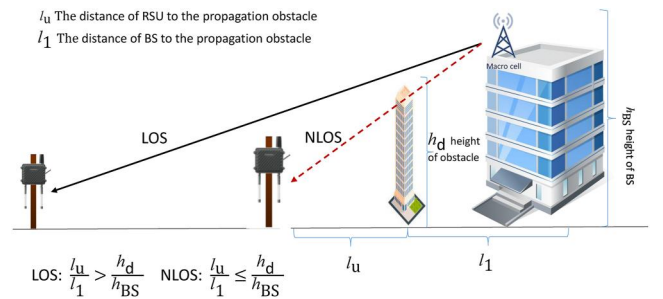


FIGURE 3 Channel model of LOS and NLOS.

$$\mathbb{P}(N(\mathcal{B}) = k) = \exp(-\Lambda A) \frac{(\Lambda A)^k}{k!}. \quad (2)$$

An important quantity is the distance r separating a typical RSU from its identified Quantum Key Base Station (QKBS), that is, the AP communicating with the KM and establishing the QK secured communication to the RSU. Since each RSU communicates with the closest BS, no other BS can be closer than r . In other words, all interfering base stations must be farther than r . The RSUs are attached to the closest QKBS, with a random variable distance R , and from the Eq. (2), $k = 0$, so the probability of no QKBS closer than r is,

$$\mathbb{P}[R > r] = \mathbb{P}[\text{no QKBS closer than } r] = e^{-\Lambda_{\text{BS}} \pi r^2}, \quad (3)$$

where Λ_{BS} is the density of QKBSs.

Therefore, the cumulative distribution function of the closest QKBS is

$$F_R(r) = 1 - e^{-\Lambda_{\text{BS}} \pi r^2} \quad (4)$$

and the probability density function (pdf) of to the closest QKBS can be found as follows:

$$f_R(r) = \frac{dF_R(r)}{dr} = 2\Lambda_{\text{BS}} \pi r e^{-\Lambda_{\text{BS}} \pi r^2} \quad (5)$$

5.2 | LOS channel

As mentioned, for reliability, the delivery of a QK requires an LOS channel between RSU and the distributing QKBS. Therefore, the distance d between RSU and QKBS should be (see Figure 3):

$$d \geq \frac{l_1(h_d + h_{\text{BS}})}{h_{\text{BS}}} \quad (6)$$

The locations of the RSUs are independent and modelled via a Poisson Point Process (PPP). The expectation of a non-negative continuous random variable X is $\mathbb{E}[X] = \int_{t>0} \mathbb{P}(X > t) dt$. With the PPP and fading distribution, the expectation distance for any single RSU with the LOS QKBS is:

$$\mathbb{P}(d_{\text{LOS}} > \zeta) = \int_0^{+\infty} \mathbb{P}\left\{\frac{l_1(h_d + h_{\text{BS}})}{h_{\text{BS}}} > \zeta\right\} d\zeta \quad (7)$$

where ζ is the threshold distance that RSU can have an LOS channel to QKBS.

5.3 | Quantum key outage probability

There are two requirements of a QK being successfully delivered to an RSU from a QKBS, (1) the RSU should be

located within the coverage of the QKBS and (2) the communication channel between the RSU and QKBS is LOS. Therefore, the event of a QK distribution outage is defined as the RSU is not within the QKBS coverage or there being no LOS channel. Thus, the probability of the QK outage is as follows:

$$\begin{aligned} \mathbb{P} &= 1 - \mathbb{P}(R > r) \mathbb{P}(d_{\text{LOS}} > \zeta) \\ &= e^{-\Lambda_{\text{BS}} \pi r^2} \int_0^{+\infty} \mathbb{P}\left\{\frac{l_1(h_d + h_{\text{BS}})}{h_{\text{BS}}} > \zeta\right\} d\zeta \end{aligned} \quad (8)$$

In our work, the value of the distance from RSU to the QKBS is a dependent discrete variable; therefore, the probability of the outage can be written as follows:

$$\mathbb{P} = e^{-\Lambda_{\text{BS}} \pi r^2} \sum_{i=1}^{\Phi} \frac{l_1(h_d + h_{\text{BS}})}{h_{\text{BS}}} > \zeta \quad (9)$$

where Φ is the set of all possible RSU locations.

Using the above model, it is possible to see the effect of varying RSU density in an environment.

6 | PEER ASSISTANT QKD

To examine if the successful delivery of a QK can be enhanced, we introduced a peer-assisted QKD. In the case of an RSU with NLOS to a QKBS AP, an algorithm examines neighbouring RSUs to find the closest to the NLOS RSU. The aim is to deliver a QK over the RSU V2X channel, utilising the HSM security protocol. Algorithm 1, utilising the system model parameters, is the Peer Assistant QKD method in the case of NLOS for an RSU.

Algorithm 1 Peer Assistant QKD

function PEERASSISTANT(l_1 , h_d , h_{BS} , Λ_{BS} , ζ , r)

When \mathbb{P} of U_d occurred as Eq. (9).

for $i, j \in \Phi$ **do**

DISTANCE(d_i , U_d closest U_i)

if $d_i \neq \emptyset$ **then**

Pass the QK to U_i

DISTANCE(d_j , U_d closest U_j)

if $d_j \neq \emptyset$ **then**

Pass the QK to U_j

else

Outage occurred

end if

else

Outage occurred

end if

Until U_d reached

end for

end function

In summary, the algorithm is:

1. When the outage occurs (NLOS), the QKBS selects the RSU, U_i , which is the closest distance to the destination RSU U_d , and with an LOS channel to the QKBS; if no RSU is found meeting the condition, outage occurred.
2. The QKBS sends the QK to U_i that passes the QK to its neighbouring RSU U_j ; if no RSU is found meeting the condition, outage occurred.
3. U_j passes the QK to its neighbouring RSU (becoming the new U_j) closet to U_d ; if no RSU is found meeting the conditions, outage occurred.
4. Repeat step 3 until the destination RSU is reached, otherwise outage occurred.

6.1 | Outage probability of peer assistant Quantum Key Distribution

The outage probability of the Peer Assistant QKD is defined when the QKBS or relay RSU cannot find a neighbouring RSU with an LOS channel to the QKBS. Therefore, it can be written as follows:

$$\mathbb{P}_{\text{Peer,out}} = 1 - \prod_{j=1}^J [1 - \mathbb{E}(\mathbb{P}_{j,\text{out}})] \quad (10)$$

where $\mathbb{E}(\mathbb{P}_{j,\text{out}})$ is the probability of a single assistance and the total number of assistance J is determined by the density of RSU in the network.

The outage of U_i to its neighbouring RSU can be obtained from (3)

$$\mathbb{P}_{\text{P2P}} = 1 - e^{-\Lambda_{\text{RSU}} \pi r_{\text{RSU}-i}^2} \quad (11)$$

7 | NUMERICAL RESULTS

All the above models are programmed and executed within the MATLAB software tool. A building model was used to provide objects for the study of LOS/NLOS situations for the RSU/QKBS AP communications channels, that is, the values for the system model parameters. The built environment used is part of Ottawa City in Canada [37]. A $0.93 \text{ km} \times 0.56 \text{ km}$ grid comprises approximately 80 buildings of various shapes and dimensions. The 3D city model is shown in Figure 4. The RSUs are distributed along the streets running between the buildings. The greater the number of RSUs used, the greater the RSU density within those streets.

The results from executing the models within MATLAB are shown in Figures 5 and 6 with and without the peer-assisted QK delivery within the city environment.

The first figure, Figure 5, shows the QK delivery outage probability for varying RSU densities. It shows an expected decrease in the outage probability when the number of RSUs distributed increases (i.e., increased RSU density) as the RSU density decreases; there is a greater chance that the QK delivery will fail because an AP cannot find an LOS channel to an RSU. At that point, the peer assistance scheme is tried, that is, the peer assistant is enabled when there is NLOS from QKBS

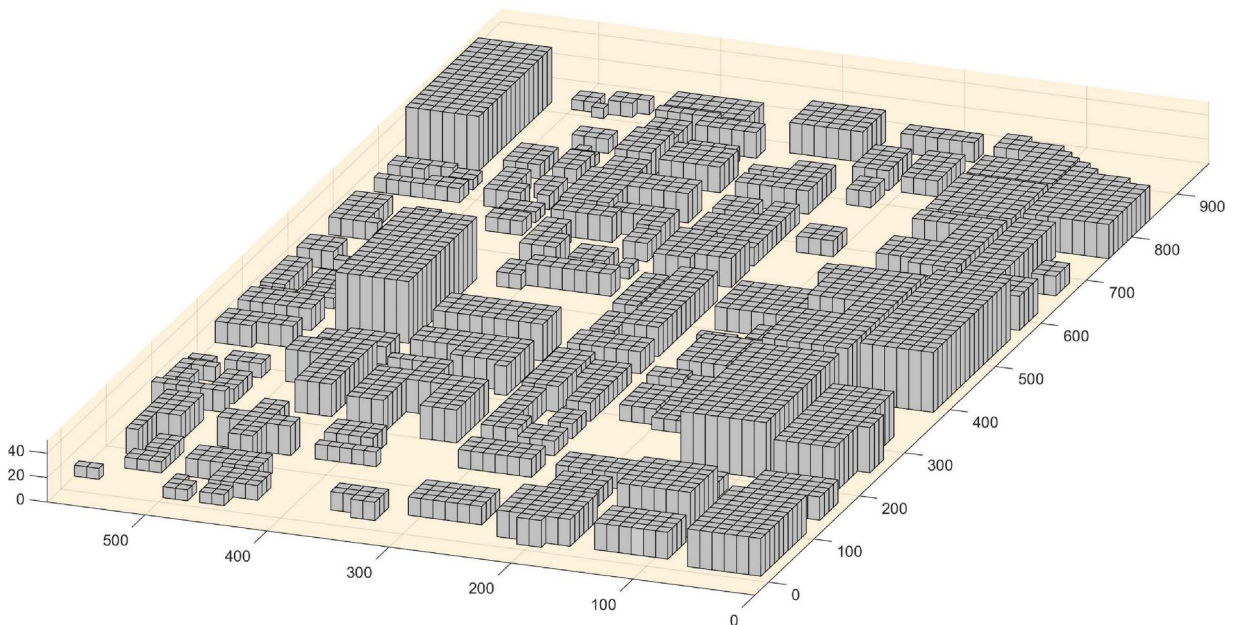


FIGURE 4 3D building model (m^2) of a section from Ottawa City.

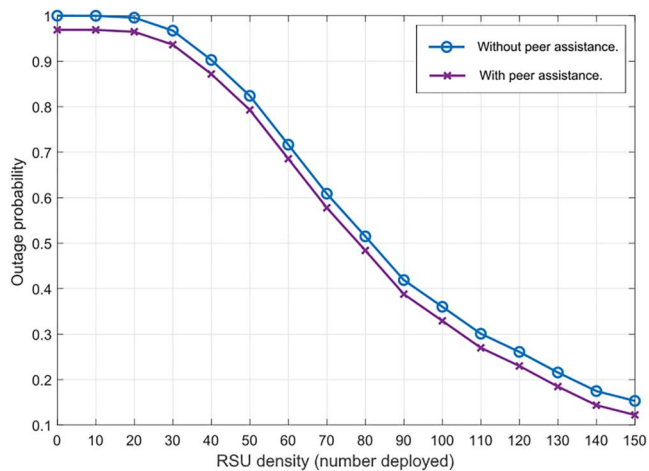


FIGURE 5 Quantum Key delivery outage probability for varying road Side Unit densities within the city environment.

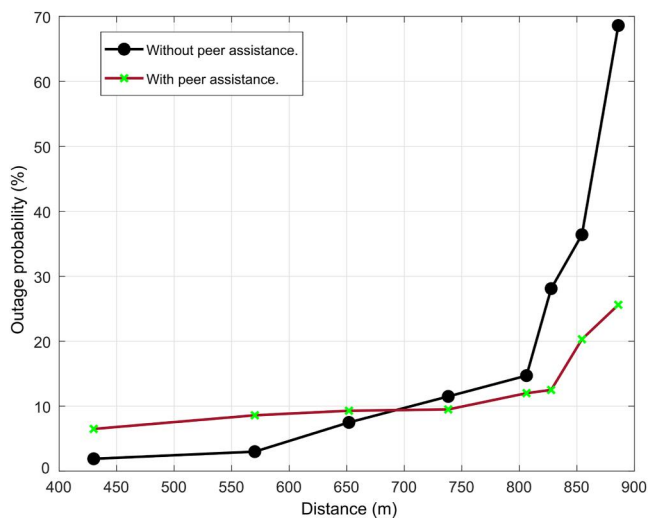


FIGURE 6 Quantum Key delivery outage probability percentage with differing distance from quantum Key Base Station access point to road side unit.

AP to the desired destination RSU. The QKBS AP will choose neighbouring RSUs as a relay to deliver the QK. Points of note from the results shown in Figure 5:

- The chosen peer-assisted method improves the QK delivery outage, but the difference is not large. For the chosen city model and RSU density, it equates to a saving of around 10 RSUs for the same outage probability.
- The outage probability is low when the total distributed RSUs is 150. However, the outage is above 0.1, which is likely insufficient for an effective V2X system. For example, the model needs to be improved to consider a variation in the mounting height of the RSUs.
- The outage probability should reach 1.0 for the lowest density of RSUs, even with the peer assistance algorithm. This is not indicated and is likely due to a rounding error at the low end and requires further model refinement.

Figure 6 presents the outage percentage change based on the distance the QK travels between a QKBS AP and the target RSUs. The outage probability climbs to 69% when the QK travel distance between AP and RSU went to 877 m without peer assistance, that is, the outage probability increases with the greater distance to an RSU for a QK (as before, the longer distance gives a greater chance there is a LOS blockage). Points of note from the results shown in Figure 6:

- Considering distance travelled compared to density shows a larger difference in the data between Figures 5 and 6. Peer assistance QK delivery has a larger noticeable impact.
- The peer assistance scheme did not enhance the outage performance when the distance travelled was shorter than 687 m.
- The peer assistance aids the longer QK delivery distances, particularly farther than 800 m. When the distance is over 875 m, the peer assistance algorithm improves the outage performance by a factor of 2.55 down from 69% to 27%.

The model has indicated that NLOS issues are of concern within a city environment. Despite a high density of RSUs and the use of an alternative path to route a QK to a consuming device, for the particular city environment used, a 100% delivery was not seen. Further work will determine where the model can be improved, for example, in the consideration of the mounting height of RSUs and the onward impact of transmissions to the OBU. In addition, trying other city environments, particularly much larger city models, for comparison, can help to assess the impact of building height and locations on QK delivery.

8 | CONCLUSIONS

A secure, efficient, reliable, and resilient communication infrastructure is required to support developments in CAM systems. 6G communication systems offer an opportunity to integrate QKD and other quantum-based technologies into vehicular environments, protecting against advances in quantum computation that are rendering many of the classical algorithms that underpin PKI obsolete. However, there is work to perform in assessing the use of these technologies in 6G-V2X systems. The AirQKD project has used V2X as an application use case to explore some of the issues that are present as discussed in Sections 2 and 3.

AirQKD partners have designed and implemented an architecture to consume the keys from an FSO-QKD system. However, this work shows that implementing it on a city-wide scale requires addressing NLOS issues. A complex urban environment cannot support a simple arrangement of key-consuming RSU devices. Future work will see further simulation and practical experiments being performed to understand how efficient placement of RSUs and APs can be achieved to reach a 100% deployment of keys generated from the FSO-QKD system to those devices.

AUTHOR CONTRIBUTIONS

Hu Yuan: Conceptualization; data curation; formal analysis; investigation; methodology; software; validation; visualization; writing—original draft. **Daniel S. Fowler:** Conceptualization; investigation; project administration; writing—review and editing. **Carsten Maple:** Conceptualization; funding acquisition; project administration; resources; supervision; writing—review and editing. **Gregory Epiphaniou:** Project administration; supervision; writing—review and editing.

ACKNOWLEDGEMENTS

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

CONFLICT OF INTEREST STATEMENT


None.

DATA AVAILABILITY STATEMENT

Data are available on request from the authors.

ORCID

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

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

REFERENCES

- Lord, A.: Where does QKD fit in a post-quantum secure world? In: Quantum West. International Society for Optics and Photonics. SPIE (2021).1171405
- Jahid, A., Alsharif, M.H., Hall, T.J.: A contemporary survey on free space optical communication: potentials, technical challenges, recent advances and research direction. *J. Netw. Comput. Appl.* 200, 103311 (2022). <https://doi.org/10.1016/j.jnca.2021.103311>
- Gyongyosi, L., Imre, S., Nguyen, H.V.: A survey on quantum channel capacities. *IEEE Commun. Surv. and Tutorials* 20(2), 1149–1205 (2018). <https://doi.org/10.1109/comst.2017.2786748>
- Guo, H., et al.: Vehicular intelligence in 6g: networking, communications, and computing. *Vehicular Commun.* 33, 100399 (2022). <https://doi.org/10.1016/j.vehcom.2021.100399>
- Biddlestone, S., et al.: An integrated 802.11p wave dsrc and vehicle traffic simulator with experimentally validated urban (los and nlos) propagation models. *IEEE Trans. Intell. Transport. Syst.* 13(4), 1792–1802 (2012). <https://doi.org/10.1109/tits.2012.2213816>
- Aygun, B., et al.: Geometry-based propagation modeling and simulation of vehicle-to-infrastructure links. In: 2016 IEEE 83rd Vehicular Technology Conference, pp. 5. VTC Spring (2016)
- Alalewi, A., Dayoub, I., Cherkaoui, S.: On 5g-v2x use cases and enabling technologies: a comprehensive survey. *IEEE Access* 9, 107710–107737 (2021). <https://doi.org/10.1109/access.2021.3100472>
- Rahim, N.A., 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>
- Gyawali, S., et al.: Challenges and solutions for cellular based v2x communications. *IEEE Commun. Surv. and Tutorials* 23(1), 222–255 (2021). <https://doi.org/10.1109/comst.2020.3029723>
- Emara, M., Filippou, M.C., Sabella, D.: Mec-enhanced information freshness for safety-critical c-v2x communications. In: 2020 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–5. IEEE (2020)
- Klapez, M., Grazia, C.A., Casoni, M.: Application-level performance of ieee 802.11 p in safety-related v2x field trials. *IEEE Internet Things J.* 7(5), 3850–3860 (2020). <https://doi.org/10.1109/jiot.2020.2967649>
- TransAID Project: D5.1 Definition of V2x Message Sets (2019). <https://www.transaid.eu/deliverables/>
- Ansari, K.: Joint use of dsrc and c-v2x for v2x communications in the 5.9 ghz its band. *IET Intell. Transp. Syst.* 15(2), 213–224 (2021). <https://doi.org/10.1049/itr2.12015>
- Bagheri, H., et al.: 5g Nr-V2x: Towards Connected and Cooperative Autonomous Driving. *arXiv preprint arXiv:200903638*, 2020
- 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>
- Wang, J., et al.: A survey of vehicle to everything (v2x) testing. *Sensors* 19(2), 334 (2019). <https://doi.org/10.3390/s19020334>
- Ghosal, A., Conti, M.: Security issues and challenges in v2x: a survey. *Comput. Network.* 169, 107093 (2020). <https://doi.org/10.1016/j.comnet.2019.107093>
- Gitlin, J.M.: Court Rules Fcc Is Allowed to Reassign 5.9 Ghz Bandwidth, Killing V2x (2022). <https://arstechnica.com/cars/2022/08/v2x-is-finally-dead-as-court-refuses-to-stop-fccs-5-9-ghz-reallocation>
- Bréhon–Grataloup, L., Kacimi, R., Beylot, A.L.: Mobile edge computing for v2x architectures and applications: a survey. *Comput. Network.* 206, 108797 (2022). <https://doi.org/10.1016/j.comnet.2022.108797>
- 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>
- 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>
- 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>
- 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>
- Cao, Y., et al.: The evolution of quantum key distribution networks: on the road to the qinternet. *IEEE Commun. Surv. and Tutorials* 24(2), 839–894 (2022). <https://doi.org/10.1109/comst.2022.3144219>
- Arapinis, M., et al.: Quantum physical unclonable functions: possibilities and impossibilities. *Quantum* 5, 475 (2021). <https://doi.org/10.22331/q-2021-06-15-475>
- Trinh, P.V., et al.: Quantum key distribution over fso: current development and future perspectives. In: 2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama), pp. 1672–1679 (2018)
- Farooq, E., Sahu, A., Gupta, S.K.: Survey on fso communication system - limitations and enhancement techniques. In: Janyani, V., et al. (eds.) *Optical and Wireless Technologies: Proceedings of OWT 2017*, pp. 255–264. Springer Singapore, Singapore (2018)
- Castro, G., Ramos, R.V.: Enhancing eavesdropping detection in quantum key distribution using disentropy measure of randomness. *Quant. Inf. Process.* 21(2), 1–10 (2022). <https://doi.org/10.1007/s11128-022-03422-y>
- Kumar, A., et al.: An enhanced quantum key distribution protocol for security authentication. *J. Discrete Math. Sci. Cryptogr.* 22(4), 499–507 (2019). <https://doi.org/10.1080/09720529.2019.1637154>
- 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/Publication/Number/GB2589692>
- NIST: Nist Announces First Four Quantum-Resistant Cryptographic Algorithms (2022). <https://www.nist.gov/news-events/news>
- Baldi, M., Santini, P., Cancellieri, G.: Post-quantum cryptography based on codes: state of the art and open challenges. In: 2017 AEIT International Annual Conference, pp. 1–6 (2017)
- FernándezCaramés, T.M.: From pre-quantum to post-quantum iot security: a survey on quantum-resistant cryptosystems for the internet of things. *IEEE Internet Things J.* 7(7), 6457–6480 (2019). <https://doi.org/10.1109/jiot.2019.2958788>

34. Neish, A., Walter, T., Enge, P.: Quantum-resistant authentication algorithms for satellite-based augmentation systems. *Navigation* 66(1), 199–209 (2019). <https://doi.org/10.1002/navi.287>
35. Mohsan, S.A.H., Khan, M.A., Amjad, H.: Hybrid fso/rf networks: a review of practical constraints, applications and challenges. In: *Optical Switching and Networking*, pp. 47 (2023)
36. Yuan, H., et al.: Interference-aware multi-hop path selection for device-to-device communications in a cellular interference environment. *IET Commun.* 11(11), 1741–1750 (2017). <https://doi.org/10.1049/iet-com.2016.0640>
37. Yuan, H., Guo, W., Wang, S.: Emergency route selection for d2d cellular communications during an urban terrorist attack. In: 2014 IEEE

International Conference on Communications Workshops (ICC), pp. 237–242 (2014)

How to cite this article: Yuan, H., et al.: Analysis of outage performance in a 6G-V2X communications system utilising free-space optical quantum key distribution. *IET Quant. Comm.* 1–9 (2023). <https://doi.org/10.1049/qt2.12067>