Kufa Journal of Engineering
Vol. 16, No. 4, October 2025, P.P. 353-373
Article history: Received 1 November 2024, last revised 2 February 2025, accepted 2 February 2025

SIMULATION FOR PERFORMANCE EVALUATION OF SATELLITE-BASED QUANTUM COMMUNICATION SYSTEM

Adil Fadhil Mushatet[1], Shelan Khasro Tawfeeq[2] and Axel Sikora [3]

[1] Lec. Dr., Department of Information and Communication Engineering, Al-Khwarizmi College of Engineering, Baghdad University, Baghdad, Iraq, Email:adilfadhil@kecbu.uobaghdad.edu.iq

[2] Assist. Prof. Dr., Engineering and Industrial Applications Branch, Institute of Laser for Postgraduate Studies, University of Baghdad, Baghdad, Iraq, Email:shelan.khasro@ilps.uobaghdad.edu.iq

[3] Prof.Dr., Institute Reliable Embedded Systems and Communication Electronics (ivESK), Offenburg University, Germany, Email:axel.sikora@hs-offenburg.de

https://doi.org/10.30572/2018/KJE/160420

ABSTRACT

The selection and assessment of single-photon detection modules is a crucial problem in satellite-based QKD systems. The system's overall efficiency, secure key rate and quantum bit error rate are all significantly influenced by single-photon detection modules. There is a knowledge gap about the practical performance of commercially available single-photon detectors because existing research frequently relies on theoretical characteristics. This paper introduces a study on the effect of the parameters of three commercial single photon detection modules from ID Quantique company: ID Qube, ID100, and ID281 on certain Bennett-Brassard 1984 protocol parameters such as secure key rate, mean photon number per pulse, quantum bit error rate, link efficiency and zenith angle with the presence of link and geometrical losses for a downlink geostationary satellite. The study accounts for link and geometrical losses, zenith angle, and mean photon number per pulse. Results indicate that the ID281 detector outperforms the other two in maintaining a better secure key rate and quantum bit error rate, while ID100 shows superior performance in shorter wavelength ranges suitable for downlink operations. The findings suggest that global quantum key distribution coverage is achievable using geostationary satellites. To the best of our knowledge, there has been no prior study that has introduced using real parameters of commercial SPDMs to evaluate secure key rate for quantum key distribution systems based on downlink geostationary satellite.

KEYWORDS

Geometrical loss, Quantum key distribution, Satellite systems, Secure key rate, Single photon detector.

1. INTRODUCTION

In the quest for secure communication in an increasingly interconnected world, quantum key distribution (QKD) has revolutionized the field of cryptography by enabling the secure transmission of cryptographic keys based on the principles of quantum mechanics. The inherent properties of quantum physics, including the uncertainty principle and the no-cloning theorem, provide a robust framework for generating secure keys that can be invulnerable to eavesdropping and interception (C. Bennett and G. Brassard, 1984).

Utilizing the foundational ideas of quantum physics, quantum cryptography also known as QKD ensures secure key creation. The foundation of quantum cryptography's security is in the inability to foresee the potential values of a second non-commuting observable following the measurement of the first quantum observable. Bennett and Brassard created the BB84 protocol for secure key exchange in 1984 as a result of this observation. (C. Bennett and G. Brassard, 1984; Z. Eskandari and M. Rezaee, 2021). In the ideal case of BB84 protocol, Alice (one party) prepares a series of single photons, and photon polarizations are selected at random from four non-orthogonal states (e.g., horizontal (H)/vertical (V), and ±45◦). Bob, the second party, receives the photons and uses a randomly selected basis (such as H/V or ±45◦) to analyze each detected photon's polarization. Following that, the bases selected by each party are publicly compared, and the events where they used different bases are eliminated. (H. Weier et al., 2006).

The first successful implementation of QKD was deployed in 1989 (C. Bennett et al., 1992). Additionally, great successful projects of QKD network were implemented, such as DARPA Quantum Network (Elliott et al., 2005) Vienna SECOQC QKD Network (Peev et al., 2009), and Tokyo QKD Network (Sasaki et al., 2011). Over the years, various implementations of QKD have been explored, each with its advantages and limitations. One of the most promising approaches is satellite-based QKD, which utilizes the unique capabilities of satellites to achieve secure communication over vast distances. The first successful satellite-based QKD experiment performed in the Chinese satellite Micius into orbit at a height of about 500 kilometers at 850 nm wavelength with polarization encoding which was dedicated to quantum science experiments (Liao et al., 2017; H. Lo, X. Ma, and K. Chen, 2005).

A significant experiment of satellite-based entanglement dispersal across 1200 kilometers was conducted after this work (Yin et al., 2017). According to Liao et al., the Micius satellite suggests a practical way to create a secret key for an ultralong-distance global quantum network, where China and Europe can hold video conferences at 7600 km apart on Earth (Ren et al., 2017; Liao et al., 2018).

Extensive research was conducted including downlink and uplink setups with satellites at different zenith angles and altitudes under the effect of diffraction, extinction, background noise, and fading while accounting for atmospheric turbulence and pointing problems. Later, reconfigurable finite-size secret key rates have been achieved through continuous-variable quantum key distribution protocols, both for downlink and uplink setups (A. Khaleel, and S. Tawfeeq, 2018; S. Pirandola, 2021).

Furthermore, advances in satellite technology have facilitated the deployment of small-satellite-based QKD and CubeSat-based pathfinder missions for QKD applications such as CQT-Sat, UK-QUARC-ROKS, and QEYSSat, to generate secret keys even in instances of great loss. One significant obstacle for LEO satellites is the limited window of opportunity for setting up and maintaining a quantum channel with an optical ground station which limits the volume of safe keys that can be produced (Villar et al., 2021; Islam et al., 2024). A recent study by Vu et al. presented a novel satellite-based FSO/QKD system that uses LEO and GEO satellites supporting multiple wireless users (Q. Minh et al., 2023).

The selection and assessment of single-photon detection modules is a crucial problem in satellite-based QKD systems. The system's overall efficiency, secure key rate and quantum bit error rate are all significantly influenced by single-photon detection modules. There is a knowledge gap about the practical performance of commercially available single-photon detectors because existing research frequently relies on theoretical characteristics.

This paper presents a study on the BB84 QKD performance comparison based on the parameters that affect the secure key rate (R_{SK}) and quantum bit error rate (QBER) in the presence of the geometrical losses. The study focuses on utilizing the parameters of three commercial types of single-photon detection modules (SPDMs) to evaluate R_{SK} for QKD systems based downlink GEO satellite. These SPDMs are chosen from ID Quantique: ID Qube, λ : 900-1700nm (cooled InGaAs/InP avalanche photodiode), ID100, λ : 350-900nm (silicon avalanche photodiode), and ID281, λ : > 550- < 2000nm (superconducting nanowire single-photon detector (SNSPDs)). To the best of our knowledge, there has been no prior study that has introduced using real parameters of commercial SPDMs to evaluate secure key rate for quantum key distribution systems based on downlink geostationary satellite. This study examines the viability of a downlink GEO satellite configuration for global QKD networks, in contrast to many other studies that concentrate on LEO or MEO satellites. In addition, contributes to more robust system design considerations by assessing the effects of severe connection losses and zenith angles up to ±50° and understanding the wavelength-dependent

behaviors by including a broad spectral range (350 nm–1900 nm), which offers crucial information for upcoming satellite-based QKD designs.

2. SATELLITE-BASED QKD SYSTEMS

As quantum communication by ground-based fiber networks has considerable distance limitations, satellite-based QKD is a feasible way to expand these networks across global distances. The two best choices for satellite QKD applications are LEO and GEO orbits. GEO satellites offer significant advantages over LEO because GEO satellites are visible to ground observers at a fixed point in the sky due to their circular geosynchronous orbit, which is located 35,786 km above Earth's equator thus the satellite, require very little tracking from ground stations communicating with them. On the other hand, satellites in LEO —2000 km or below— pass through at least ten orbits every day. Furthermore, because of their broad coverage over pertinent terrestrial areas and high link availability (weather allowing), GEO satellites have a clear advantage over LEO satellites when it comes to delivering QKD services from space. (P. Hajipour, and A. Shahzadi, 2017; Dirks et al., 2021).

Since polarization encoding of individual photons is best suited for free-space communication, satellite QKD usually uses it. The photons are obtained from polarization-entangled photon-pair sources or weak coherent pulse sources when utilizing polarization encoding (R. Bedington et al., 2017). The majority of BB84 schemes use weak coherent pulse sources that have seen significant design advancements in order to produce photons. One of the limitations to the development of high-speed BB84 schemes was the requirement for active polarization adjustment, which requires a lot of power and slow. One solution that got around this restriction used four laser diodes inside of a single transmitter each one with a unique polarization state (R. Bedington et al., 2017). This method's disadvantage is that the diodes' spectra aren't always the same, opening up a potential side channel for eavesdroppers. Variable power lasers, which might also be able to serve as a laser beacon, could be used in an alternate design. For more information about the satellite QKD systems using different light sources with polarization-encoding see (R. Bedington et al., 2017).

The optical link between the satellite and the ground station using a telescope to guide the photons source at the transmitter and at the receiver. Since the links have the most losses, they have the greatest impact on the QBER. (Aspelmeyer et al., 2003). When the downlink arrangement is used, diffraction losses increase with the inverse square of wavelength and are influenced by the telescope's design and beam spatial mode essentially accounts for the majority of optical loss. In contrast, in the uplink configuration, atmospheric turbulence which decreases

with increasing wavelength has a substantially larger effect, adding over 20 dB of loss. Selecting between transmitting and reflecting telescopes is a trade-off when building the telescope optics. Larger reflective mirrors are possible, but caution must be used when using polarization-based QKD to avoid significant depolarization effects. Reflector telescope secondary mirrors are frequently positioned in the beam's path to partially obscure the primary mirror and impact diffraction spreading. In addition to stray light, the optical signal that reaches the receiving detectors consists of QKD photons. In addition to being combined with dark counts, the detector output is regarded as a raw key that needs to be processed in order to create a private encryption key (Aspelmeyer et al., 2003).

The type of SPD is one of the most important factors influencing the performance of any QKD systems, including satellite-based systems. Given that the quantum non-cloning theorem states that the optical signal cannot be increased in comparison to classical light signals, the SPD must have high detection efficiency and a low dark count rate in order to ensure the high fidelity of the single photon during transmission (Yang et al., 2019).

Avalanche photodiodes (APDs), SNSPDs, and photomultiplier tubes (PMTs) are examples of SPDs that are commonly employed in QKD. The wavelength employed in satellite-based QKD is close to 800 nm. PMTs have low detection effectiveness (less than 10%) at this wavelength, and SNSPDs need large, heavy cryocoolers. On the other hand, inexpensive and small silicon-based APDs are better suited for satellite-based QKD since they have a detection effectiveness of about 65% at the 800 nm wavelength (Yang et al., 2019). SNSPDs are an emerging technology with great potential to advance QKD and quantum technology, including single-photon detection and advanced photon-counting applications (A. Mushatet, and S. Tawfeeq, 2019).

SNSPDs have been demonstrated in a variety of applications, such as QKD and satellite laser range, and are superior to semiconductor detectors because of their higher system detection efficiency, lower dark count rates, and lower timing jitter (O. Lee, and T. Vergoossen, 2019; You et al., 2018). SNSPDs are currently limited by cooling technologies, and all previous experimental demonstrations were ground-based applications. This limits SNSPD application to downlink satellite-QKD where photon detectors are located at one of the ground stations. Moreover, current development in SNSPDs allow them to operate in space can allow them to be incorporated in a greater variety of satellite-based QKD systems (You et al., 2018).

To exchange quantum encryption keys between earth and space, the photon source can be located either in space or on the ground as shown in Fig. 1 which illustrates the possible satellite-based QKD options (Bedington et al., 2016). When photons are steered from space to

ground i.e. down-link, the turbulence in the atmosphere has less effect on the optical transmission channel as compared with steering the photons from the ground to space i.e. up-link because of the reduced thickness of the atmosphere close to earth's surface, optical link losses are reduced (Bourgoin et al., 2014).

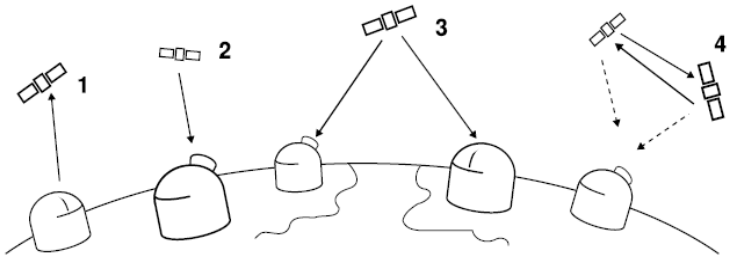

Fig. 1. Options for possible satellite-based QKD implementations. 1. Ground-to-space, where the photon source is on the ground and the satellite only carries detectors. 2. Space-to-ground, where the satellite carries a source and detectors. 3. A platform for entangled photon sources at the satellite. 4. Inter-satellite QKD is the building block for a long baseline test of quantum correlations (Bedington et al., 2016)

In the event that two ground stations choose to share the keys through choices 1 or 2 of Fig 1, the satellites must be believed to be safe key exchanging nodes. The trust requirement is waived for option 3, however, when entanglement-based QKD is used, as only Alice and Bob will be aware of the polarizations and the generated key is private if one photon of each generated pair of photons is directed to Alice (at the ground station) and the other photon of the pair is directed to Bob (at the other ground station) (Bedington et al., 2016). Bell violation test can be used in entanglement-based QKD to ensure key security (A. Ekert, 1991). Due to the requirement that ground stations be concurrently within the satellite's field of view and the fact that both photons in a pair are traveling along high-loss paths, there is very little chance that both photons in a pair will reach their ground stations, this protocol's key generation rate is extremely slow. Option 4 represents inter-satellite QKD (Bedington et al., 2016).

3. THEORETICAL PART

Various performance metrics are defined to quantify the efficiency and readability of the proposed system. The performance of QKD systems can be studied by evaluating R_{SK} with different factors that affect the performance of the system, such as mean photon number per pulse (μ), QBER, link efficiency (η), geometrical losses, and SPDMs parameters. Mainly, weak coherent pulses are used in practical quantum communication experiments to prepare single photons, with a nonzero probability of creating multiphoton states.

Eve, the eavesdropper, might launch a photon-number-splitting (PNS) attack using multiphoton pulses. She can split, store, and measure a photon from the multiphoton pulse on the proper

basis once Alice and Bob's bases are made public. Eve won't cause any noise in the channel if she sends Bob the remaining multiphoton pulse, allowing for the full bit's information to be retrieved without being detected. Tagged bits are those that have disclosed information to the listener. In this case, it is still possible to distill a secure key and determine the key generation rate by (C. Bonato, 2009; Etengu et al., 2011):

$$R_{SK} \geq \frac{S}{2}[(1-\Delta) - f(QBER)H_2(QBER) - (1-\Delta)H_2(QBER/(1-\Delta))] \quad (1)$$

Where S is the probability that Bob detects a non-empty pulse and it is equal to 1 for BB84 protocol, $f(QBER)$ is the efficiency of error correction. $f(QBER)$ is equal to 1.16 for the best-known performing algorithms with $f(QBER) \leq 5$ (A. Khaleel, and S. Tawfeeq, 2018; E. Waks et al., 2022), $H_2(x)$ is the binary entropy function:

$H_2(x) = -xlog_2(x) - (1-x)\ log_2(1-x)$, and Δ is the fraction of tagged bits.

The fraction of multiphoton pulses over the fraction of non-empty pulses detected by Bob is defined as (C. Bonato et al., 2009):

$$\Delta \approx \frac{\mathbf{1-e^{-\mu}-\mu e^{-\mu}}}{\mathbf{1-e^{-\eta\mu}}} \quad (2)$$

$\boldsymbol{\eta}$ includes attenuation of the atmosphere and pointing losses,

$$\eta = \eta_0(1 - e^{-\frac{2R^2}{W_{LT}^2}}) \quad (3)$$

η_0 is the empirical value equal to 0.1, w_{LT} is the long-term beam width and R is the radius of the receiving telescope.

η can be found by the ratio of the power measured at the receiver point to the total power sent from the transmitter and is expressed by (C. Zhang et al., 2020):

$$\frac{P_r}{P_t} = 20\ log\frac{{D_r}^2 D_t}{{D_r}^2 + 2.44mL\lambda} \quad (4)$$

Where,

P_t is the laser power before the transmitting telescope main mirror

P_r is the power measured at the receiver point

D_t is the transmitter aperture diameter

D_r is the receiver aperture diameter

L is the link distance

λ is the wavelength

m is introduced to indicate the degree to which the laser beam's real far-field divergence angle resembles the theoretically ideal case determined as: $(\frac{2.44\lambda}{D_t})$.

The zenith angle (Z_θ) greatly affects η. Accordingly, ground-to-satellite (and satellite-to-ground) link, η can be determined by (Etengu et al., 2011):

$$\eta = T_0^{Z_\theta} \quad (5)$$

Where T_0 is the atmospheric transmission at Z_θ for the ground-to-satellite direction.

4. SIMULATION OF SATELLITE-BASED QKD SYSTEMS STATE OF THE ART

The advantages of the satellite-based QKD systems motivate academics and funding organizations to sponsor research articles on this emerging technology in order to increase investment in it. In Feb 2024, V Marulanda Acosta, et al. reported a paper discusses the investigation of the function of adaptive optics in this optimization, concentrating on practical baseline configurations of the prepare-and-measure quantum key distribution that incorporate finite-size effects and both discrete and continuous-variable encoding. The analysis used allows for estimating the secret key rate for a range of critical parameters, including turbulence strength, satellite altitude, and ground telescope diameter by modeling the coupled signal statistics following a wavefront distortion correction with adaptive optics using existing experimental turbulence datasets, both during the day and at night (Acosta et al., 2024). Aristeidis Stathis, et al. using BB84 protocol at 1550 nm, this article highlights the advantages and difficulties of combining satellite-based QKD with current terrestrial networks, providing a thorough technical and feasibility analysis to estimate R_{SK} based on various operational situations, such as variable telescope apertures and detection methods for LEO, MEO, and GEO satellite orbits (Stathis et al., 2024). Davide Orsucci, et al. present a comprehensive assessment that outlines the benefits and drawbacks of the state-of-the-art satellite QKD technologies and offers recommendations for future system architectures that strive for safe worldwide quantum communication. This study comes to the conclusion that the most feasible protocol for near-term satellite QKD implementations is the BB84 protocol, which makes use of trusted nodes and downlink configurations (Orsucci et al., 2024). In 2023, Aleksandr V. Khmelev, et al. model provides important insights for upcoming quantum communication technologies and provides a useful tool for assessing and improving satellite-to-ground QKD systems. Results from the Chinese Micius satellite were used to validate atmospheric extinction data that were obtained in clear and cloudy conditions. The 300 mm and 600 mm aperture telescope QKD links are simulated by this model (Khmelev et al., 2023). For Abhishek Khanna, et al. work, a numerical simulation QBER model offers an all-inclusive instrument for examining and developing upcoming satellite-based QKD systems, assisting engineers in maximizing efficiency and guaranteeing safe communication. The authors point out that limiting errors and optimizing QBER depend heavily on system components such telescope aperture size, field of view, and the usage of adaptive optics. Particular suggestions are made for preserving secure

quantum communication channels and enhancing system performance (A. Khanna et al., 2024). Junyong Wang, et al. reported a paper that finds a worldwide QKD network's performance may be greatly improved by carefully optimizing satellite constellations and orbital characteristics. Future research might concentrate on adding more sophisticated inter-satellite links technology and expanding to several orbital planes (J. Wanga et al., 2021). Keshav Kasliwal et al., work focuses on the use of QKD to improve satellite-to-ground communication using LEO orbit as follows, the model covers the various types of losses that occur during transmission through the environment, such as geometric, pointing, and atmospheric losses. Adaptive optics is one method that helps lower these losses. By examining R_{SK} at varying channel losses, it is found that the key rate is greatly reduced at larger channel losses and the QBER saturates at 0.5. The study simulates diffraction loss and beam dispersion over distance, emphasizing that geometric losses are minimized by bigger transmitter and receiver apertures. In comparison to the BB84 protocol, a thorough comparative investigation reveals that Decoy BB84 can withstand higher channel losses (up to 45 dB), which makes it more appropriate for long-distance satellite communication. Finally, an analysis between the zenith angle and the key rate reveals that as the zenith angle rises, the key rate falls (K. Kasliwal et al., 2023). The subject of Chunmei Zhang et al study (C. Zhang et al., 2020) is the analysis of link loss in a downlink QKD satellite. Some important factors have been considered for analysis including geometric losses, atmospheric losses, and losses resulting from the system architecture (e.g., telescope structure, pointing and tracking errors, and single-photon detectors). The main results can be illustrated as follows; the primary cause of a link loss resulting from beam spreading between the satellite and the ground station is a geometric loss. The size of the telescope's aperture was discovered to be critical in reducing these losses. Greater aperture diameters, for example, lessen geometric loss and beam divergence. In addition, rain and aerosols are two weather-related factors that significantly affect atmospheric loss and the quantum link. The findings indicate that visibility is crucial, with rural locations performing better in terms of transmission than urban or marine settings. Evaluations were conducted on tracking, pointing, and acquisition system losses, single-photon detector efficiency, and telescope obstruction losses. For instance, the central obstruction of a conventional Cassegrain telescope structure results in a loss of -1.6 dB, whilst the detection efficiency of single-photon detectors adds approximately a -2.21 dB loss. The total loss was calculated to be roughly -35 dB for a CubeSat system operating at 780 nm wavelength, 500 km altitude, 8 cm transmitting aperture, and 70 cm receiving aperture. This value is used as a reference for evaluating QKD protocol performance. The 500 MHz decoy state BB84 protocol obtained a R_{SK} of about 4 kbps. In contrast, the R_{SK} of the 1MHz

entanglement E91 protocol, was far lower at 0.02 bps. Both protocols kept their QBERs below 0.01 (C. Zhang et al., 2020).

4.1. The Simulation Process Flow

In this section, the structuring flow of the simulation model is explained. The proposed algorithm is given in Fig. 2, where the following definitions hold:

1. Start the process.
2. Variables initialization, such as μ, dark counts, detector efficiency, $f(QBER)$, η_0, and S.
3. Functions definitions: some functions are to be calculated;$H_2(QBER)$, $H_2(QBER/(1-\Delta))$, efficiency, etc. are defined.
4. Looping: for each different set of parameters e.g. dark counts, some values are calculated repeatedly such as, η, gain, $QBER$ and R_{SK}.
5. Parameters checking: repeat the loop if there are more parameters that need to be calculated e.g. geometrical loss, otherwise, end the process.
6. End.

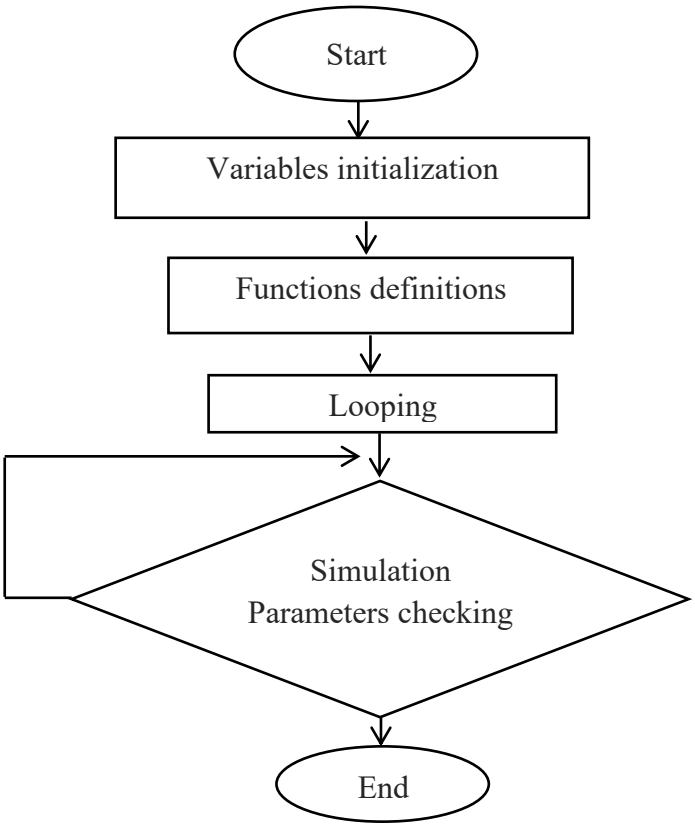

Fig. 2. Simulation process steps

4.2. Simulation Setup

In this study, Matlab simulation software was used to evaluate the performance of the proposed system. Several simulation parameters are carefully defined to capture and evaluate the

quantum communication in a satellite systems context. The simulation parameters of the modeled downlink GEO-QKD satellite based on the BB84 protocol are listed below in Table1. Regarding the parameters related to the quantum channel, attenuation due to atmospheric turbulence is considered.

Table 1. Simulation Parameters of The Modeled Downlink Geo - Qkd Satellite Based On Bb84 Protocol

Parameter	Value
L	40000 km
Encoding Type	Polarization Encoding
μ	0.1
λ	350-1900 nm
m	1
D_t	0.3 m
D_r	1 m
Dark counts (c/s)	IDQube ID100 ID281 6×10^{-5} 6×10^{-6} 6×10^{-8}

5. RESULTS AND DISCUSSION

Depending on the parameters listed in Table 1, the effects of QBER, μ, m, η and Z_θ on R_{SK} were studied. Our simulation results have been compared to other published theoretical results, specifically, (K. Kasliwal et al., 2023) and (C. Zhang et al., 2020). Fig. 3. illustrates that all SPDMs tend to reduce R_{SK} as the QBER increases it indicates more errors in the transmitting quantum bits hence leading to an increase the effect of eve by gaining some of the transmitted key. Thus additional error correction and privacy amplification steps are required which as a result reduce the final generated key rate. On the other hand, for a specific R_{SK} ID281 offers lower QBER compared to ID100 and ID Qube due to its lower dark counts and noise characteristics and higher detection efficiency in comparison with the other SPAD types which have higher dark counts and afterpulsing effects which can represent additional error sources. To make a comparison, the model presented in (K. Kasliwal et al., 2023) will be compared to our simulated data in terms of the calculated QBER range. Table 2. Lists the parameters used in our study against (K. Kasliwal et al., 2023) model.

Table 2. The Parameters Used For R_{SK} With Qber Comparison With (K. Kasliwal Et Al., 2023)

Parameter	(K. Kasliwal et al., 2023)	Modeled data
L (km)	500	40000
μ	0.1	0.1
Dark counts (c/s)	10^{-3}	0.66×10^{-8}

Referring to (K. Kasliwal et al., 2023) and our results, all QBER values are considerably far lower than the established threshold of 15% due to the used lower dark counts and μ which will lead to an increase in the photon detection probability leading to less interference and low

QBER indicating that the system is appropriate for the GEO secure QKD system. A comparable QBER values with (K. Kasliwal et al., 2023) despite the difference in the orbit distance used is due to the noticeable difference in the dark counts used as shown in Table 2. For each type of SPDM, there is a range for the values of μ that gives the highest value of R_{SK}. As the value of the dark count rate decreases, μ can be varied for a longer range giving a higherR_{SK}. This is clear in Fig. 4. , where ID281 can operate effectively over a wide range of μ due to its high efficiency and low noise characteristics which give the highest R_{SK} for long-range of μ. In contrast, at low μ IDQube and ID100 exhibit reduced R_{SK} due to factors such as dark count rates and afterpulsing effects, which become more significant relative to the weak incoming signal. Thus, ID281 outperforms ID Qube and ID100 in terms of R_{SK} versus μ, particularly in low-light conditions. In addition, it is noticed that all SPDMs reach the highest value of R_{SK} at the same value of μ which is approximately equal to 0.4.

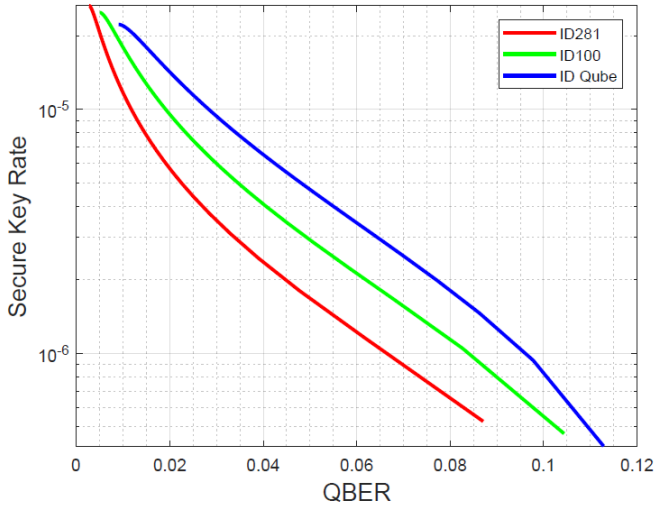

Fig. 3. Secure Key Rate With Qber

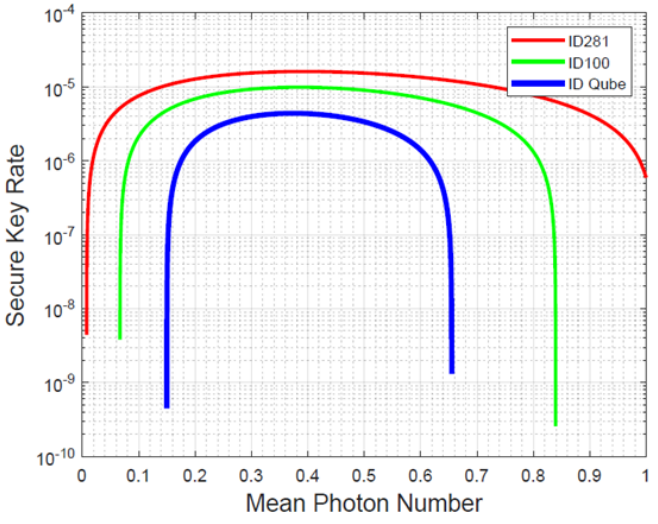

Fig. 4. Secure key rate with mean photon number

The effect of the link loss on R_{SK} is also tested. Fig. 5 shows that using ID281 gives the highest R_{SK} and is the most tolerant SPDM even in the presence of substantial link loss. IDQube and ID100 show a reduction in R_{SK} with increasing link loss in response to their higher dark counts and decreased detection efficiency under low signal conditions.

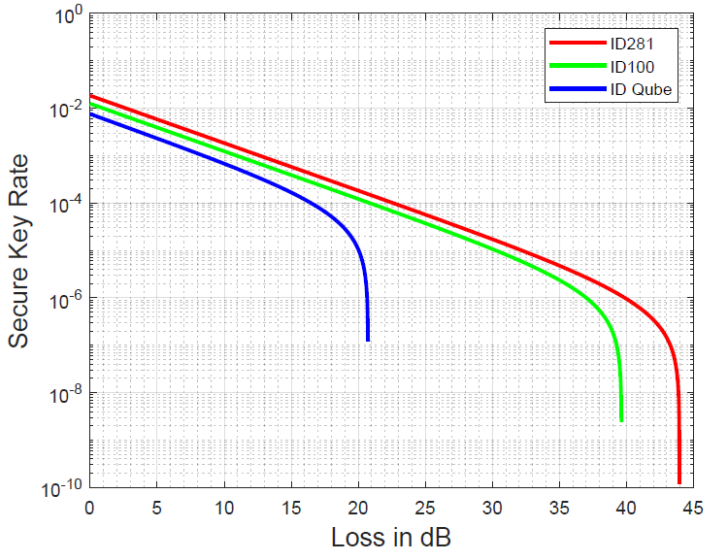

Fig. 5. Secure key rate with link loss

For a comparison between our simulated data with (K. Kasliwal et al., 2023) in terms of R_{SK} as a function of channel losses, the parameters that are used for both studies are listed in Table 3.

Table 3. The Parameters Used For R_{SK} With Link Loss Comparison With (K. Kasliwal Et Al., 2023)

Parameter	(K. Kasliwal et al., 2023)	Modeled data
L (km)	500	40000
μ	0.4	0.1
Dark counts (c/s)	10^{-3}	0.66×10^{-8}

Table 4 lists our collected R_{SK} in bits/s as a function of channel loss against (K. Kasliwal et al., 2023) model.

Table 4. A Comparison Between (K. Kasliwal Et Al., 2023) And Modeled Models In Terms Of R_{SK} Against Link Loss.

Link Loss (dB)	R_{SK} (kbit/s) (K. Kasliwal et al., 2023)	R_{SK} (kbit/s) Modeled
-35	0.1	1
-30	1	10
-20	10	100
-10	100	1000

It can be seen from the Table.4 our collected R_{SK} is higher than what was obtained in (K. Kasliwal et al., 2023) in spite of the difference in the orbit distance used. The reason is also due to the difference in the dark counts used as well as the noticeable difference in μ. This

difference in these parameters will lead to increase the key detection rate in our simulated data compared to (K. Kasliwal et al., 2023).

The effect of the zenith angle which is the angle between a point on the Earth's surface and the vertical (or zenith) direction, affects the optical signal path length through the Earth's atmosphere on the R_{SK} is analyzed as depicted in Fig. 6, the relationship between R_{SK} and zenith angle is influenced by atmospheric attenuation, signal, and background noise. Higher zenith angles result in increased atmospheric attenuation and background noise levels, which can reduce R_{SK}.

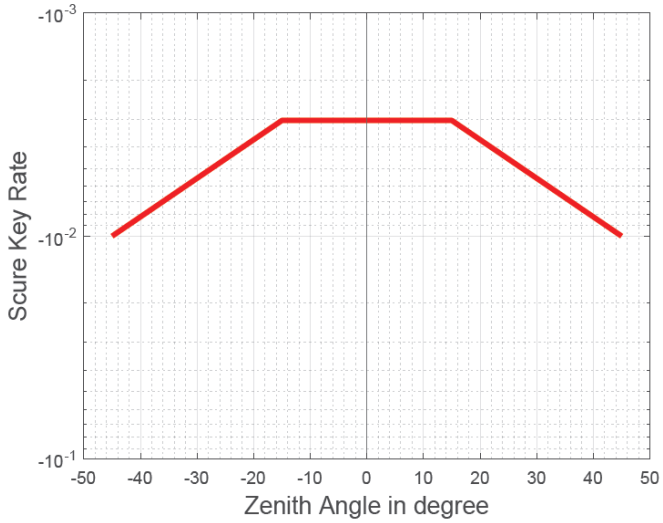

Fig. 6. Secure key rate with zenith angle

The correctness of this point can be tested using the data reported in (K. Kasliwal et al., 2023). The zenith angle range used in (K. Kasliwal et al., 2023) is extended from (-2 to 2) rad. where's in our simulated data is extended from (-50 to 50) deg. The input parameters are almost identical between both simulations except L and μ. In (K. Kasliwal et al., 2023), L = 500 km and μ= 0.3. Where's we used L = 40000 km and μ= 0.1. The overall performance is identical for both simulations in which R_{SK} is maximum at θ= 0 .i.e. the satellite is above the ground station. In contrast, R_{SK} decreases as the satellite goes toward the horizon .i.e. increase in zenith angle.

The spectral range used in this work is between 350nm to 1900nm which represents the range of operation for the SPDMs used in our analysis. Fig. 7. Shows that longer wavelengths give higher link loss for all SPDMs used in this study as these wavelengths are more susceptible to scattering and absorption phenomena in the atmosphere. As shown in this figure, ID100 which operates within the range of (350-900nm) generally outperforms ID281 & IDQube in terms of geometric link loss tolerance and wavelength sensitivity. Although ID100 has narrower wavelength range compared to ID281 & IDQube, it is optimized for a specific wavelength for downlink channel operation which is around 670nm.

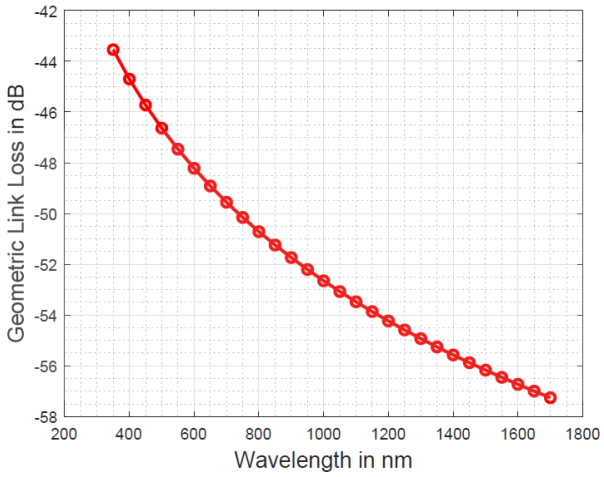

Fig. 7. Geometric link loss with wavelength

Table 5 represents the results illustrated in (C.Zhang et al., 2020) and our obtained data in terms of geometric link loss as a function of λ. Table 6 represents the main parameters that are used for both studies. The difference between the modeled results and (C.Zhang et al., 2020) results is due to the type of the satellite orbit and the type of the SPAD modules that are used for both simulations.

Table 5 A Comparison Between (C.Zhang Et Al., 2020) And Modeled Models In Terms of Λ Against Geometric Link Loss

λ(nm)	Geometric link loss (dB) (C.Zhang et al., 2020)	Geometric link loss (dB) Modeled
500	-10	-47
1000	-15.2	-52.5
1500	-19	-56
2000	-20	-57

Table 6 The Parameters Used For Λ Against Geometric Link Loss Comparison With (C.Zhang Et Al., 2020)

Parameter	(C.Zhang et al., 2020)	Modeled
L (km)	500	40000
D_t (m)	0.3	0.3
D_r (m)	1	1
λ (nm)	780	780

Furthermore, the geometric link loss was also studied with the beam quality factor, m, for ID281 and IDQube (their maximum detection efficiency @1550nm) and for ID100 (its maximum detection efficiency @500nm). Fig.8 shows that the ID281 and ID Qube have the same response with the beam quality factor compared to ID100. It is clear from this figure, at these specific wavelengths ID100 less sensitive to variations in beam quality in terms of mode matching and beam divergence and aberrations compared to ID281 and IDQube as their maximum detection

efficiency @1550nm are more susceptible to scattering and absorption phenomena in the atmosphere which signifies deviations from ideal Gaussian laser beam.

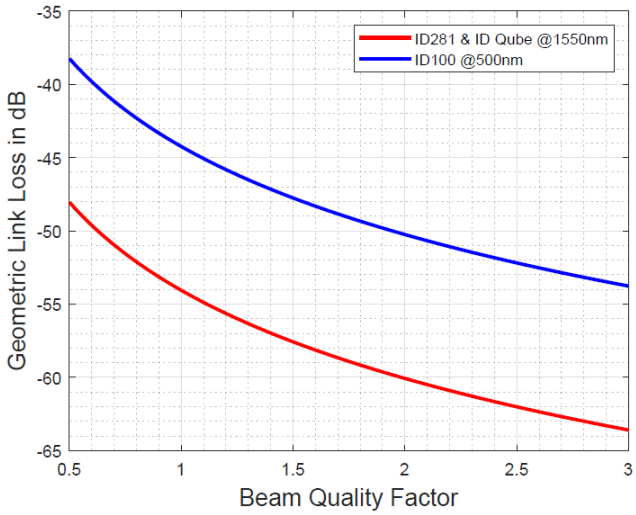

Fig.8. Geometric link loss with beam quality factor

For validation purpose, Table 7 represents the data reported in (C.Zhang et al., 2020) and our obtained data in terms of geometric link loss as a function of beam quality factor. The parameters that are used in Table.6 is also used in this part. Due to the type of the satellite orbit and the type of the SPAD modules that are used for both simulations, our obtained system results exhibit high losses compared to (C.Zhang et al., 2020).

Table.7 A Comparison Between (C.Zhang Et Al., 2020) And Modeled Models In Terms of Beam Quality Factor Against Geometric Link Loss.

Beam quality factor	Geometric link loss (dB) (C.Zhang et al., 2020)	Geometric link loss(dB) Modeled
0.5	-7	-38
1	-11	-44
1.5	-14	-47
2	-16	-50

6. CONCLUSION

In this work, an estimation of the secure key rate for the QKD- BB84 protocol based downlink geostationary satellite was investigated, considering the parameters of three commercial single photon detection modules from ID Quantique company: IDQube, ID100, and ID128. Link loss, mean photon number per pulse, quantum bit error rate, link efficiency, zenith angle, and geometrical losses were also considered to determine the secure key rate. For comparing between different single photon detection modules which differ in detection mechanism involves understanding their respective characteristics and limitations. Results show that the ID281 module which its operations based on the superconducting properties of nanowires

allowing it to detect photons with high detection efficiency and low dark count rate is preferable on ID100 and IDQube in terms of keeping up a better secure key rate and quantum bit error rate under different conditions of μ and link loss. In contrast, ID100 which its operation based on avalanche multiplication phenomena in semiconductors outperforms ID281 and IDQube in terms of it has a better performance for a shorter wavelength range which is preferable for downlink operation. In summary, the choice between the different IDQ modules requires a trade-off between the required secure key rate and the allowable link loss. Different factors such as environmental conditions and communication requirements will play an important role in this choice.

7. REFERENCES

Acosta et al. (2024) 'Analysis of satellite-to-ground quantum key distribution with adaptive optics', New Journal of Physics, 26, 023039. https://doi.org/10.1088/1367-2630/ad231c.

Aspelmeyer et al. (2003) 'Long-Distance Quantum Communication with Entangled Photons Using Satellites', IEEE Journal of Selected Topics in Quantum Electronics, 9 (6), pp.1541-1551.https://ieeexplore.ieee.org/abstract/document/1263786/similar#similar.

Bedington et al. (2016) 'Nanosatellite experiments to enable future space-based QKD missions', EPJ Quantum Technology, 3. https://doi.org/10.1140/epjqt/s40507-016-0051-7.

Bedington, R., Arrazola, J. and Ling, A. (2017) 'Progress in satellite quantum key distribution', npj Quantum Information, 3. https://doi.org/10.1038/s41534-017-0031-5.

Bennett, C. and Brassard, G. (1984) 'Quantum Cryptography: Public Key Distribution and Coin Tossing', In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp.175-179. http://dx.doi.org/10.1016/j.tcs.2011.08.039.

Bennett, C. et al. (1992) 'Experimental Quantum Cryptography', Journal of Cryptology, 5, pp. 3-28.

Bonato, C. et al. (2009) 'Feasibility of satellite quantum key distribution', New Journal of Physics, 11, 11045017. https://doi.org/10.1088/1367-2630/11/4/045017.

Bourgoin et al. (2014) 'A comprehensive design and performance analysis of low Earth orbit satellite quantum communication', New Journal of Physics, 16, 069502. https://doi.org/10.1088/1367-2630/16/6/069502.

Dirks et al. (2021) ‘quantum key distribution from a geostationary satellite’, in Proceedings of SPIE 11852, International Conference on Space Optics — ICSO, 118520J. https://doi.org/10.1117/12.2599164.

Ekert, A. (1991) ‘Quantum Cryptography Based on Bell's Theorem’, Physical ReviewLetter, 67, pp. 661-663. https://link.aps.org/doi/10.1103/PhysRevLett.67.661.

Elliott et al. (2005) ‘Current status of the DARPA Quantum Network’ in Proceedings of SPIE 5815, Quantum Information and Computation III, Orlando, Florida, United States, pp.138-149. https://doi.org/10.1117/12.606489.

Eskandari, Z. and Rezaee, M. (2021) ‘Error reconciliation based on integer linear programming in quantum key distribution’, Journal of Information Systems and Telecommunication, 9, pp. 51–59. https://doi.org/10.52547/jist.9.36.51.

Etengu et al. (2011) ‘Performance Comparison of BB84 and B92 Satellite-Based Free Space Quantum Optical Communication Systems in the Presence of Channel Effects’, Journal of Optical Communication, 32, pp. 37-47. https://doi.org/10.1515/JOC.2011.007

Hajipour, P. and Shahzadi, A. (2017) ‘Analysis of Imperfect Space Channel for the Next Generation Satellite Networks’, Journal of Information Systems and Telecommunication, 5 (4), pp. 236-241. http://jist.ir/fa/Article/15016.

https://doi.org/10.1007/BF00191318.

Islam et al. (2024) ‘Finite resource performance of small satellite-based quantum key distribution missions’, Quantum Physics, 5, 03010. https://doi.org/10.1103/PRXQuantum.5.030101.

Kasliwal, K. et al. (2023) ‘Enhancing satellite-to-ground communication using quantum key distribution’, IET Quantum Communication, 4 (2), pp. 57-69. https://doi.org/10.1049/qtc2.12053.

Khaleel, A. and Tawfeeq, S. (2018) ‘Key rate estimation of measurement-device-independent quantum key distribution protocol in satellite-earth and intersatellite links’, International Journal of Quantum Information, 16 (3), 1850027. https://doi.org/10.1142/S0219749918500272

Khanna, A. et al. (2024) ‘Quantum BER estimation modelling and analysis for satellite-based quantum key distribution scenarios’, IET Quantum Communication, 5 (2), pp. 157-163. https://doi.org/10.1049/qtc2.12081.

Khmelev et al. (2023) ‘Semi-Empirical Satellite-to-Ground Quantum Key Distribution Model for Realistic Receivers’, Entropy, 25 (4). https://doi.org/10.3390/e25040670.

Lee, O. and Vergoossen, T. (2019) ‘An updated analysis of satellite quantum-key distribution missions’, arXiv:1909.13061v2 [quant-ph]. https://arxiv.org/abs/1909.13061.

Liao et al. (2017) ‘Satellite-to-ground quantum key distribution’, Nature, 549, pp. 43-47.https://doi.org/10.1038/nature23655.

Liao et al. (2018) ‘Satellite-Relayed Intercontinental Quantum Network’, Physical Review Letters, 120, 030501. https://doi.org/10.1103/PhysRevLett.120.030501.

Lo, H., Ma, X. and Chen, K. (2005) ‘Decoy State Quantum Key Distribution’, Physical Review Letters, 94, 230504. https://doi.org/10.1103/PhysRevLett.94.230504.

Minh, Q. et al. (2023) ‘Design of Satellite-Based FSO/QKD Systems using GEO/LEOs for Multiple Wireless Users’, IEEE Photonics Journal, 15 (4), 7303314. https://doi.org/10.1109/JPHOT.2023.3294723.

Mushatet, A. and Tawfeeq, S. (2019) ‘An efficient performance evaluation modeling tool for SNSPD used in QKD systems’, International Journal of Quantum Information, 17 (7), 1950059. https://doi.org/10.1142/S021974991950059X.

Orsucci et al. (2024) ‘Assessment of practical satellite quantum key distribution architectures for current and near-future mission’, arXiv:2404.05668v1 [quant-ph]. https://doi.org/10.48550/arXiv.2404.05668.

Peev et al. (2009) ‘The SECOQC quantum key distribution network in Vienna’, New Journal of Physics, 11, 075001. https://doi.org/10.1088/1367-2630/11/7/075001.

Pirandola, S. (2021) ’Satellite quantum communications: Fundamental bounds and practical security’, Physical Review Research, 3, 023130. https://doi.org/10.1103/PhysRevResearch.3.023130.

Ren et al. (2017) ‘Ground-to-satellite quantum teleportation’, Nature, 549, pp. 70-73.https://doi.org/10.1038/nature23675.

Sasaki et al. (2011) ‘Field test of quantum key distribution in the Tokyo QKD Network’, Optics Express, 19 (11), pp. 10387-10409. https://doi.org/10.1364/OE.19.010387.

Stathis et al. (2024) 'Toward Converged Satellite/Fiber 1550 nm DS-BB84 QKD Networks: Feasibility Analysis and System Requirements', Photonics, 11 (7). https://doi.org/10.3390/photonics11070609.

Villar et al. (2020) 'Entanglement demonstration on board a nano-satellite', Optica, 7 (7), pp.734-737. https://doi.org/10.1364/OPTICA.387306

Waks, E., Santori, C. and Yamamoto, Y. (2022) 'Security aspects of quantum key distribution with sub-Poisson light', Physical Review A, 66, 042315. https://doi.org/10.1103/PhysRevA.66.042315.

Wanga, J., Chena, H. and Zhua, Z. (2021) 'Modeling research of satellite-to-ground quantum key distribution constellations', Acta Astronautica, 180, pp. 470–481. https://doi.org/10.1016/j.actaastro.2020.12.039.

Weier, H. et al. (2006) 'Free space quantum key distribution: Towards a real life application', Fortschritte der Physik, 54 (8-10), pp. 840–845.https://doi.org/10.1002/prop.200610322.

Yang et al. (2019) 'Space borne low-noise single-photon detection for satellite-based quantum communications', Optics Express, 27 (25), pp. 36114-36128. https://doi.org/10.1364/OE.27.036114.

Yin et al., (2017) 'Satellite-based entanglement distribution over 1200 kilometers', Science, 356 (6343), pp. 1140–1144. https://www.science.org/doi/10.1126/science.aan3211

You et al. (2018) 'Superconducting nanowire single photon detection system for space applications', Optics Express, 26 (3), pp. 2965 – 2971. https://doi.org/10.1364/OE.26.002965.

Zhang, C. et al. (2020) 'Link loss analysis for a satellite quantum communication downlink', in Proceedings of SPIE 11540, Emerging Imaging and Sensing Technologies for Security and Defense V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defense III , United Kingdom. https://doi.org/10.1117/12.2573489.