IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 7, 2021, accepted December 17, 2021, date of publication December 21, 2021,
date of current version December 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3137357

Reliability and Security Analysis of an Entanglement-Based QKD Protocol in a Dynamic Ground-to-UAV FSO Communications System

NANCY ALSHAER[1], (Member, IEEE), AHMED MOAWAD[2], AND TAWFIK ISMAIL[2,3], (Senior Member, IEEE)

[1]Department of Electronics and Electrical Communication, Faculty of Engineering, Tanta University, Gharbiya 31527, Egypt
[2]Wireless Intelligent Networks Center (WINC), Nile University, Giza 12677, Egypt
[3]National Institute of Laser Enhanced Sciences, Cairo University, Giza 12613, Egypt

Corresponding author: Tawfik Ismail (tismail@cu.edu.eg)

This work was supported by the Science, Technology and Innovation Funding Authority (STIFA) of Egypt, under Grant 38121.

ABSTRACT Quantum cryptography is a promising technology that achieves unconditional security, which is essential to a wide range of sensitive applications. In contrast to optical fiber, the free-space optical (FSO) link is efficiently used as a quantum channel without affecting the polarization of transmitted photons. However, the FSO link has several impairments, such as atmospheric turbulence and pointing errors, which affect the performance of the quantum channel. This paper proposes a quantum key distribution (QKD) scheme that uses a time-bin entanglement protocol over the FSO channel that suffers from various channel impairments. Due to the interest in unmanned aerial vehicles (UAVs) and their usefulness for many social, internet-of-things (IoT), civil, and military applications, the proposed QKD-FSO system is integrated with the ground-to-UAV platform. Furthermore, variances in the position and orientation of the UAV are investigated using a tracking system. These variances are considered when evaluating the overall performance of the proposed integrated system. For this purpose, closed-form expressions are obtained for the system average symbol error rate (ASER) and outage probability. The Monte Carlo simulation is used to verify the validity of the proposed expressions. The system security is investigated assuming photon number splitting (PNS) attack. Moreover, the transmit power, time-bin number, and modulation order are optimized to maximize the raw and secret key rates. The results show that for 500 m link, ASER $< 10^{-1}$ and link outage probability $< 10^{-1}$ with tolerating boresight displacement up to 30 cm, the system should be configured at receiver's field-of-view > 22 mrad and signal-to-noise ratio > 7.5 dB which leads $\text{SNR}_{th} < 2.5$ dB and raw key rate maximized by adjusting the number of time bins according to the received SNR.

INDEX TERMS FSO communication, channel fluctuations, quantum cryptography, entanglement photon, E91 protocol, raw key rate, unmanned aerial vehicles (UAVs), tracking system, Kalman filter, performance evaluation, photon number splitting (PNS).

I. INTRODUCTION

Maintaining a high-performance communication system, including the appropriate security level, is of great importance for many applications. Secure communication between the two parties, namely Alice and Bob, can be accomplished by encrypting their messages using a one-time-pad scheme. This involves a long random string of secret bits, i.e., a secret key, to be exchanged securely between the two legitimate parties. Unfortunately, all traditional key distribution approaches are inherently unpredictable as they rely entirely on computational mechanisms that are vulnerable to future developments in computer hardware and algorithms. With the exponential growth of quantum computing, it is expected that the existing

The associate editor coordinating the review of this manuscript and approving it for publication was Yafei Hou.

public key infrastructure will become more vulnerable within a few years due to the availability of large-scale quantum computers [1], [2].

Quantum Key Distribution (QKD) or quantum cryptography is a revolutionary security technology that uses the principle of unconditional security based on the laws of quantum physics. Quantum cryptography involves the random generation and distribution of a secret key over the quantum channel. In the QKD protocols, the eavesdropper, namely Eve, cannot preserve a perfect copy of the quantum signals because perfect quantum copy machines cannot exist. Also, Eve is prevented from perfect eavesdropping due to the quantum non-cloning principle that no measurement can be performed without perturbing the quantum system unless it is compatible with the quantum state. For this unique characteristic, QKD is becoming an essential element of the future secure quantum communication [3]. Furthermore, the QKD protocols can be implemented in both optical fiber and free-space optical (FSO) communication links [4]–[6].

There are currently two main QKD protocols: a continuous variable (CV) and a discrete variable (DV). In CV-QKD protocols, the shared key encodes in the continuous quantum variables expressed by the amplitude and/or phase of weakly modulated light pulses [7]–[9]. In the DV-QKD, the shared key is mapped to discrete variables of the quantum state of a single photon, such as the polarization or phases. The DV-QKD protocols can be subdivided into the prepare-and-measure protocol (PMP) and entanglement-based protocol (EBP), depending on how the random key is encoded into the states of a single photon [10]. In PMP, Alice prepares a random quantum state and then sends it to Bob through a quantum channel, which performs a measurement and detects which state was sent. The best-known PMPs are the Bennett-Brassard-1984 (BB84) protocol [11] and the Bennett-1992 (B92) protocol [12]. Unlike PMP, the EBP was developed to share entangled photon pairs between two parties where Alice possesses an entangled bipartite state for which she sends the first engagement photon to Bob while chooses and measures the state of the second one. The famous EBPs are the Ekert-1991 (E91) protocol [13] and the Bennett-Brassard-Mermin-1992 (BBM92) protocol [14].

The FSO is a communication technology used to transmit data wirelessly employed light propagating in free space. The FSO is a narrow line-of-sight (LoS) technology that offers high data security [15], [16]. Moreover, the FSO has an added benefit of flexibility and cost-effectiveness in infrastructure deployment compared to the optical fiber. However, the performance of the FSO systems is highly affected by the misalignment between the transmitter and the receiver. Thus acquisition, tracking, and pointing (ATP) mechanisms are necessary to achieve such alignment. Hence attaining the LoS, which is vital for effective FSO communications [17]–[19]. Recently, communications using FSO links with QKD technology offer an innovative way of sharing secure information. A drawback in the QKD-based FSO systems is the probability of multiple photons emission, which was made based on the Poisson distribution of the optical source. This might cause a possibility of photon-number-splitting (PNS) that can be captured by eavesdroppers.

Unmanned aerial vehicle (UAV) is a lightweight aerospace platform that is getting the most attention recently because it can be used in various applications, such as surveillance, search, and monitoring. UAV-based communication draws attention because it can be deployed much faster, especially in emergency scenarios. Although UAV communication offers a variety of advantages, it also faces security challenges. Integrating UAVs with FSO systems allows a large set of applications involving transmitting huge amounts of data [20].

In [21], an entanglement-based quantum key distribution over 144 km FSO link has been experimentally demonstrated. Additionally, implementing an active stabilization of their optical link via a closed-loop tracking system to correct the beam drifts induced by atmospheric changes. A free-space entanglement-based QKD experiment using a parametric down-conversion (PDC) source was reported in [22]. The distances between the PDC source and two receivers are both above 7.8 km. The final key rate is increased compared to the standard BB84 protocol. Authors of [23] have demonstrated a satellite-based distribution of entangled photon pairs to two locations separated by 1203 km on the Earth. The first quantum entanglement distribution from an octocopter drone to share polarization-entangled photons to ground stations has been demonstrated in [24] and [25]. In [24], the main devices have been developed for a lightweight airborne quantum node to fit into a small drone airframe, including a polarization entanglement source and acquiring, pointing, and tracking (APT) units while focusing on a local-area network with 40 minutes and 200 m of on-demand coverage. In [25], the flying drone has been generalized for multiple mobile nodes with optical relay among them. Besides developing the first optical relay to reshape the wavefront of photons for their low diffraction loss in free-space transmission. The previously mentioned researchers were interested in the experimental implementation, and their goal was increasing the transmission distance. However, they did not consider channel modeling or parameters optimization.

Moreover, an accurate and computationally efficient channel model was presented in [26] for hovering UAV-based FSO communication links. Also, it considered the optimization of the transmitter/receiver (Tx/Rx) tunable parameters. A simplified and more robust channel model for UAV-based FSO systems was introduced in [27]. The authors in [28] has analyzed the performance of UAV-assisted FSO systems using an Avalanche photodiode (APD) at the receiver and modeled end-to-end signal to noise ratio of the considered FSO link and derived closed-form expressions for the BER of the system under different turbulence conditions. The outage probability for multi-hop vehicle-to-vehicle FSO communication system over the atmospheric turbulence has been studied in [29]. The bit error rate was analyzed under three different channels Nakagami-*m*, Rayleigh, and Weibull.

Furthermore, the BER was examined for the three- and four-relay based system under Rayleigh distribution. However, Those references did not include QKD protocols, neither security analysis in their systems. Also, they did not deal with UAV tracking. The integration between UAV, FSO, and QKD, including UAV tracking mobility, security analysis of the quantum channel, outage probability, and secrecy capacity, are the key objectives of this work.

Additionally, One of the challenges associated with quantum key distribution requires time synchronization between the receiver and the transmitter. Synchronous resolution of 1.023 ns was achieved in [30] adopting a synchronous pulse that has the same wavelength as the quantum signal, and a single photodetector was used to detect the synchronous pulse. A high-resolution time measurement module was utilized to measure the instance of synchronous pulse and signal pulse. A design method was given in [31] for the process that detected the time frame, which included an optical pulse during synchronization. In addition, the specifications of the applied SPAD were described. To ensure a probability of correct detection higher than 99.9%, optimal criteria for limiting the sampling scope in each time window were established. A technique presented in [32] allowed exchanging time-bin encoded photons between Alice and Bob without the need for synchronized time references. This was accomplished using a framing protocol that permitted Alice to encode a time reference along with a key determined by her before transmission. An absolute timing synchronization with an accuracy of 20 ps was demonstrated.

This work proposes an FSO system from Earth to UAV to satisfy on-demand services while achieving security requirements using the E91-QKD protocol. The main contributions of this paper, summarized in Fig.1, are (1) develop an automatic correction-tracking system that minimizes the error-variance of tracking system between mobile UAV and fixed ground station; (2) introduce a QKD system over an optical free space channel applying time-bin with EBP considering a variety of channel impairments; (3) propose closed-form expressions of average-symbol error rate (ASER) and outage probability for UAV-based FSO communication link considering misalignment due to tracking errors and non-zero boresight pointing errors; (4) obtain expressions of raw-key and secret-key rates to perform the security analysis and capacity of the QKD system; (5) report the optimal value of σ_o, σ_p, and θ_{FoV} parameters of the proposed system for achieving high performance.

The rest of this paper is structured as follows. In Section II preliminary research information is given. Section III introduces the proposed MPPM-entanglement system model. The components and algorithm of the tracking system are explained in Section IV. The model of the free-space optical channel is demonstrated in Section V. The derivation of the proposed closed-form expressions for the average symbol error rate, outage probability, and the system security analysis are described in Section VI. Numerical results which validated the derived expressions and optimized the system parameters are presented in Section VII. Finally, conclusions are drawn in Section VIII.

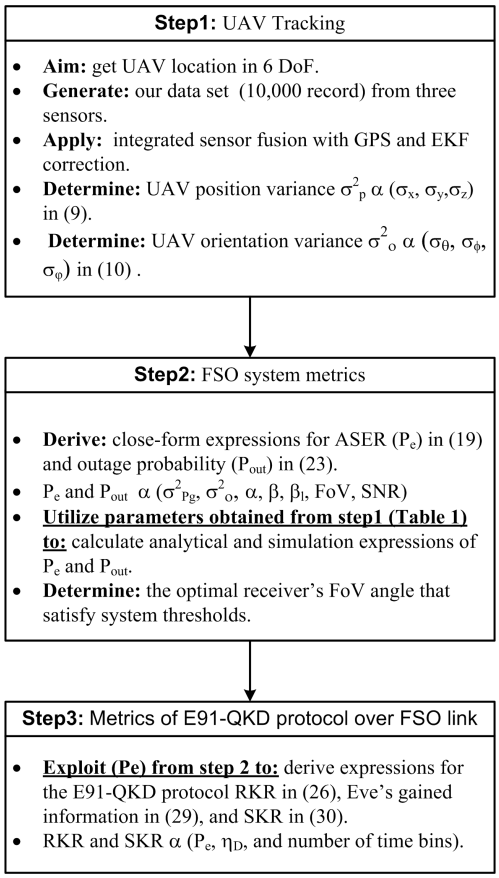

FIGURE 1. Concatenation of paper contributions.

II. PRELIMINARIES

A. ENTANGLEMENT-BASED PROTOCOL (E91)

The E91 protocol uses the Einstein–Podolsky–Rosen photons pair (EPR pair) to establish a sequence of shared keys between the sender (Alice) and the receiver (Bob). It was invented by Artur Ekert in 1991 and developed experimentally over short and long transmission distances. The entangled photons can be prepared by Alice, Bob, or any third party and are distributed in such a way that Alice and Bob have one photon of each pair. In FSO-based QKD, the polarization entanglement is preferred to be used since free space does not affect light polarization. Furthermore, the air is a perfect channel for polarization-entanglement QKD. In the E91 protocol, photons are distributed so that both Alice and Bob end up with one photon of each pair. The scheme is based on entanglement properties. Until measurement occurs, none of the two photons carrying any information, i.e., neither has a definite polarization state. As soon as one of the two parties performs photon measurement, the state of the other one will immediately be determined due to quantum entanglement. This is valid regardless of the spatial separation between the two measurements (non-local correlation). Alice and Bob

then exchange the resulting photon states via a classical (public-authenticated) channel. Finally, Alice and Bob agree on identical measured states and the corresponding bits for the shared key and discard the mismatched measurements. We assume that the FSO link between Alice and Bob is completely time-synchronized, and they will discard any insecure data in case the photon sent by Alice does not interact with Bob [33]. The block diagram of photon entanglement and key verification is shown in Fig. 2.

Single entangled photon pair generation is critical for improving the efficiency of QKD systems. However, many entangled sources are not accurate single entangled photon-pair sources. For example, in parametric down-conversion sources, the emission of entangled pairs is probabilistic with the generation of multiple pairs of entangled states. The multiple pairs of entangled states can be a source of dropping by Eve. She can use a beam splitter to steal parts of the shared photons. This became impossible if (1) she is located away from Bob (time-secure) or (2) a single generated photon (splitting-secure). In any case, Alice and Bob will detect the eavesdropping and will terminate the connection.

In an eavesdropping attack, Eve should also be a UAV who suffers from Bob's same challenging issues when locating herself close to Bob. This is a novel security situation completely different from a traditional scenario with Eve in a fixed position. She must also maintain a safe distance from Bob to avoid crashing with Bob due to random hovering, but she must remain within the beam footprint to receive a signal. The relative distance between Eve and Bob concerning the random misalignments of the beam centroid should have a considerable impact on the possible SKR, especially when pointing errors in the legitimate links are assumed. This practical issue is out of the scope of the current framework of this paper, and we assumed that Eve has a mechanism that keeps her close to Bob and avoid collision with him.

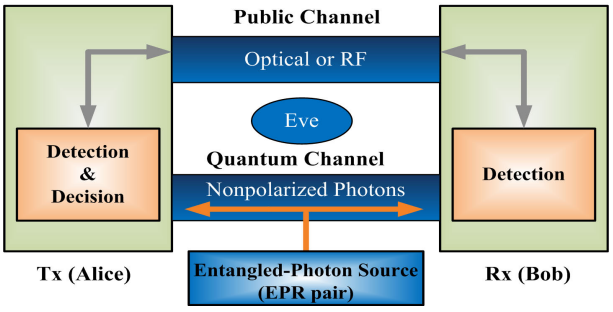

FIGURE 2. Schematic diagram of the E91-protocol.

B. PHOTONS GENERATION WITH MPPM-TIME-BIN ENCODING

A single-photon light beam is such a beam constituted of individual photons separated by some time delay. The generation of a single photon is an essential requirement for optical quantum communications. However, this is practically difficult even in extremely low intensity (weak) laser beam. Given the Poisson statistics of the distribution of the photons in a laser beam [34]:

$$P_i = e^{-\mu} \times \frac{\mu^i}{i!}, \tag{1}$$

where μ is the mean number of photons per pulse, i is the number of photons per pulse, and P_i is the probability that a pulse contains i photons when the average is μ. Fig.3 shows the measured photon statistics of generating photon number with different mean values μ. If μ is 0.2, the probability of generating a single photon is 18%, which increases by increasing μ. However, a higher value of μ increases the probability of producing more than one photon per pulse. The μ with a value less than 1.2 is considered to be the dominant value. In contrast, the probability of having a single generation at $\mu = 1$ is 38%, while the probability of two photons is 20%, and the other is less than 5%.

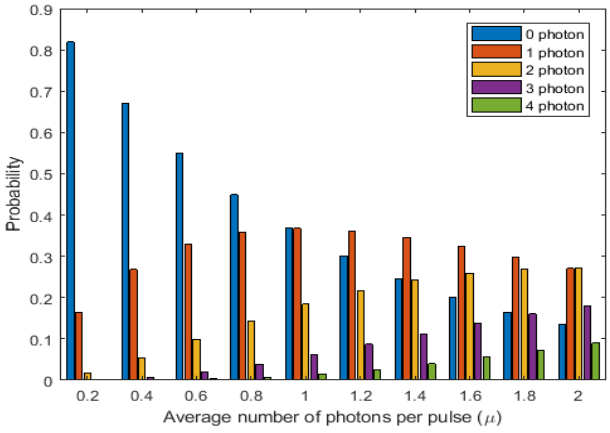

FIGURE 3. Generating probability of photons per pulse.

The Free space-based QKD system with a single-photon transmission offers a fully secure quantum channel. However, it limits the communication distance to only a few hundred meters or data transmissions less than a few Mbps due to low transmitted energy with single-photon and atmospheric turbulence of FSO link. If the distance increases, the performance of the QKD systems is highly decreasing. In order to overcome this problem and achieve a longer communication distance, it is required to increase the number of transmit photons per pulse or reduce the transmission rate. However, with the advantage of the power efficiency of M-ary pulse position modulation (MPPM), it can be considered a reliable solution to overcome this issue. Therefore, integrating MPPM into the QKD protocol (MPPM-QKD protocol) could significantly improve system performance and increase the communication distance. It helps to increase the utilization efficiency of weak laser pulses. Furthermore, each generated photon will introduce $\log_2 M$ bits in the raw key rather than only one bit in the system without an MPPM scheme. Additionally, using a time-bins compression technique with an MPPM scheme

can further improve power efficiency and increase system security [35], [36].

In the classical MPPM scheme, the pulse occupies a single time slot in a symbol with M slots, i.e., the number of time-bins is *one* as shown in Fig. 4(a). On the other hand, if the number of time-bins is higher than *one*, this implies a pulse to be compressed to fill a particular time-bin in the slot rather than the entire slot time as seen in Fig. 4(b,c). Accordingly, the time-averaged transmit power will increase with increasing the number of time bins. The number of time-bins is adapted according to the power, and the position of the active bin is randomly selected to improve the system security and reduce the system quantum bit error rate (QBER) [37].

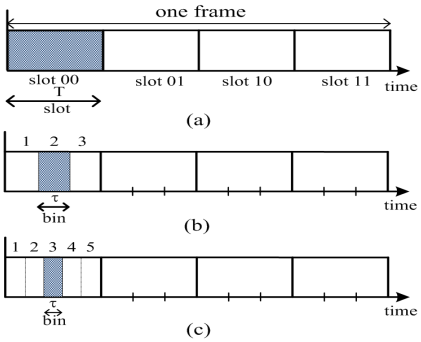

FIGURE 4. MPPM scheme with $M = 4$ (a) classical MPPM (time-bins = 1), (b) compressed MPPM (time-bins = 3), and (c) compressed MPPM (time-bins = 5).

III. PROPOSED MPPM-ENTANGLEMENT SYSTEM

This section presents the overall system architecture, including photon generation and detection and MPPM modulation scheme with time-bin.

A. OVERALL SYSTEM ARCHITECTURE

Fig. 5 shows a schematic diagram of the architecture components and connectivities of the system. The system is composed of three primary components: the ground control station (GCS), the unmanned aerial vehicle (UAV), and the mobile base station (MBS). The FSO connection represents the quantum channel that is utilized to transmit shared keys from the GCS to the UAV. The microwave link constitutes the conventional (public) channel used for key verification and data communication such as GPS, sensing, video, etc…, from the UAV to the GCS. Furthermore, it is also used for controlling purposes by the GCS. A tracking system on the GCS offers a high pointing accuracy within a limited, narrow field of view (FoV). It is supported by a coarse tracking subsystem, which locates and mechanically points the GCS in the direction of the location of the UAV.

B. QUANTUM PREPARATION AND DETECTION

In the proposed system shown in Fig. 6, Alice performs two operations, entanglement generation, and entanglement

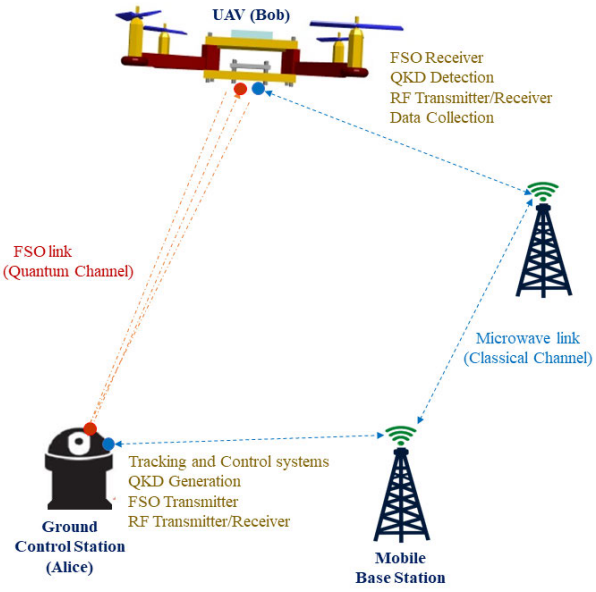

FIGURE 5. Overall system architecture.

detection. In contrast, Bob has only the detection entanglement operation. A random bit stream emits from a random number generator (RNG) and modulates with the MPPM technique [36], [38]. In the classical MPPM, each symbol contains only one pulse located in a specific time slot. In compressed MPPM each slot is divided into several time-bins and the pulse is compressed to occupy only one time-bin. This increases the transmitted power and minimizes the quantum bit error rate (QBER) as well present in the results section. A laser source operates at 775 nm wavelength is modulated with an electro-optic-modulator (EOM) drives with the MPPM electrical signal. The modulated light is then attenuated via the variable optical attenuator (VOA). The output focuses by a lens into a nonlinear beta-barium-borate (BBO) crystal of type II. Using the phenomenon of a PDC, which is a nonlinear instant optical process that converts one photon of higher energy (a pump photon) into a pair of photons (a signal photon and an idler photon) of lower energy following the law of conservation of energy and law of conservation of momentum, an entangled photon pair is generated with 1550 nm wavelength and orthogonal polarization with states given by [39], [40]:

$$|\Psi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|H_A\rangle|V_B\rangle + |V_A\rangle|H_B\rangle\right) \tag{2}$$

where $|H\rangle$ and $|V\rangle$ are the horizontal and vertical polarization respectively, and the subscripts A and B label Alice and Bob systems. Half-wave plates (HWP) and phase compensation crystals (PCCs) in the form of small BBO plates are used to compensate for the relative delay of signals of opposite polarization in the birefringent crystal. The photon energy entering the BBO crystal decays into two photons, each with half the original energy, after a nonlinear process. One photon is transmitted through a transmitter lens over the

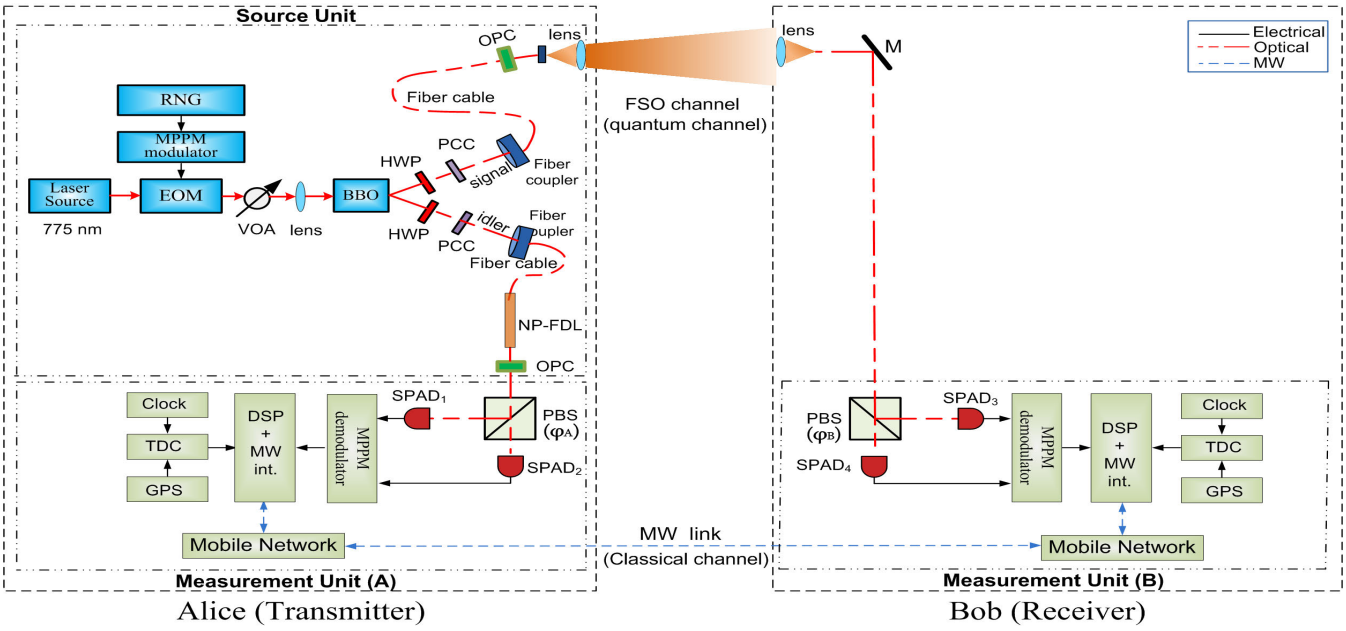

FIGURE 6. Block diagram of the integrated MPPM-E91 system. RNG: random number generator; VOA: variable optical attenuator; HWP: half wave plate; PBS: polarizing beam splitter; SPAD: single-photon avalanche detector; EOM: electro-optic modulator; DSP: digital signal processor; TDC: time-to-digital converter; MW int.: microwave interface; GPS: global positioning system; NP-FDL: non-polarized fiber-delay-line; PCC: phase compensation crystal; OPC: optical pulse compressor.

free-space optical link (quantum channel) to the Bob end, after being compressed through an optical pulse compressor (OPC). The bin selection of the transmitted photon is chosen randomly using the RNG. The RNG uses to produce a number from 1 to 4. This produced number controls the OPC of both the Alice and Bob paths. At Alice end, the entangled photon is delayed by the propagation time via a non-polarized fiber-delay-line (NP-FDL), compressed through the OPC, and then measured locally in the Alice measurement unit.

At the measurement units, Alice and Bob perform polarization measurements in bases randomly chosen by the polarizing beam splitters (PBSs) by using two single-photon avalanche detectors (SPADs) at the output. Alice will obtain the measurement results 0 or 1 (that represent the quantum states $|H\rangle$ and $|V\rangle$), corresponding to the detection of a photon by $SPAD_1$ or $SPAD_2$, respectively, each with equal probability. Since the photons' polarization states are entangled, the state of the photon at Bob will be determined as soon as Alice performs her measurement. Consequently, Bob's beam splitter will detect the same quantum state as Alice, and its corresponding bit value will be detected correctly by the corresponding SPAD. This is known as the sifting process. As a result, compared to the well-known BB84 and B92 protocols, entanglement photons improve the basis-sift factor from 0.5 to 1. This can be guaranteed by the proper orientation φ_A and φ_B of PBSs at Alice and Bob, respectively. The quantum prediction for the number of cases where Alice detects $|H\rangle$ with her PBS at orientation φ_A and Bob detects $|H\rangle$ with orientation φ_B is given as [41]:

$$N\left(H_{\varphi_A}, H_{\varphi_B}\right) = \frac{N_o}{2}\cos^2\left(\varphi_A - \varphi_B\right), \tag{3}$$

where N_o is the number of pairs emitted by the source. The same is valid when detecting $|V\rangle$ at both parties. This procedure is valid in whatever basis of polarization that Alice decides to perform the measurements. Bob will produce the same outcome if he selects the same basis. Since the photon state is entangled, Alice can predict the outcome of Bob with certainty immediately.

Time-to-digital converters (TDCs) are used to record separately the individual times at which each detection event occurred with the time scale disciplined by both the global positioning system (GPS) for coarse synchronization and the local crystal oscillator for fine synchronization. The TDCs are linked to digital signal processor (DSP) connected through a microwave (MW) link (public channel). Bob transmits his time records and detected bits via the public channel to Alice. The corresponding photon pairs (using the measured bit values) could be identified in real-time and maximizing the cross-correlation of recorded time using fast time-correlation software. Alice accepts bits with the same values for creating raw keys simultaneously, while other bits are discarded.

The output of the MPPM modulator modulates the intensity of the laser source via an EOM. The EOM output aligns to the BBO crystal after being attenuated to a proper value by the VOA, which produces a single/multiple entanglement photon pair/s. The enlargement pairs are then compressed

into a single time bin using an optical pulse compressor and sent to Alice and Bob.

The SPAD operates above the breakdown voltage in the so-called "gated Geiger mode," in which the absorption of a single photon can result in the generation of a macroscopic current that can be detected by electronic threshold detection [42]. It is essentially noiseless; however, false counts (i.e., dark counts) can be induced by creating dark carriers by thermal or tunneling processes. The noise variance σ_n^2 of the gated Geiger-Mode avalanche photodiode (GM-APD), assuming no afterpulsing, is $[e^{(\mathrm{PDE}.\lambda_p+\lambda_d)} - 1]\, n_{\mathrm{gates}}$, where PDE is the photon detection efficiency, λ_p is the average number of photo-generated carriers per gate, the average number of dark current-generated carriers per gate is λ_d, and n_{gates} is the total number of gates [43].

IV. TRACKING SYSTEM

This section aims to apply a tracking system in order to determine its position and altitude angles in real-time. Different sensors have been used for the six degrees of freedom to generate our data set for both position and attitude angles. Sensor fusion using an accelerometer, a gyroscope, a magnetometer, and a global positioning system (GPS) is implemented to reduce the uncertainty of position and attitude angles and define the UAV location more precisely. Furthermore, an extended Kalman filter (EKF) is being developed to combine the data sensing from multiple sensors [44], [45].

Assuming position (1) is the current UAV location and attitude angles that satisfy the LoS connection. In contrast, position (2) might be the current state of the UAV resulting from the uncertainty as shown in Fig. 7. The goal is to evaluate the UAV position and attitude variances by applying the extended Kalman filter (EKF) algorithm. The UAV position variance is calculated in the Cartesian coordinates in the directions x, y, and z. In contrast, the UAV attitude variance is determined in Euler coordinates by pitch (θ), roll (ϕ), and yaw (ψ) orientation angles. Such parameters, position and attitude variances, help evaluating the Ground-to-UAV system reliability against outage (link failure), as will be discussed in details.

UAVs state measurement systems are often divided into two subsystems: the attitude and heading reference system (AHRS) and the position-velocity estimator known as the global positioning system/inertial nvigation system (GPS/INS). The tracking system used in this work is responsible for determining the instantaneous position and attitude of the UAV. The AHRS function is related to the stability of the UAV [46]. Its main task is to provide the UAVs with an attitude. On the other hand, GPS/INS calculates the position and the translational velocity of the vehicle, relying mainly on the GPS unit.

One of the key technologies focused on high-precision, and real-time position and attitude estimation is the data fusion of multiple sensors. Different filtering techniques are applied to combine multiple sensing data. For example, the

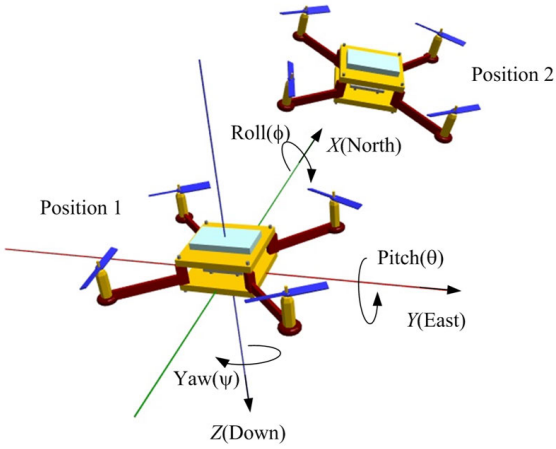

FIGURE 7. Position and attitude variations of the UAV.

Kalman filter (KF) is widely used in linear system estimation [47]. However, the process and measurement model of most position and attitude estimation systems are nonlinear. The extended Kalman filter (EKF) and unscented Kalman filter (UKF) with the core idea of approximation are proposed with the characteristics of different degrees of linearization errors [48], [49]. The block diagram of sensor fusion and filtering using EKF is presented in Fig. 8. As will be seen later, multiple sensor data (including those from an accelerometer, gyroscope, magnetometer, and GPS) are integrated with an EKF algorithm to calculate the position and attitude variations (σ_p and σ_0).

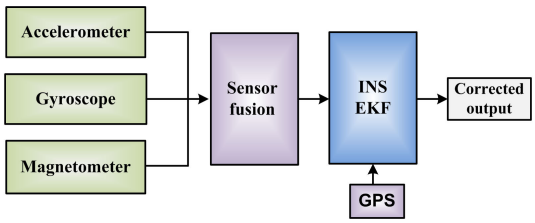

FIGURE 8. Sensor fusion and filtering.

The operation of the Kalman filter requires the design of two mathematical models, the process model and the measurement model [50]. In the process model, the UAV condition at each step consists of the position, velocity, and orientation angles. The inputs to the process model are the specific force (the output of the accelerometer is the difference between the inertial and gravitational acceleration referred to as the specific force) and the angular rate measurements. Position and velocity in x, y, and z axes might well be expressed in 3D state vectors as $P_k = [p_x\ p_y\ p_z]^T$ for position and $V_k = [v_x\ v_y\ v_z]^T$ for velocity. Also, the quaternion approach is used to represent the orientation of the UAV rather than the representation of the Euler Angle since it does not suffer from singularity [51]. However, the system dimensions are increased to four $q_k = [q_0\ q_1\ q_2\ q_3]^T$. Accordingly, the state vector and inertial measurement input

vector are defined as:

$$X_k = \begin{bmatrix} P_k \\ V_k \\ q_k \end{bmatrix} \in R^{10} \quad \text{and} \quad u_k = \begin{bmatrix} f_k \\ \omega_k \end{bmatrix} \in R^6, \tag{4}$$

where X is the state vector, $P_k \in R^3$ [m], $V_k \in R^3$ [m/s], and $q_k \in R^4$ [-] denote the position, velocity, and attitude angles (quaternion representation) of the navigation system at time instant k, respectively. Further, u is a known exogenous control input, $f_k \in R^3$ [m/s2] and $\omega_k \in R^3$ [rad/s] denote the specific force and angular velocity at time instant k, respectively. The process model is given by the non-linear equation:

$$X_k = f(X_{k-1}, u_k) = FX_{k-1} + Bu_k, \tag{5}$$

where F is a transition matrix, B is the control matrix.

The position and velocity are given as

$$P_k = P_{k-1} + \Delta t V_{k-1} + \frac{\Delta t^2}{2}(C_b^n(q_{k-1})f_k - g), \tag{6}$$

$$V_k = V_{k-1} + \Delta t(C_b^n(q_{k-1})f_k - g), \tag{7}$$

where Δt is the system sample interval, and $C_b^n(q)$ denotes the directional cosine matrix (rotation matrix) that rotates a vector from the body coordinate frame (b-frame) to the navigation coordinate frame (n-frame). Further, g denotes the gravity vector expressed in the navigation coordinate system.

According to [52], the discrete-time form of the system process model for the quaternion representation can be described as:

$$q_k = \{I_{4\times4} + \frac{\Delta t}{2}[\Omega\times]\}q_{k-1}. \tag{8}$$

where $[\Omega\times]$ denotes the first-order quaternion dynamic model, which is given by the angular rate $\omega_k = (\omega_x, \omega_y, \omega_z)^T$.

The EKF algorithm is summarized in Algorithm 1. In this algorithm, we included the measuring models for GPS and magnetometers for the measurements. The GPS provides the position and velocity, and the magnetometer measures the yaw in the global frame. After filtering the raw data, the attitude angles of θ, ϕ, and ψ can be determined from the quaternion representation according to [53]. The data set derived from the fusion sensors is analyzed to determine the standard position and orientation variance, as seen in the results section. The variance of position deviation of the UAV is given by:

$$\sigma_p^2 = \sigma_x^2 + \sigma_y^2 + \sigma_z^2, \tag{9}$$

where σ_x^2, σ_y^2, and σ_z^2 are the position variances in x, y, and z directions, respectively. The variance of the orientation deviation is given by:

$$\sigma_o^2 = \sigma_\theta^2 + \sigma_\phi^2 + \sigma_\psi^2, \tag{10}$$

where σ_θ^2, σ_ϕ^2, and σ_ψ^2 are the attitude variances calculated by θ, ϕ, and ψ orientation angles. Equations (9) and (10), derived from fusing the data set of various sensors, will be employed in Section VI to calculate the average symbol error rate and outage probability. Moreover, the numerical values declared in Table 2 will be exploited in the numerical results and discussion section.

Algorithm 1 Extended Kalman Filter for Position and Attitude Estimation

1: $k = 1$
2: $X_o \leftarrow$ Initial State
3: $P_o \leftarrow$ Initial Kalman filter state covariance matrix
4: **while** no abort command received **do**
5: **State Prediction**: Predict the state vector with the process model and the inertial measurement unit (IMU) measurements.

$$X_k^- = FX_{k-1} + Bu$$

6: **Covariance Prediction**: Time update of the KF state covariance with the covariance matrix of process model noise (Q).

$$P_k^- = FP_{k-1}F^T + Q$$

7: **if** GPS and magnetometer measurements available **then**
8: **Kalman Gain**: Update the Kalman gain with the covariance matrix of the measurement model noise (R).

$$G_k = P_k^-[P_k^- + R]^{-1}$$

9: **State Correction**: Update the state vector with the GPS measurements vector (Z_k).

$$X_k = X_k^- + G_k(Z_k + X_k^-)$$

10: **Covariance Update**: Update of the state covariance

$$P_k = [I_{4\times4} - G_k]P_k^-$$

11: **end if**
12: **end while**

V. OPTICAL FREE-SPACE CHANNEL MODEL

The model introduced in this work considers the combined effect of four channel impairments, namely, the atmospheric path loss h_a, the atmospheric turbulence h_t due to intensity fluctuations of the optical signal while traveling through space, the pointing error loss h_p due to misalignment between the beam and detector centers, and the link interruption h_{pa} due to the angle-of-arrival (AoA) fluctuations. Note that the factor h_a is constant at given propagation distance and weather conditions while the other factors are random variables. The ground-to-UAV instantaneous channel state h is obtained as [27]:

$$h = h_a\, h_t\, h_p\, h_{pa}. \tag{11}$$

Considering a ground-to-UAV FSO link, the probability density function (PDF) of the channel under moderate-to-strong turbulence condition is given as [26]:

$$f_h(h) = \exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\delta(h) + \left[1 - \exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\right] \times \sum_{j=0}^{J} \frac{1}{j!}\left(\frac{\alpha\beta}{A_0 h_a}\right)^j \left(v_j(\alpha,\beta)h^{\beta-1+j} - v_j(\beta,\alpha)h^{\alpha-1+j}\right), \quad (12)$$

where

$$v_j(\alpha,\beta) = \frac{\pi\gamma^2\left(\frac{\alpha\beta}{A_0 h_a}\right)^{\beta}[\sin((\alpha-\beta)\pi)]^{-1}}{\Gamma(\alpha)\Gamma(\beta)\Gamma|j-(\alpha-\beta)+1)| - (\beta-\gamma^2+j)|} \times \exp\left(\frac{-s^2}{2\sigma_{pg}^2} - \frac{s^2\gamma^2/\sigma_{pg}^2}{2\beta-2\gamma^2+2j}\right), \quad (13)$$

and

$$v_j(\beta,\alpha) = \frac{\pi\gamma^2\left(\frac{\alpha\beta}{A_0 h_a}\right)^{\alpha}[\sin((\beta-\alpha)\pi)]^{-1}}{\Gamma(\alpha)\Gamma(\beta)\Gamma|j+(\alpha-\beta)+1)| - (\alpha-\gamma^2+j)|} \times \exp\left(\frac{-s^2}{2\sigma_{pg}^2} - \frac{s^2\gamma^2/\sigma_{pg}^2}{2\alpha-2\gamma^2+2j}\right), \quad (14)$$

(13) and (14) are deduced in [54] considering the general case of nonzero boresight pointing error. α and β are the effective number of large-scale and small-scale turbulence eddies, respectively; they are directly related to the atmospheric conditions [55]. Also, $A_0 = [\text{erf}(\nu)]^2$ is the fraction of power collected at $r = 0$, r is the radial displacement from the photodetector (PD) center [56, Fig.2], $\nu = \sqrt{\pi/2}(r_a/\omega_z)$ is the ratio between aperture radius r_a and the beam waist ω_z at distance z, and erf(.) is the standard error function [56]. Moreover, $\lfloor J = \gamma^2 - \alpha \rceil$, $\gamma = \omega_{zeq}/2\sigma_{pg}$ is the ratio between the equivalent beamwidth $\omega_{zeq}^2 = \omega_z^2\left(\sqrt{\pi}\text{erf}(\nu)/2\nu\exp(-\nu^2)\right)$ and jitter standard deviation (SD), that measures the pointing error severity [54].

The radial displacement $r = |\mathbf{r}| = \sqrt{r_x^2 + r_y^2 + r_z^2}$ follows the Beckmann distribution [57]. The Beckmann distribution is a versatile distribution used to describe the PDF of fading channels in general. It includes many distributions as a special case. For example, it can be specialized to Rician, Raylight, Hoyt, and single-sided Gaussian according to the values of the means and variances of the random variables r_x, r_y, and r_z [54]. Generally, r_x, r_y, and r_z are modeled as nonzero mean Gaussian distributed independent RVs, i.e., $r_x \sim \mathcal{N}(\mu_x, \sigma_x^2)$, $r_y \sim \mathcal{N}(\mu_y, \sigma_y^2)$, and $r_z \sim \mathcal{N}(\mu_z, \sigma_z^2)$, respectively. In addition to the random jitters, this work considers a nonzero boresight error, where $s = \sqrt{\mu_x^2 + \mu_y^2 + \mu_z^2}$ is the boresight displacement. The jitter displacement is $\sigma_{pg}^2 = \sigma_p^2 + \sigma_g^2$, where σ_g^2 is the variance of Tx position fluctuations. In this work, the Tx is fixed on a ground station. Thus its variance is small and can be ignored relative to the Rx on-board UAV.

VI. ERROR AND OUTAGE PROBABILITIES WITH SECURITY ANALYSIS

In this section, closed-form expressions for the average symbol error rate (ASER) and outage probability (P_{out}) are derived for MPPM modulation in the ground-to-UAV optical link considering atmospheric turbulence, atmospheric attenuation, nonzero boresight pointing errors, and the link interruption due to the AoA fluctuations.

A. PROPOSED EXPRESSION FOR AVERAGE SYMBOL ERROR RATE

The upper bound of the received instantaneous error probability $P_e(h)$ for MPPM for a given channel state h is deduced in [58] and provided as a function of average signal to noise ratio $\overline{\text{SNR}}$ in [59] and [60] as:

$$P_e(h) \leq \frac{M-1}{2}\text{erfc}\left(\sqrt{\frac{(M\log_2 M)\,\overline{\text{SNR}}\,h^2}{4}}\right), \quad (15)$$

where $\overline{\text{SNR}}$ is given by [43]:

$$\overline{\text{SNR}} = \frac{\text{PDE}\,\lambda_p\,n_{\text{gates}}}{\sqrt{\frac{p}{(1-p)}\,n_{\text{gates}}}}, \quad (16)$$

where $p = 1 - e^{(\text{PDE}.\lambda_p+\lambda_d)}$. Considering the effect of the quantum channel $\lambda_p = \eta_s \times \mu$, where $\eta_s \in [0,1]$, is the transmittance coefficient of the quantum channel, which represents the percentage of photons arrive at the receiver aperture through the channel.

The average symbol error rate is obtained by averaging the instantaneous error probability $P_e(h)$ of MPPM over the PDF $f_h(h)$ as [58]:

$$P_e = \int_0^{\infty} P_e(h) f_h(h) dh, \quad (17)$$

From (12) and (15) the ASER in (17) is obtained as:

$$P_e = \frac{M-1}{2}\int_0^{\infty}\text{erfc}\left(\sqrt{\frac{(M\log_2 M)\,\overline{\text{SNR}}\,h^2}{4}}\right) \times \left[\exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\delta(h) + \left[1-\exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\right] \times \sum_{j=0}^{J}\frac{1}{j!}\left(\frac{\alpha\beta}{A_0 h_a}\right)^j\left(v_j(\alpha,\beta)h^{\beta-1+j} - v_j(\beta,\alpha)h^{\alpha-1+j}\right)\right]dh. \quad (18)$$

The close-form expression of the ASER is extracted by using [61, eq.(06.27.21.0132.01)], as:

$$P_e = \frac{M-1}{2}\left[\exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\right] + \frac{M-1}{2\sqrt{\pi}}\left[1-\exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\right]\sum_{j=0}^{J}\frac{1}{j!}\left(\frac{\alpha\beta}{A_0 h_a}\right)^j$$

$$\times \left[\frac{\Gamma(\frac{\beta+j+1}{2})}{\beta+j} \left(\sqrt{\frac{\left(M \log_2 M\right) \overline{\mathrm{SNR}}}{4}} \right)^{-(\beta+j)} v_j(\alpha, \beta) - \frac{\Gamma(\frac{\alpha+j+1}{2})}{\alpha+j} \left(\sqrt{\frac{\left(M \log_2 M\right) \overline{\mathrm{SNR}}}{4}} \right)^{-(\alpha+j)} v_j(\beta, \alpha) \right]. \tag{19}$$

B. PROPOSED EXPRESSION FOR OUTAGE PROBABILITY

A further figure of merit in determining the performance of the ground-to-UAV system is the outage probability, which is defined as the probability that the instantaneous signal-to-noise ratio $\mathrm{SNR}(h) = \overline{\mathrm{SNR}}\, h^2$ goes below a certain threshold SNR_{th}, and it is given by [60], [62]:

$$\begin{aligned} P_{\text{out}} &= P_r(\mathrm{SNR}(h) < \mathrm{SNR}_{th}) \\ &= P_r(h < \gamma_o) = F_h(\gamma_o), \end{aligned} \tag{20}$$

where $\gamma_o = \sqrt{\mathrm{SNR}_{th}/\overline{\mathrm{SNR}}}$ and $F_h(\gamma_o)$ is the well known cumulative distribution function (CDF) of h, defined as:

$$F_h(\gamma_o) = \int_0^{\gamma_o} f_h(h)\, dh. \tag{21}$$

Substituting (12) and (21) into (20), the outage probability is obtained as:

$$\begin{aligned} P_{\text{out}} = &\int_0^{\gamma_o} \exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\delta(h)\, dh + \left[1 - \exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\right] \\ &\times \int_0^{\gamma_o} \sum_{j=0}^{J} \frac{1}{j!} \left(\frac{\alpha\beta}{A_0 h_a}\right)^j \\ &\times \left[\left(v_j(\alpha, \beta) h^{\beta-1+j} - v_j(\beta, \alpha) h^{\alpha-1+j}\right)\right] dh, \end{aligned} \tag{22}$$

The integration in (22) can be calculated using simple integration rules, then close-form expression for P_{out} is derived as:

$$\begin{aligned} P_{\text{out}} = &\left[\exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\right] + \left[1 - \exp\left(\frac{-\theta_{FoV}^2}{2\sigma_o^2}\right)\right] \\ &\times \frac{\exp(\frac{-s^2}{2\sigma_{pg}^2})\pi\gamma^2}{\Gamma(\alpha)\Gamma(\beta)\sin(\pi(\alpha-\beta))} \sum_{j=0}^{J} \left(\frac{\alpha\beta}{A_0 h_a}\right)^j \\ &\times \left[\frac{\left(\frac{\alpha\beta}{A_0 h_a}\right)^{\beta} \exp(-\frac{s^2\gamma^2/\sigma_{pg}^2}{2\beta-2\gamma^2+2j})\, \gamma_o^{(\beta+j)}}{(\beta+j)\Gamma(j-(\alpha-\beta)+1)\lvert-(\beta-\gamma^2+j)\rvert} \right. \\ &\left. - \frac{\left(\frac{\alpha\beta}{A_0 h_a}\right)^{\alpha} \exp(-\frac{s^2\gamma^2/\sigma_{pg}^2}{2\alpha-2\gamma^2+2j})\, \gamma_o^{(\alpha+j)}}{(\alpha+j)\Gamma(j+(\alpha-\beta)+1)\lvert-(\alpha-\gamma^2+j)\rvert} \right]. \end{aligned} \tag{23}$$

C. RKR AND SKR ANALYSIS

The probability distribution of the atmospheric channel transmittance that describes the fluctuations of the transmittance η_s is given by [63, Eq. (15)]. The transmittance is mainly affected by beam wandering, and distortion of the spot size and shape. It can be accurately (provided beam ellipticity is small) approximated by the transmittance of the circular Gaussian beam as [64]:

$$\eta_s = \eta_0 \exp\left[-\left(\frac{r_0}{\mathrm{R}}\right)^{\Lambda} \right], \tag{24}$$

where Λ and R are the shape and scale parameters, respectively, r_0 is the beam-deflection distance, and η_0 is the transmittance for the centered beam, i.e. for $r_0 = 0$.

The raw key rate (RKR) and secret key rate (SKR) of the quantum channel are important metrics for measuring the efficiency of the FSO link. Here, we present the expressions for the RKR and SKR when the MPPM-E91 protocol is used. As described in (1), the probability of generating a pulse with i photons is $P_i = e^{-\mu}\mu^i/i!$ while $i \geq 0$ and the probability of generating a pulse with zero photons is $\mathrm{P}_0 = e^{-\mu}$. Moreover, the probability that an MPPM-frame of length M has a slot with a pulse of i photons while the remaining $(M-1)$ slots are empty follows the Binomial distribution as [35]:

$$P_{\text{i, MPPM}} = \binom{M}{1} P_i\, P_0^{(M-1)}. \tag{25}$$

The raw key rate (RKR) per frame is given as [65]:

$$R_{\text{raw}} = \frac{\log_2 M}{M} \sum_{i\geq 1} P_{\text{i, MPPM}}[1 - (1 - \eta_D \eta_s)^i], \tag{26}$$

where η_D is the detector efficiency. The RKR of MPPM-E91 protocol over the quantum (free space) channel, $R_{\text{raw,qu}}$, taking into account the free space channel impairments discussed in Section V is derived by using the ASER, P_e, in (19) and the RKR in (26) as follows:

$$R_{\text{raw,qu}} = R_{\text{raw}} \times \left(1 - \frac{P_e}{\log_2 M}\right). \tag{27}$$

In a PNS attack, the Poisson photon source allows Eve to acquire information due to the probability of multiple-photon generations. Considering a pulse with multiple photons, Eve could trap one or more photons from the quantum channel. After both parties (Alice and Bob) identified and preserve the states, Eve could easily predict the shared key. The information collected by Eve through the PNS is given as [65]:

$$R_{\text{Eve}} = \frac{\log_2 M}{M} \sum_{i\geq 2} P_{\text{i, MPPM}}\, \eta_D \tag{28}$$

Taking into account the deterioration effects of the quantum (FSO) channel, Eve's gained information is derived from (19) and (28) as:

$$R_{\text{Eve,qu}} = \frac{\log_2 M}{M} \sum_{i\geq 2} P_{\text{i, MPPM}}\, \eta_D \times \left(1 - \frac{P_e}{\log_2 M}\right) \tag{29}$$

The SKR of MPPM-E91 protocol over the quantum channel is obtained using (27) and (29) as:

$$R_{\text{SKR,qu}} = R_{\text{raw,qu}} - R_{\text{Eve,qu}}. \tag{30}$$

TABLE 1. FSO communication system and simulation parameters.

Parameter	Symbol	Value
System Parameters		
UAV altitude	L	500 m
Transmitter diameter	D_T	0.2m
Receiver diameter	D_R	0.1 m
Wavelength	λ	1550 nm
Modulation order	M	4,8,16
Detector efficiency	η_D	0.8
Bit rate	R_B	500 Mbps
Atmospheric attenuation coefficient	β_l	2 dB/km
Photon detection efficiency	PDE	0.5
Number of photons absorbed per gate	λ_p	0.01 to 0.25
Number of dark current carriers generated per gate	λ_d	0.03
Number of gates	n_{gates}	40
Channel Parameters		
Transmittance coefficient	η_s	0.5
Rytov variance	σ_R^2	2.5
Effective number of large-scale cells	α	4.034
Effective number of small-scale cells	β	1.539

where $R_{\text{SKR,qu}}$, is normalized to the system bit rate, R_B. Thus, the SKR generated by the proposed system in bits/sec is $R_{\text{SKR,qu}} \times R_B$.

VII. NUMERICAL RESULTS AND DISCUSSION

In this section, the numerical results in terms of ASER and outage probability are given. These expressions are used to evaluate the impact of essential parameters and channel influences such as receiver's FoV angle, propagation distance, and boresight displacement in the proposed ground-to-UAV FSO system. The system parameters adopted here are shown in Table 1 according to relevant recent literature in [27] and [66]. The Monte Carlo simulation confirm the validity of the resulting closed-form expressions. Moreover, the system security is investigated in terms of RKR and SKR assuming a PNS attack, taking into account the effect of the modulation order M, the total number of photons per pulse, and the number of time-bins.

The standard deviation of the position x, y, and z from RTK-GPS and before applying the fusion algorithm with EKF was around 11 cm for the x and y and 16cm for z. The use of the fusion algorithm limits the standard deviation to 5.21 cm, 5.02 cm, and 7.03 cm for the places in x, y, and z, respectively. The variation of position is presented in Fig. 9, where the sample output is calculated using the noisy data and the outputs given by the fusion algorithm. According to those results, the standard deviation of the position variations (σ_p) is determined from (9) as 10 cm.

Furthermore, the standard deviation of the angle of attitude before implementing the fusion algorithm with EKF was about 5mrad for the angle of pitch/roll and 7.5 mrad for the angle of yaw. Since implementing the fusion algorithm, it was reduced to 2.6 mrad, 2.04 mrad, and 4.06 mrad for pitch, roll, and yaw angles. The variance of the angle of attitude is seen in Fig. 10. Attitude angles are computed in the

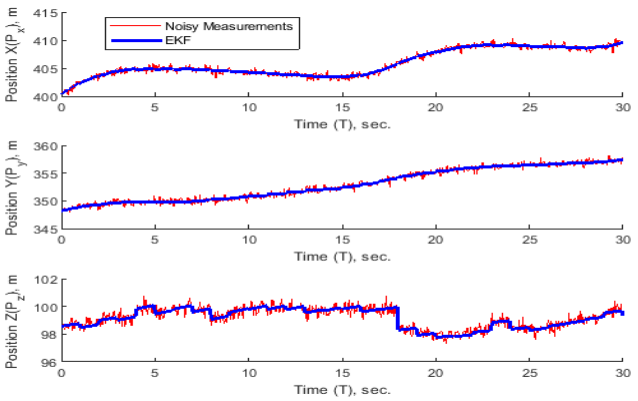

FIGURE 9. Position estimation by raw outputs and the fusion algorithm.

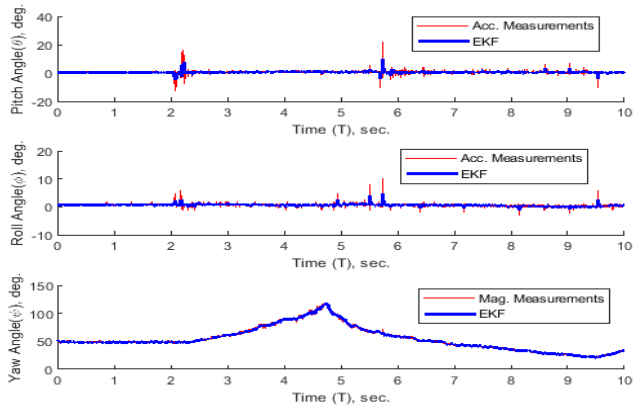

FIGURE 10. Attitude angles estimation by raw outputs and the fusion algorithm.

TABLE 2. Tracking system results.

Parameter	Symbol	Value
Orientation		
Standard deviation of fluctuations around pitch	σ_θ	2.6 mrad
Standard deviation of fluctuations around roll	σ_ϕ	2.04 mrad
Standard deviation of fluctuations around yaw	σ_ψ	4.06 mrad
Position		
Standard deviation of fluctuations in x-direction	σ_x	5.21 cm
Standard deviation of fluctuations in y-direction	σ_y	5.02 cm
Standard deviation of fluctuations in z-direction	σ_z	7.03 cm

sample output using raw outputs (angles of the accelerometer and magnetometer sensors) and outputs given by the fusion algorithm. Based on those values, the standard deviation of the orientation variance (σ_o) is determined from (10) to be 5 mrad. Table 2 summarizes the tracking results.

The simulation and analytical results of ASER versus the FoV of the receiver is presented in Fig. 11 for SNR of 5 dB, 10 dB, and 15 dB. As soon as $\theta_{FoV} \geq 18$ mrad, there is an exactly matching between the simulation and analytical results. Nevertheless, if $\theta_{FoV} < 18$ mrad, there is a little mismatch. Therefore, we will consider that when setting the value of θ_{FoV} in the proposed results. Furthermore, the figure

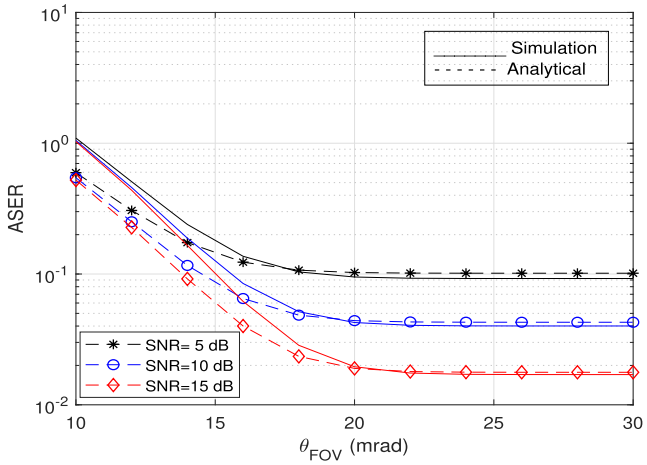

FIGURE 11. The ASER versus the receiver's FoV with different signal-to-noise ratio, M = 16, $\sigma_o = 5$ mrad, and $\sigma_p = 10$ cm.

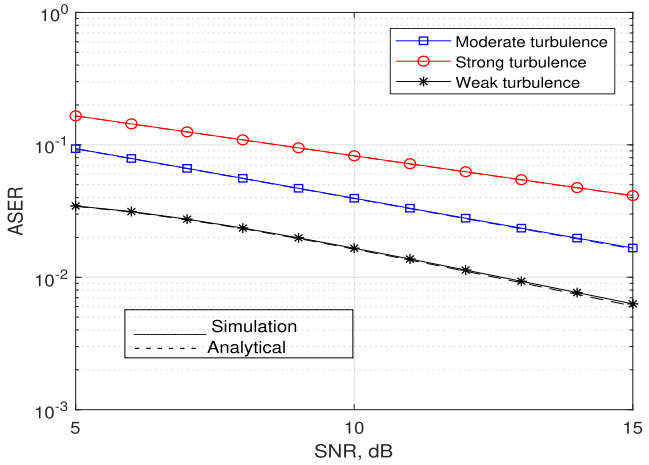

FIGURE 13. ASER versus average SNR of FSO link for different turbulence conditions, L = 500 m and $\theta_{FoV} = 22$ mrad.

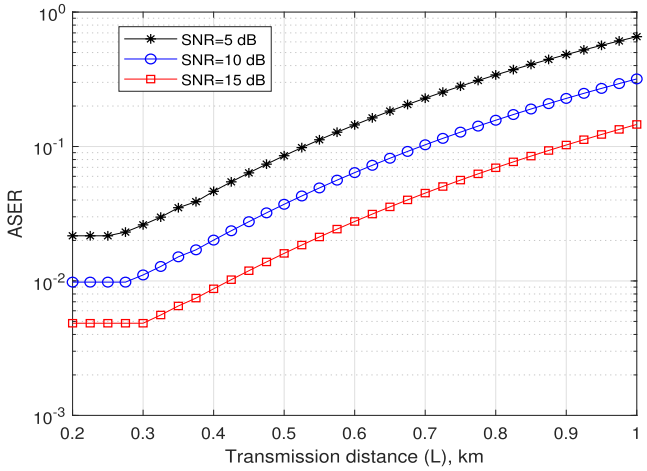

FIGURE 12. Effect of SNR on the ASER as a function of the FSO link distance with $M = 16$, $\sigma_o = 5$ mrad, $\sigma_p = 10$ cm, and $\theta_{FoV} = 22$ mrad.

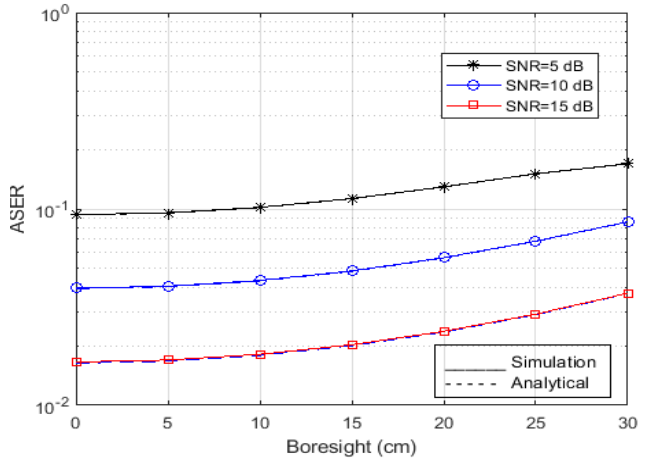

FIGURE 14. The effect of boresight displacement on the ASER for different SNR with $M = 16$, $L = 500$ m, and optimal θ_{FoV}.

illustrates that the ASER reduces as θ_{FoV} increases for all SNR values, achieving an optimal value at $\theta_{FoV} = 18$ mrad, 20 mrad, and 22 mrad for SNR 5 dB, 10 dB, and 15 dB, respectively. As a result, we will use $\theta_{FoV} = 22$ mrad for precision results in order to assure accuracy while also keeping the ASER below $10 - 1$.

Fig. 12 shows the relationship between the ASER and the FSO transmission distance at signal-to-noise ratio of 5 dB, 10 dB, and 15 dB, with $M = 16$, standard orientation deviation $\sigma_o = 5$ mrad, and position standard deviation $\sigma_p = 10$ cm. As expected, the ASER increases with longer transmission distances. In order to limit ASER below 10^{-1}, the maximum allowable link distances are 525 m, 700 m, and 900 m for SNR 5 dB, 10 dB, and 15 dB, respectively. In this work, the operating transmission distance is chosen to be 500 m to satisfy ASER threshold for 5 dB < SNR < 15 dB.

The performance is also evaluated for 5 dB < SNR < 15 dB under different atmospheric turbulence, including strong turbulence ($\sigma_R^2 = 5.5$), moderate turbulence ($\sigma_R^2 = 2.5$), and weak turbulence ($\sigma_R^2 = 0.5$). By considering $\theta_{FoV} = 22$ mrad and $L = 500$ m, Fig. 13 clearly shows exactly matching between the simulation and analytical results of the ASER expressions in (18) and (19). It is aslo given that the ASER can be kept below the system threshold of 10^{-1} for turbulence conditions provided that the average SNR > 9 dB.

Note that all of the above results have been calculated at zero boresight displacement. Therefore, the effect of non-zero boresight on the ASER is presented in Fig. 14 at different SNR with $M = 16$ and $L = 500$ m. Using the optimized values of σ_o, σ_p, and θ_{FoV}, the ASER is lightly affected by the variation in boresight displacement from 0 to 30 cm. In addition, the composed PDF has been verified by comparing the proposed and stimulated results, as shown in Fig. 15. From the results, we can recognize an exactly matching between the two proposed and stimulated PDFs with the achieved results from the previous discussions.

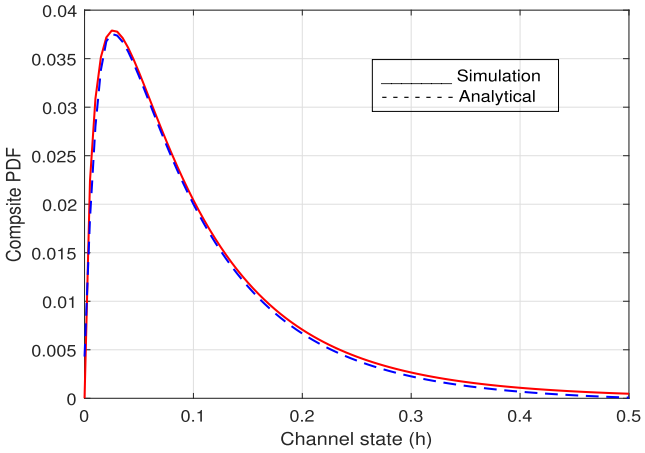

FIGURE 15. Composite probability density function versus the channel state.

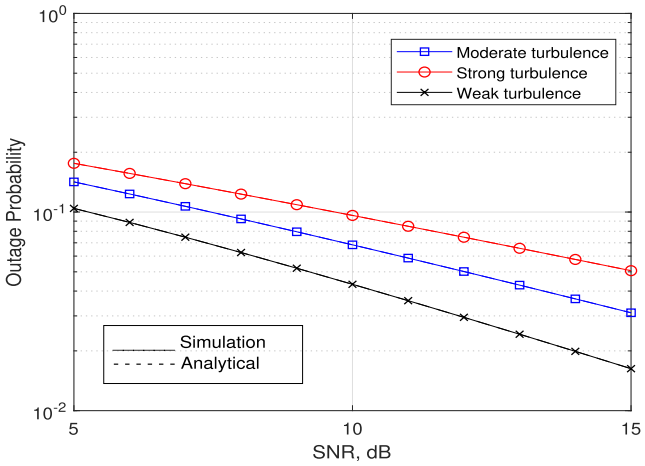

FIGURE 16. Outage probability versus average SNR of FSO link for different turbulence conditions, L = 500 m and θ_{FoV} = 22 mrad.

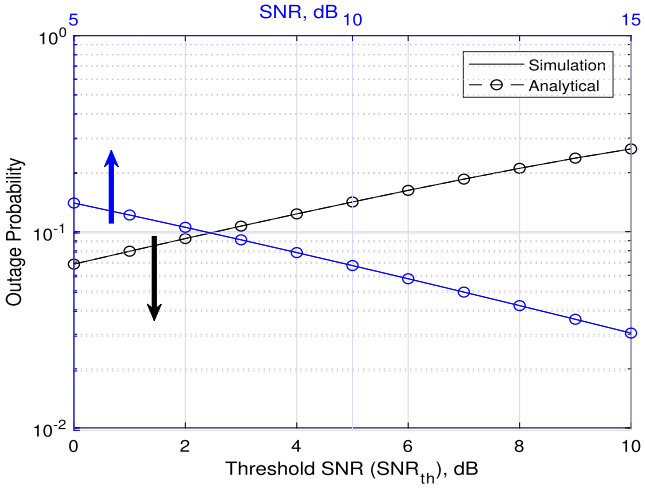

FIGURE 17. Outage probability versus the signal-to-noise ratio and the threshold SNR, L = 500 m.

With θ_{FoV} = 22 and a communication distance of L = 500 m, Fig. 16 illustrates that the simulation and analytical

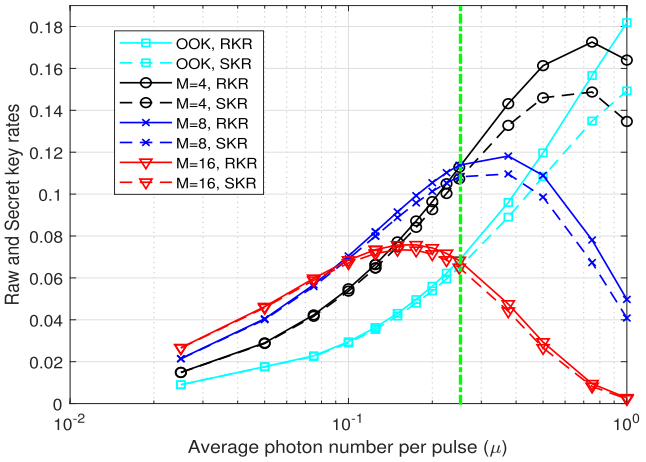

FIGURE 18. key rate comparison between MPPM and OOK.

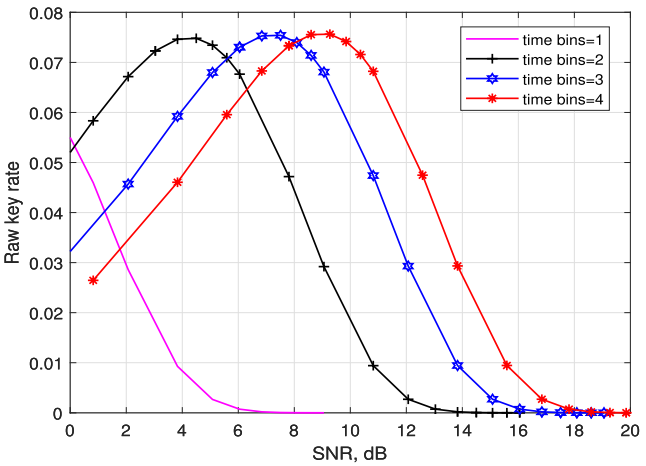

FIGURE 19. The RKR versus the SNR with different number of time-bins, M = 16, and L = 500 m.

results of the outage probability (P_{out}) expressions in (22) and (23) are exactly the same. It is also shown that the outage probability can be kept below the system threshold of 10^{-1} for SNR > 10 dB under different turbulence, as illustrated in Fig. 16. Therefore, under the three types of atmospheric turbulence, the SNR greater than 10 dB is necessary to ensure efficient system performance in terms of ASER and outage probability.

The results of the outage probability as a function of received SNR and the threshold SNR (SNR_{th}) under moderate turbulence are illustrated in Fig. 17 for the proposed closed-form and Monte Carlo simulation. The outage probability is directly proportional to SNR_{th} and inversely proportional to SNR. For the outage probability to be less than 10^{-1}, the system should be configured at SNR> 7.5 dB, which equivalent to $SNR_{th} < 2.5$ dB.

Fig. 18 illustrates the effects of modulation order on the system performance and security in terms of RKR and SKR. It can be seen that MPPM outperforms OOK when $\mu < 0.25$ which has very low probability of multi-photon

generation as shown in fig.3. Considering the operation below $\mu = 0.25$, at $M = 16$, the RKR is 0.08 which is almost the same as the SKR. That means guaranteeing system security against PNS attack. On the other hand. increasing the modulation order leads to higher RKR at expense of increased opportunity of Eve's attack.

Fig. 19 shows the effect of the number of time-bins on the received SNR as a function of the RKR. The outage probability versus the SNR and SNR_{th} is seen in Fig. 17. It is necessary to maintain SNR $>$ 8 dB and SNR$th = 2$ dB in order to keep the outage probability below the threshold of $10 - 1$ for moderate turbulence. Therefore, keeping the SNR at the required value either by increasing the transmitted energy or increasing the number of time-bins. Furthermore, this could improve the probability of transmission errors and therefore increase the PKR. The channel state information can be exploited to satisfy the required RKR at a specific value of the received SNR. On the other hand, Fig. 19 also shows that a certain value of RKR is achieved while gaining higher SNR at the receiver employing greater time bins.

VIII. CONCLUSION

In this paper, the integration of GCS, UAV, QKD, and FSO systems have been proposed. We developed an algorithm based on the EKF for real-time tracking of GPS location-aware moving UAVs. The complete architecture of the quantum key sharing mechanism (preparation and detection) based on the E91 protocol is presented. This mechanism used a time-bin-based MPPM scheme to allow for multiple key bits to be encoded in a single photon, thus increasing the fidelity of the transmitted keys. The channel model considered the combined effects of atmospheric attenuation, atmospheric turbulence (Gamma-Gamma model), nonzero boresight pointing error, and angle-of-arrival (AoA) fluctuations. The secret key is generated over the FSO (quantum) channel using MPPM-E91 protocol with the time-bin technique taking into account channel impairments. Moreover, we studied the effect of different system parameters, i.e., received SNR, receiver field-of-view, length of the GCS-UAV link, and different modulation order on the performance of the system.

Based on the standard deviation of the UAV position and orientation variations extracted from the tracking system, it is found that the optimum values of θ_{FoV} that achieved threshold ASER of 10^{-1} are 18, 20, and 22 mrad for SNR 5, 10, and 15 dB, respectively. For a 500m link distance, optimal θ_{FoV}, and SNR $>$ 7.5, the system exhibits good reliability in terms of ASER and outage probability for a boresight displacement up to 30 cm. Using laser source with $\mu < 0.25$ the proposed MPPM-E91 protocol outperforms OOK in terms of the RKR. System security against PNS attack is guaranteed at M $= 16$, while lower modulation orders introduces higher RKR at expense of increased chance of Eve's attack. The system's RKR is maximized by adapting the number of time bins according to the received SNR.

The validity of analytical results deduced in this paper was verified using the Monte-Carlo simulation that showed an exactly matching between the simulation and analytical results. The derived expressions and analytical results in this paper will help design and optimize such integrated systems. This study might further be extended to include the implementation of different QKD protocols, the Malaga distribution, which can be used as a general statistical model, and fine-tracking techniques.

REFERENCES

[1] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, "Quantum key distribution over FSO: Current development and future perspectives," in *Proc. Prog. Electromagn. Res. Symp. (PIERS-Toyama)*, Aug. 2018, pp. 1672–1679.

[2] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, "Secure quantum communication technologies and systems: From labs to markets," *Quantum Rep.*, vol. 2, no. 1, pp. 80–106, Jan. 2020.

[3] J. D. Morris, M. R. Grimaila, D. D. Hodson, D. Jacques, and G. Baumgartner, "A survey of quantum key distribution (QKD) technologies," in *Emerging Trends in ICT Security*. Amsterdam, The Netherlands: Elsevier, 2014, pp. 141–152.

[4] H. Zhao and M.-S. Alouini, "On the performance of quantum key distribution FSO systems under a generalized pointing error model," *IEEE Commun. Lett.*, vol. 23, no. 10, pp. 1801–1805, Oct. 2019.

[5] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1149–1205, 2nd Quart., 2018.

[6] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," *J. Lightw. Technol.*, vol. 24, no. 8, pp. 3114–3120, Aug. 7, 2006.

[7] N. Alshaer, T. Ismail, and M. E. Nasr, "Performance evaluation and security analysis of ground-to-satellite FSO system with CV-QKD protocol," *IET Commun.*, vol. 14, no. 10, pp. 1534–1542, Jun. 2020.

[8] Y.-M. Li, X.-Y. Wang, Z.-L. Bai, W.-Y. Liu, S.-S. Yang, and K.-C. Peng, "Continuous variable quantum key distribution," *Chin. Phys. B*, vol. 26, no. 4, pp. 1–7, 2017.

[9] N. Alshaer, M. E. Nasr, and T. Ismail, "Hybrid MPPM-BB84 quantum key distribution over FSO channel considering atmospheric turbulence and pointing errors," *IEEE Photon. J.*, vol. 13, no. 6, pp. 1–9, Dec. 2021.

[10] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *NPJ Quantum Inf.*, vol. 2, no. 1, pp. 1–11, Nov. 2016.

[11] C. H. Bennett and G. Brassard, "An update on quantum cryptography," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* New York, NY, USA: Springer, 1984, pp. 475–480.

[12] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[13] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[14] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992.

[15] T. Ismail, E. Leitgeb, and T. Plank, "Free space optic and mmWave communications: Technologies, challenges and applications," *IEICE Trans. Commun.*, vol. 99, no. 6, pp. 1243–1254, 2016.

[16] A. K. Majumdar, *Advanced Free Space Optics (FSO): A Systems Approach*. New York, NY, USA: Springer, 2014, vol. 186.

[17] Y. Kaymak, R. Rojas-Cessa, J. Feng, N. Ansari, M. Zhou, and T. Zhang, "A survey on acquisition, tracking, and pointing mechanisms for mobile free-space optical communications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1104–1123, 2nd Quart., 2018.

[18] J. H. Ryu, S. C. Kim, J. R. Ryoo, and S. Y. Yi, "Tracking control for free-space optical communication of unmanned aerial vehicle," in *IEEE 3rd Int. Conf. Commun. Inf. Syst. (ICCIS)*, Dec. 2018, pp. 132–136.

[19] B. Chen and H. Yu, "Visual tracking for mobile optical wireless communications," *Opt. Exp.*, vol. 28, no. 21, pp. 31119–31126, 2020.

[20] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, Nov. 2016.

[21] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Phys.*, vol. 3, pp. 481–486, Jun. 2007.

[22] Y. Cao, H. Liang, J. Yin, H.-L. Yong, F. Zhou, Y.-P. Wu, J.-G. Ren, Y. H. Li, G. S. Pan, T. Yang, and X. Ma, "Entanglement-based quantum key distribution with biased basis choice via free space," *Opt. Exp.*, vol. 21, no. 22, pp. 27260–27268, 2013.

[23] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, and G.-B. Li, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[24] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Drone-based entanglement distribution towards mobile quantum networks," *Nat. Sci. Rev.*, vol. 7, no. 5, pp. 921–928, May 2020.

[25] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Optical-relayed entanglement distribution using drones as mobile nodes," *Phys. Rev. Lett.*, vol. 126, no. 2, pp. 1–6, Jan. 2021.

[26] M. T. Dabiri, S. M. S. Sadough, and M. A. Khalighi, "Channel modeling and parameter optimization for hovering UAV-based free-space optical links," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 2104–2113, Sep. 2018.

[27] M. T. Dabiri, S. M. S. Sadough, and I. S. Ansari, "Tractable optical channel modeling between UAVs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 11543–11550, Dec. 2019.

[28] S. Khankalantary, M. T. Dabiri, and H. Safi, "BER performance analysis of drone-assisted optical wireless systems with APD receiver," *Opt. Commun.*, vol. 463, pp. 1–7, May 2020.

[29] K. Dautov, S. Arzykulov, G. Nauryzbayev, and R. C. Kizilirmak, "On the performance of UAV-enabled multihop V2 V FSO systems over generalized $\alpha - \mu$ channels," in *Proc. Int. Conf. Comput. Netw. Commun. (CoCoNet)*, Aug. 2018, pp. 69–73.

[30] J.-G. Ren, J. Yin, B. Yang, F. Zhou, Z.-H. Yi, C.-Z. Peng, R. Shu, and J.-Y. Wang, "Time synchronization for quantum key distribution from ground to satellite," *J. Infr. Millim. WAVES*, vol. 30, no. 4, pp. 381–384, Mar. 2012.

[31] A. Pljonkin, K. Rumyantsev, and P. K. Singh, "Synchronization in quantum key distribution systems," *Cryptography*, vol. 1, no. 3, pp. 1–9, 2017.

[32] J. Williams, M. Suchara, T. Zhong, H. Qiao, R. Kettimuthu, and R. Fukumori, "Implementation of quantum key distribution and quantum clock synchronization via time bin encoding," *Proc. SPIE*, vol. 11699, Mar. 2021, Art. no. 1169908.

[33] Z. Wang, R. Malaney, and B. Burnett, "Satellite-to-earth quantum key distribution via orbital angular momentum," *Phys. Rev. A, Gen. Phys.*, vol. 14, no. 6, pp. 1–15, Dec. 2020.

[34] G. Keiser, *Optical fiber communications*. New York, NY, USA: McGraw-Hill, 1983.

[35] H. Zhou and G. Wornell, "Adaptive pulse-position modulation for high-dimensional quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 359–363.

[36] T. Ismail, E. Leitgeb, Z. Ghassemlooy, and M. Al-Nahhal, "Performance improvement of FSO system using multi-pulse pulse position modulation and SIMO under atmospheric turbulence conditions and with pointing errors," *IET Netw.*, vol. 7, no. 4, pp. 165–172, Jul. 2018.

[37] X. Liu, X. Yao, H. Wang, H. Li, Z. Wang, L. You, Y. Huang, and W. Zhang, "Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km," *Appl. Phys. Lett.*, vol. 114, no. 14, pp. 141104–141109, 2019.

[38] N. Alshaer, T. Ismail, and M. E. Nasr, "Generic evaluation of fso system over mÃİlaga turbulence channel with mppm and non-zero-boresight pointing errors," *IET Commun.*, vol. 14, no. 18, pp. 1534–1542, 2020.

[39] H. J. Lee, H. Kim, M. Cha, and H. S. Moon, "Simultaneous type-0 and type-II spontaneous parametric down-conversions in a single periodically poled $KTiOPO_4$ crystal," *Appl. Phys. B, Lasers Opt.*, vol. 108, no. 3, pp. 585–589, Sep. 2012.

[40] S. Magnitskiy, D. Frolovtsev, V. Firsov, P. Gostev, I. Protsenko, and M. Saygin, "A SPDC-based source of entangled photons and its characterization," *J. Russian Laser Res.*, vol. 36, no. 6, pp. 618–629, Nov. 2015.

[41] D. Bouwmeester and A. Zeilinger, *The Physics of Quantum Information*. Berlin, Germany: Springer, 2000.

[42] M. A. Itzler, X. Jiang, R. Ben-Michael, B. Nyman, and K. Slomkowski, "Geiger-mode APD single photon detectors," in *Proc. Opt. Fiber Commun. Conf.*, 2008, pp. 1–4.

[43] K. E. Kolb, "Signal-to-noise ratio of geiger-mode avalanche photodiode single-photon counting detectors," *Opt. Eng.*, vol. 53, no. 8, Mar. 2014, Art. no. 081904.

[44] R. Abdelfatah, A. Moawad, N. Alshaer, and T. Ismail, "UAV tracking system using integrated sensor fusion with RTK-GPS," in *Proc. Int. Mobile, Intell., Ubiquitous Comput. Conf. (MIUCC)*, May 2021, pp. 352–356.

[45] V. Gudmundsson, H. Kristinsson, S. Petersen, and A. Hasan, "Robust uav attitude estimation using a cascade of nonlinear observer and linearized Kalman filter," in *Proc. Dyn. Syst. Control Conf.*, 2018, pp. 1–10.

[46] P. Marantos, C. P. Bechlioulis, and K. J. Kyriakopoulos, "Robust stabilization control of unknown small-scale helicopters," in *Proc. Int. Conf. Robot. Automat. (ICRA)*, May 2014, pp. 537–542.

[47] R. G. Valenti, I. Dryanovski, and J. Xiao, "A linear Kalman filter for MARG orientation estimation using the algebraic quaternion algorithm," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 2, pp. 467–481, Feb. 2015.

[48] X. Tong, Z. Li, G. Han, N. Liu, Y. Su, J. Ning, and F. Yang, "Adaptive EKF based on HMM recognizer for attitude estimation using MEMS MARG sensors," *IEEE Sensors J.*, vol. 18, no. 8, pp. 3299–3310, Apr. 2018.

[49] H. G. de Marina, F. J. Pereda, J. M. Giron-Sierra, and F. Espinosa, "UAV attitude estimation using unscented Kalman filter and TRIAD," *IEEE Trans. Ind. Electron.*, vol. 59, no. 11, pp. 4465–4474, Nov. 2011.

[50] G. Welch and G. Bishop, *An Introduction to Kalman Filter*. NC, USA: Citeseer, 1995.

[51] Y. S. Suh, "Orientation estimation using a quaternion-based indirect Kalman filter with adaptive estimation of external acceleration," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 12, pp. 3296–3305, Dec. 2010.

[52] N. Trawny and S. I. Roumeliotis, "Indirect Kalman filter for 3D attitude estimation," Dept. Comput. Sci. Eng., Univ. Minnesota, Minneapolis, MN, USA, Tech. Rep, 2005, pp. 1–25, vol. 2.

[53] D. J. Attitude, *Euler Angles, Unit Quaternions, and Rotation Vectors*. Stanford, CA, USA: Stanford Univ., 2006.

[54] F. Yang, J. Cheng, and T. A. Tsiftsis, "Free-space optical communication with nonzero boresight pointing errors," *IEEE Trans. Commun.*, vol. 62, no. 2, pp. 713–725, Feb. 2014.

[55] K. Kiasaleh, "Channel estimation for FSO channels subject to gamma–gamma turbulence," in *Proc. Int. Conf. Space Opt. Syst. Appl. (ICSOS)*, Corsica, France, Oct. 2012, pp. 1–7.

[56] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *J. Lightw. Technol.*, vol. 25, no. 7, pp. 1702–1710, Jul. 1, 2007.

[57] P. Beckmann and A. Spizzichino, *The Scattering of Electromagnetic Waves From Rough Surfaces*. Norwood, MA, USA: Artech House, 1987.

[58] A. E. Morra, H. S. Khallaf, H. M. H. Shalaby, and Z. Kawasaki, "Performance analysis of both shot- and thermal-noise limited MultiPulse PPM receivers in gamma–gamma atmospheric channels," *J. Lightw. Technol.*, vol. 31, no. 19, pp. 3142–3150, Oct. 15, 2013.

[59] T. Ismail, E. Leitgeb, Z. Ghassemlooy, and M. Al-Nahhal, "Performance improvement of FSO system using multi-pulse pulse position modulation and SIMO under atmospheric turbulence conditions and with pointing errors," *IET Netw.*, vol. 7, no. 4, pp. 165–172, Jul. 2018.

[60] N. Alshaer, T. Ismail, and M. E. Nasr, "Generic evaluation of FSO system over Málaga turbulence channel with MPPM and non-zero-boresight pointing errors," *IET Commun.*, vol. 14, no. 18, pp. 3294–3302, Nov. 2020.

[61] *Wolfram.Functions*. Accessed: Nov. 15, 2020. [Online]. Available: https://functions.wolfram.com/HypergeometricFunctions/MeijerG/21/02/03/01/

[62] S. Yu, J. Ding, Y. Fu, J. Ma, L. Tan, and L. Wang, "Novel approximate and asymptotic expressions of the outage probability and BER in gamma–gamma fading FSO links with generalized pointing errors," *Opt. Commun.*, vol. 435, pp. 289–296, Mar. 2019.

[63] D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, "Free-space quantum links under diverse weather conditions," *Phys. Rev. A, Gen. Phys.*, vol. 96, no. 4, pp. 1–14, Oct. 2017.

[64] D. Vasylyev, W. Vogel, and A. A. Semenov, "Theory of atmospheric quantum channels based on the law of total probability," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 6, pp. 1–14, Jun. 2018.
[65] Y. Zhang and I. B. Djordjevic, "Generalized PPM-based BB84 QKD protocol," in *Proc. 16th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2014, pp. 1–4.
[66] K. Kolb and D. F. Figer, "GM-APD imaging arrays for direct imaging of exoplanets," in *Proc. IEEE Aerosp. Conf.*, Mar. 2015, pp. 1–9.

NANCY ALSHAER (Member, IEEE) received the Ph.D. degree in optical free-space communication with quantum-key distribution, in 2020. She is currently a Lecturer at the Department of Electronics and Electrical Communication, Faculty of Engineering, Tanta University, Egypt. She is also a CoPI in a funded project supported by the Science, Technology and Innovation Funding Authority (STIFA) of Egypt. She has a research collaboration with the National Institute of Laser Science, Cairo University, and the Wireless Intelligent Research Center, Nile University, Egypt. Her research interests include optical and wireless communications, quantum key distribution, quantum random number generation, tracking systems, and mobile edge computing.

AHMED MOAWAD received the B.Sc. degree in telecommunication (Hons.) from the Department of Aerospace, Faculty of Engineering, Cairo University, Egypt, in 2019. He is currently pursuing the M.Sc. degree with Nile University, Egypt. He was as a Research Assistant at the Wireless Intelligent Research Center (WINC), Nile University. His research interests include aerospace, tracking and control systems, and machine learning.

TAWFIK ISMAIL (Senior Member, IEEE) was an Associate Professor with the National Institute of Laser Enhanced Sciences, Cairo University, Egypt. He was also a Postdoctoral Research in optical and wireless communications with the Technical Institute of Microwave and Photonic Engineering, University of Graz, Austria, in 2015. In 2018, he joined the Optical Wireless Communication Research Group, Department of Engineering and Sciences, University of Oxford, U.K., to work in the research of quantum communication in free space. He is currently the Director of the Wireless Intelligent Networks Research Center (WINC), Nile University. Since 2014, he has been with several research projects funded nationally by NTRA, ASRT, STDF, and ITIDA, Egypt, and internationally by Innove UK, U.K. In addition, he has research stays at the Technical Institute of Microwave and Photonic Engineering, University of Graz; The American University in Cairo, Egypt; Cairo University; and the Malaviya National Institute of Technology, India. He has established and led a research group for optical and wireless communications at Cairo University. His research interests include optical and wireless communications, mmWave, mobile edge computing, quantum cryptography, information security, blockchain, artificial intelligence, and machine learning applications in optical and wireless communication systems.