Chapter

Advancements in Optical Data Transmission and Security Systems

Menachem Domb

Abstract

Optical Communication (OC) for data transmission was introduced more than 30 years ago. It employs two main technologies, fiber optics using a physical wire and Free Space Optical (FSO) wireless transmission. Fiber optics has been well developed over the years in terms of distance, bandwidth, speed, reliability, and other enhancements that contribute to its use. Recent developments in FSO transmission has made it the mainstream and a better alternative compared to RF wireless transmission, concerning all parameters. In this chapter, we focus on advancements in OC that represent innovative ideas of how to enable new methods of secured optical data transmission in different ways and not simply as an extension to current methods and technologies.

Keywords: optical communication, free space optical (FSO), security, multiplexing, network coding (NC), optical wireless communication (OWC), orbital angular momentum (OAM), quantum key-distribution (QDK)

1. Introduction

The use of wireline and wireless communications is very common in a wide range of devices. The increased complexity of the core transmission systems is reflected in a set of advancements in data communications and specifically in Optical Communication [1]. The elastic Optical Network (EON) concept is an optical network architecture able to support the increased need for elasticity in allocating optical network resources. Flexible bandwidth allocation is performed to adapt to different transmission techniques, such as Orthogonal Frequency Division Multiplexing (OFDM), Nyquist WDM (NWDM), transponder types (BVT1, S-BVT), modulation formats (QPSK, QAM), and coding rates. This flexibility makes resource allocation much more challenging. Dynamic control, enables on-demand reconfiguration, virtualization, and reconfiguring the optical setup poses challenges in terms of network re-optimization, spectrum fragmentation, amplifier power settings, which requires strict integration between the control elements (controllers and orchestrators) and optical monitors working at the hardware level. EON is just an example of the recent expansion of the optical communication area. Hence, more information is presented in the rest of this chapter.

The chapter is organized as follows: Section 2 provides an overview of recent OC advancements in terms of capacity, speed, and error handling. Section 3 provides a brief overview of the security issues and corresponding solutions in the physical

layer of OC. In Section 4 we describe new concepts and technologies in implementing advanced OC capabilities. Section 5 presents two examples of constraint situations where OC provides the best solution in terms of capacity, throughput, and security strength. In Section 6 we describe the use of OC for ultra-distance and ultra-secure free-space key exchange mechanisms and in Section 7 we describe in detail a unique use of OC for secured key exchange. Section 8 provides the summary and conclusions of this chapter.

2. OC super-channel with high speed and high capacity

In this section, we outline recent advancements in optical communications concerning capacity, speed, and security. Recent demands for high-speed optical transmission technology triggered the development of advanced modulation formats, such as dual polarization-1024-level-quadrature amplitude modulation, ultra-fast digital-to-analog converters at the transmitter terminal, and nonlinearity intolerance. A new technology called super-channel [2], provides a feasible solution that offers very high-speed, long-distance, spectral-efficient, and large data capacity links with reliable performance. It involves the use of multiple sub-carriers for data transmission over a single-channel using dual polarization-quadrature phase shift keying (DP-QPSK). These unique modulation formats have a capacity of more than 100 Gbps over a single channel. However, they suffer from multipath fading, nonlinearity loss, and phase distortion loss, and limitation of maximum supported links. These limitations are mitigated using coherent detection and digital signal processing (DSP) at the receiver terminal for enhanced performance. In Nyquist-WDM super-channel transmission, the spectral-efficiency of the link is improved by transmitting independent wavelength channels using lower-order advanced modulation formats with channel spacing equal to the baud rate of the system. Experiments demonstrated the transmission of 1 Tbps data over a 7200 km transoceanic link with 2.86 bits/s/Hz spectral efficiency using a digital Nyquist-WDM super-channel.

The transmission of 1.232 Tbps using DP-QPSK signals with a noise-suppressed Nyquist-WDM super-channel transmission over 2100 km single-mode fiber link with DSP at the receiver terminal for enhanced performance. The performance of dual polarized-binary phase shift keying, DP-QPSK, dual polarized-8-level-quadrature amplitude modulation, and DP-16-QAM based Nyquist-WDM super-channel transmission over pure silica-core fiber with Raman amplification. In high-speed optical fiber links, the main causes of signal deterioration are Kerr nonlinearities, polarization mode dispersion, chromatic dispersion, and optical fiber cable attenuation which limit the maximum link capacity. In contrast, in FSO links, signal attenuation offered by the external environmental condition is the main factor that determines the link performance.

Optical communication is sensitive to various environmental interference and noise, leading to transmission errors [3]. The main reasons are wind misalignment, beam divergence due to propagation, weather tempering losses due to fog, smoke, and snow, atmospheric turbulence, and background noise due to artificial lights, and in FSO the optical beam position may be missed due to misalignment between the transmitter and receiver structures.

To mitigate these effects new modulation schemes have developed such as on–off keying (OOK), forward error correction (FEC), pulse width modulation (PWM), pulse position modulation (PPM), multiple PPM, digital pulse interval modulation (DPIM), binary phase-shift keying (BPSK), concatenated RS codes, short hops systems leading to performance improvements, turbo codes, low-density parity-check codes, and spatial diversity.

Practical testing and simulations [4] of PPM show that the probability of error is minimum for the maximum likelihood estimate of the stationary beam position, and for the dynamically varying beam position, a filter with a large number of particles provides a close-to-optimal probability of error performance.

3. OC security threats and solutions

The continuous evolution of optical networks in terms of heterogeneity, flexibility, applications, data flow volume, bandwidth, and reliable performance, raises security issues which are unique to OC. Optical networks are vulnerable to several types of security breaches aiming to disrupt the service or gain unauthorized access to the system. The evolution of programmable and flexible node architecture software has resulted in new security vulnerabilities that need to be considered during network design and operation. This section provides an overview of potential security issues in current and future optical networks and identifies possible attacks that utilize the associated vulnerabilities. It includes privacy, authentication, integrity, denial of service, and confidentiality. An attacker can snoop by tapping into the optical fiber or by interference radiated from an adjacent spectrum of confidential signals and go undetected for quite some time. An overview of common security issues and attack methods targeting optical networks is presented below.

- **Eavesdropping** is a major security attack in optical networks. Eavesdropping entails breaching the encryption key by removing the fiber coating and bending the fiber to cause the signal to leak out of the core into a photodetector that captures the information. To detect such intrusions, the network uses an intrusion detection alarm, triggered by insertion loss changes in fiber connections. Such detections require an active monitoring system that runs across the network.

- **Monitoring ports** allow access to the channel, which is available in different network components, such as amplifiers, wavelength selective switches (WSSs), or multiplexers. The optical signal is mirrored by an optical splitter to allow the connection of monitoring devices without traffic interruption. By obtaining onsite access, an attacker can use these ports to capture the carried traffic. To protect the carried data from eavesdropping, encryption is implemented in the optical transponders. Encryption keys transferred over the network are isolated from the data load.

- **Insertion of harmful signals**: service denial and quality degradation occur when harmful signals are inserted into the network, such as excessive power optical signals that exceed the signal level used in the network.

- **Jamming signals:** Networks comprising Optical Add-Drop Multiplexers (OADMs) with variable optical silencers, high-power signals can damage the co-propagating user signals inside its optical fibers, amplifiers, and switches. Jamming signals can also affect normal signals by increasing the in-band crosstalk. Signals traversing common physical links with the jamming signal can suffer from out-of-band effects. Lead to out-of-band crosstalk by leaking to adjacent channels and increasing non-linear effects and gain competition, and instead of legitimate signals the stronger jamming signals are amplified, making the situation much worse.

- **Alien wavelength attacks**: Alien wavelength [5] refers to the ability to share the same fiber-optic-line by multiple telecom-service-providers. It is possible by "dividing" the communication line into separated "colors" or wavelengths such that each "color" is considered as a separate communication channel. Each provider uses one "color" and can transmit its data concurrently with others using the same physical fiber line. This technology expands the utilization of the fiber line. The possibility of Alien Wave insertion without any impact to existing services has a big advantage to the telecom industry.
  Alien wavelengths are implemented in the network to allow network upgrades and efficient transmission of high-capacity connections over the existing infrastructure. When there is no alien wavelength support, each connection is terminated and regenerated by a node at the edge of the domain, while alien wavelengths can pass through multiple domains without optical conversions, which create vulnerability in network security, especially due to the lack of control on the performance of the alien channels. In such systems, alien wavelengths can be subjugated to jamming risking the network. To overcome this security hazard, a control system is required to block any unauthorized messaging.

- **Mixed line rate** (MLR) networks enable the coexistence of different modulation formats in the same infrastructure. A severe security vulnerability of MLR networks stems from nonlinear effects between high-speed and low-speed signals of adjacent channels. Amplitude-modulated on–off-keyed (OOK) 10G channels deteriorate the quality of the higher bitrate, due to cross-phase modulation (XPM). This entails an extra penalty for the higher speed channels, depending on the modulation format and channel launch power. A service degradation attack in MLR networks is caused by inserting an OOK channel nearby a high-speed channel, without allowing sufficient guard band. Thus, the attacking signal could significantly deteriorate the legitimate signals.

- **Software-defined networking (SDN**) manages the interface between the hardware and the SDN applications, including traffic engineering and data collection applications. Malicious attackers who can gain access to the data potentially may hijack the network.

- **Architecture on Demand (AoD)** uses an optical backplane to support interconnections among optical modules enabling the use of these modules, which are required for switching and processing. New modules are added to a node by plugging them into the optical backplane. This modularity exposes the network to security vulnerabilities.

Network Coding (NC) proposed to cope with physical OC security issues:

Network Coding (NC) is used in optical networks for protection against link failures, to improve spectral efficiency in multicasting, and protect confidential connections against eavesdropping attacks. The confidential signals are XOR-ed with other signals transmitted via different nodes in their path through the network. The signals are combined either at the source node or at intermediate nodes. To implement NC for confidential connections, a set of constraints for the NC and RSA are incorporated in the corresponding algorithms. The combination of signals through NC increases the security of confidential connections since an eavesdropper will receive a combination of signals from different connections, complicating the decryption of the confidential signal. Experiments show that NC provides comprehensive security envelop for confidential connections with minimum spectrum usage.

Using NC, connection data is merged with other connection data, generating a network-code that changes based on the connection's transmitted data. Encrypted Transmission (ET) relates to all links of the selected path transmitting an encrypted version of their data with at least one XOR operation with other established connections. To satisfy the ET constraint, an established connection has at least two common nodes with a confidential connection. The Frequency Slot Matching (FSM), which is a subset of the frequency slots utilized by the confidential connection, must have the same id and frequency as the slots of the rest of the established connections used in the XOR operations. It is assumed that the signals used for the XOR operation are on the same frequency. Thus, an established connection with at least two common nodes with the confidential connection can either provide security for the entire path of the confidential demand (source and destination as common nodes), or it can provide security for part of the connection (source/intermediate node to intermediate/destination node). For a confidential connection to be considered secure, the selected established connections must collectively secure all links of that connection. The confidential connection is considered as secure even if only part of the signal is XOR-ed since the eavesdropper would still have to access all connections used in the encryption process to decrypt the transmitted data.

4. Selected technologies in implementing OC capabilities

The demand for very large capacity and high-speed channels for heavy data transmission is growing increasing the demand for quick solutions. As a result, we are witness to a wide variety of proposed solutions using optical fiber and free-space wireless channels. Several solutions that have successfully coped with the transmission demand and the security challenges are presented below.

4.1 OAM multiplexing for high capacity secured optical communications

In this section, we outline recent advances in the use of Orbital Angular Momentum (OAM) to increase transmission capacity and speed [6]. It employs the orthogonality among OAM beams to enable efficient demultiplexing. Free-space communication links are widely used for data transfer applications, using optical communication or radiofrequency (RF) waves. The capacity of a communication system is increased by multiplexing and simultaneously transmitting multiple independent data streams. This is done by using the properties of the electromagnetic (EM) wave, such as time, wavelength, and polarization. Multiple data streams can be efficiently multiplexed and demultiplexed. To cope with the increasing demand for very high bandwidth, new forms of data channel multiplexing are used. One approach utilizes orthogonal spatially overlapping and copropagating spatial modes, where multiple channels, each identified by a different spatial mode, are multiplexed at the transmitter and separated at the receiver. The transmission capacity and spectral efficiency are increased by a factor equal to the number of transmitted spatial modes. Each data symbol is sequentially transmitted by a different OAM beam, within each time slot. A group of orthogonal OAM beams is used to spatially multiplex multiple data streams. Combining OAM multiplexing with polarization we can get very high xTpbs speed communications such as four OAM beams on each of the two orthogonal polarizations are combined resulting in multiplexed eight OAM modes. The received OAM beams are then de-multiplexed at the receiver and sequentially detected to recover the data streams. All eight OAM data channels are located on the same wavelength, providing spectral benefits. Then the experiment was expanded by adding the wavelength dimension, simultaneously

using OAM, polarization, and wavelength for multiplexing. A total of 1008 data channels were carried by 12 OAM values, two polarizations, and 42 wavelengths. Each channel was encoded with 50GBd quadrature phase-shift keying, providing an aggregate capacity of 100.8 Tbps. An additional experiment described the multiplexing process where multiple independent data channels, each on a different OAM beam, are spatially combined, and the resulting multiplexed OAM beams are then transmitted via a single aperture towards the receiver. After coaxially propagating through the same free-space channel, the arriving beams are collected at the receiver by another slot, and subsequently demultiplexed and detected for data recovery.

4.2 Chaos-based high-speed and high bandwidth secure OC

Chaotic systems provide physical layer security in secure OC [7]. This began with a data rate of 2.4 Gbps for a distance of 120 km, and later was improved to 10-Gbps for a 100-km optical fiber link and even further to 30-Gbps secure transmission over 100 km using a chaotic carrier with a bandwidth of 10 GHz. The transmission capacity of chaos-based secure communication is limited by the bandwidth of the chaotic carrier. The wider the bandwidth of the chaotic carrier the higher the transmission rate it supports. To enhance the bandwidth of chaos, several methods have been proposed such as optical injection, mutual injection, fiber propagation, feedback with parallel-coupling ring resonators, heterodyning couplings, and self-phase-modulated feedback with microsphere resonator.

Following is a description of an enhanced wideband chaos generation scheme. To increase bandwidth, it is using an external-cavity semiconductor laser (ECSL) subject to optical-electronic hybrid feedback. The output is used to modulate the output of a continuous-wave laser by an electro-optical phase modulator. The constant-amplitude self-phase-modulated light is then inserted back into the ECSL. Experiments indicate that the effective bandwidth of the generated chaos is increased to over 20 GHz, and the spectrum flatness and the complexity of the generated chaos. The experiments demonstrated that high-quality synchronization between two wideband chaos signals with an effective bandwidth greater than 20 GHz is achieved, showing the valuable potential in chaos-based secure communication, such as enhancing the transmission capacity and improving the security. The experiments prove that the significant bandwidth and the complexity enhancement of chaos are achieved in the proposed chaos generation scheme. Results indicate that the proposed scheme can easily obtain a wideband chaotic signal with an effective bandwidth larger than 20 GHz.

4.3 Intensity modulation signals for physical layer security of optical communications

The huge volume of data transmitted over optical networks requires the integration of a data protection mechanism adapted to the specific attributes of optical fiber communications. Y-00 [8] quantum-noise randomized stream cipher is built to prevent attackers from capturing the transmitted encrypted text. It merges the mathematical encryption of multi-level signaling and the physical randomness, thereby providing high performance and robust security. It uses extremely high-order modulation together with quantum and additive noises. The achieved secrecy level is high as the probability of the attackers guessing the encrypted data is very low. Experiments show that the Y-00 cipher transceiver on a 1000-km transmission range, with a data rate of 1.5-Gbps and using analytical high secrecy, performed successfully.

Y-00 cipher is a symmetric key encryption method combined with multi-level signaling of physical randomness to hide the transmitted ciphertext. A receiver recovers the original signal of plaintext from the cipher signal masked with noise using a shared key and mathematical signal processing. The light from a laser diode enables the cipher signal transmission to the receiver. The Quantum/ASE randomized noise cipher is dominant when the Y-00 cipher communication system is used in a long-haul link using optical amplifiers. Hence, masking the signal with an additive quantum noise is more robust against attackers and is a practical advantage compared to classical cryptography utilizing just mathematical encryption. The probability that an attacker will guess the correct encrypted text is considerably low under such assumptions.

4.4 Optical wireless communication (OWC), the underlying technology for 5G and IoT

The availability of 5G communications and the Internet of Things (IoT) exponentially increase the number of devices connected to the internet, generating a huge volume of transmitted data [9]. The main features of the 5G communication services include high capacity, low latency, high security, vast device connectivity, low energy consumption, and high quality of experience (QoE). OWC seems to satisfy the derived requirements by its unique attributes: wide spectrum, high-data-rate, low latency, high security, low cost, and low energy consumption. OWC contains visible light communication (VLC), light fidelity (LiFi), optical camera communication (OCC), and free-space optics (FSO). Its technologies may play the role of sensing, monitoring, and resource sharing in comprehensive device connectivity of IoT, and meet 5G and IoT high-security requirements. Hence, OWC is the right fit for 5GB and IoT.

The VLC uses light-emitting diodes (LEDs) or laser diodes (LDs) as transmitters and photodetectors (PDs) as receivers. Only visible light (VL) is used as the communication medium in the VLC. LiFi provides high-speed wireless connectivity along with illumination and uses LEDs or defuse LDs as transmitters and PDs as receivers. It uses VL for the forward path and infrared (IR) as the communication medium for the return path. The OCC uses a LED array as a transmitter and a camera as a receiver. FSO uses LD and PD as the transmitter and the receiver, respectively. It is normally operated using Appl. Sci. IR as the communication means but can also use VL and UV. There are several OWC technologies. The differences between these technologies are very specific. The unique characteristic of VLC is the use of visible light as a communication media. A LiFi system supports seamless mobility, bidirectional communication, and point-to-multipoint, as well as multipoint-to-point communications. The OCC system uses a camera or image sensor as a receiver among all the OWC technologies. The OCC uses an LED array or light as a transmitter and a camera or image sensor as a receiver. OCC normally uses VL or IR as the communication medium.

The transmission rate of the 5G mobile communication systems is expected to reach an average of 1 Gbps at a 10 Gbps peak rate. An external network hacker device cannot pick up the internal optical signal. The information can be exchanged in a highly secure manner. In summary, the OWC systems offer a higher level of security for the 5G/6G and IoT networks.

5. Unique implementations of OC under constraints

The incorporation and spread out of OC technologies are dictated by the benefits and impact it is expected to achieve. Hence, most of the efforts are towards the

long-distance, high capacity, high bandwidth, and high data rate. However, some efforts are put towards local solutions and small-scale implementations. The following are two examples of such implementations.

5.1 OC for short distance high-speed data transmission

Data-center networks have much shorter transmission distances but much higher transmitted data than common network topologies [10]. Therefore, traditional telecommunication components are redundant and costly. Consequently, VCSELs, active optical cables, and parallel fiber transmission are used by data centers. With the significant increase in traffic inside the data center, the required bandwidth is increasing dramatically. Broadband optical modulators such as electro-absorption modulators (EAMs) and Mach–Zehndermodulators (MZMs) in combination with colored distributed feedback laser arrays are combined to build and Ultra-high-bandwidth and low energy links based on WDM technology. To further increase to Tbps bandwidth, a large number of lasers are used.

Another improvement is gained by using Optical switches which are completely different from electronic packet switches but when combined they complement each other. Hence, optical switches and conventional electronic switches are combined in the same architecture generating improved performance. Optical switches are used to adapt the network to specific traffic patterns, such as pairs of nodes exchanging high traffic levels that can have more bandwidth when using optical networks. However, the reconfiguration of an optical switch requires phase-locking and modifications of the routing tables. To overcome this issue and improve performance, optical reconfigurations are fully automated. Improving the utilization of the resources by reconfiguration of disaggregated elements enables the reduction of components and energy consumption by putting underused components in a sleep mode. It is possible to mitigate network congestion resulting from intense communications between servers or rack pairs by overprovisioning the network.

5.2 Integrating OC and mobile devices used in the automotive and drone industry

Automotive: Until a few years ago, only minor improvements have been implemented in the data networks used in vehicles. The introduction of autonomous vehicles and smart cities has increased the demand for automation of vehicles and inter-vehicle communication [11]. This involves the reliable transmission of data with high rates in real-time and secured from interfering signals and security attacks. Existing and vehicle-bus-communications are insufficient, and a replacement of the vehicle communication infrastructure is inevitable. Optical data communication has been implemented as it transmits high amounts of data, can multiplex several signals into a single fiber, and is robust against external effects, with little attenuation. This confirms that optical busses are very useful for automotive applications. The solution is based on a central processing unit CPU connected to the optical hybrid data bus, which comprises several fibers. To improve reliability, safety, and security, separate fibers are used for different applications and functionalities such as multimedia and sensors. The CPU forwards messages to the different fibers. In automotive applications assigning priorities to messages is required for accurate functionality. Therefore, SCTP is used as it supports ordering messages and it provides redundant paths to increase reliability. SCTP uses heartbeats to check if a connection is still valid. If a node fails, the connection will find another path, if available. The SCTP protocol also has additional security features and adaptability, which will support new vehicle communication requirements in the future.

UAV: [12] In recent years the availability and common use of drones have increased, especially the grouping of drones to perform a common task, which requires ongoing precise synchronization of the engaged drones in real-time. This is achieved by a platform of high speed and high capacity communication channels that virtually connect these drones. A technology that benefits from both, optical data rates and the mobility of drones is required. Free-space optical (FSO) communication supports the optical wireless signal transmission from the infra-red band spectrum in outdoor environments. This combined with the mobility-based outdoor communication system is the correct direction that should be considered. Optical Wireless Communications (OWC) embedded in Unmanned Aerial Vehicles (UAV) is the compound technology used.

6. Quantum key-distribution (QDK) using OC

QKD uses light-paths via optical fibers to share encryption keys between two remote parties [13]. The key-updating process and the key adaptive routing have dedicated paths protected from link failures. Sharing quantum keys between satellites requires communication channels among microsatellites capable of transmitting keys within constellations of trusted satellites. Using optical links with 10-yard pointing accuracy allows QKD of an inter-satellite distance of 400 km. In entanglement based QKD, pairs of entangled photons are generated and sent to two separate parties, where each is sent one photon from each pair. The two parties independently make measurements on a preselected property of their polarization state. Once many such pairs have been distributed and measured, the two parties perform statistical tests and ask if the received photons were entangled. Provided the entanglement measured exceeds a predefined threshold and their hardware is free of vulnerabilities, they can be sure that the security of the protocol. Then they use their private knowledge of the quantum states as a common source of entropy to derive symmetric keying material for encryption schemes.

A Quantum Module (QM) is a polarization-entangled photon-pair source and single-photon detectors that can operate as a qubit transmitter or receiver. The transmitting QM locally measures and timestamps one of the photons in each pair and sends the other photon of each pair to the receiver, where it is detected and timestamped by a receiving QM. These timestamps and measurement outcomes are used to synchronize the detections and subsequently to create a symmetric encryption key. The QM contains a laser diode that initiates spontaneous-parametric-down-conversion in beta-barium-borate crystals generating pairs of photons with specific wavelengths. The photons in each pair are entangled such that their polarization states are undefined until a measurement is made, at which point they will have correlated polarizations. In the transmitter QM, “signal” photons are transmitted, and the “idler” photons are detected within the QM by silicon avalanche photodiodes. Both satellites have a QM and both can send and receive entangled signal photons. The two satellites use a beacon laser and a beacon detector to monitor the other satellite’s beacon and control the relative pointing between them. A beam pointing correction signal is provided to a two-axis fast steering mirror, which compensates for high-frequency beam misalignment between the two spacecraft and optimizes the optical link for the transmission of entangled photons. The optical bench provides thermal and mechanical isolations and it is attached to the spacecraft structure. The reaction wheels have been placed, so that their spin axes are as near as possible to the center of gravity to minimize jitter of the pointing stability of the telescope.

7. Secured key-distribution using optical communication

Key distribution is a growing concern for symmetric cryptography. Most of the current key-distribution mechanisms assume the use of the Internet and WAN public networks, which are exposed to security risks. Robust cryptographic mechanisms, such as Diffie-Helman (DH) and RSA algorithms are used along with Certificate Authority (CA), which generates certificates and distributes them simultaneously to the sender and receiver via alternate channels. These existing solutions are limited. DH and RSA are at threat since the introduction of Quantum computing and PKI/CA are effective in relatively local cases. Hence, new ideas are required. This section introduces a new approach for a safe key transmission using high-speed optical camera communication (OCC), Visible light communication (VLC) is a type of wireless communication. The data is transmitted through modulating the visible light spectrum. The key transfer is done using VLC with blinking LED lights in a specific sequence and frequency, following a coding system. The receiver decodes the received blinks to a bit string using a corresponding image processing application. Optical communication ensures secure transfer without the ability to quote it. Experiment results show that this method is feasible, robust, efficient, and implementable.

7.1 Introduction

In symmetric cryptography, the same key is used for encrypting and decrypting the exchanged data. Sharing the same key requires a key transmission between the sender and the receiver. To avoid key discovery while transmitted, several protocols have been proposed, such as the Diffie-Hellman protocol and Asymmetric Cryptography such as RSA. The evolvement of Quantum Computing makes redundant any known cryptography. Using a reliable third-party able to generate certificates and encryption keys and simultaneously distributes it to the two parties who intend to exchange data. It is using alternate distributing channels different from the channel the two parties use for transferring the data. However, due to the growing globalization and growing distance among users and systems, and the introduction of cloud computing, this approach is complicated to manage and so became irrelevant over time. A secured key transition uses an optical communication platform.

7.2 Related work

Optical communication is simple, low cost and secured signal transmission. One of the technics is based on under-sampled differential phase shift on–off keying that can encode binary data. Arai et al. [14] define a new framing approach for high-speed optical signals transmission for road-to-vehicle communication. Luo et al. [15] use dual LED to triple the data rate transmission. Roberts [16] proposes encoding/decoding, using camera-subsampling synchronized with the camera frame rate. Leu et al. [17] introduce a new modulation scheme where the phase difference between two consecutive samples represents one-bit data.

7.3 Optical camera communications (OCC)

The optical communication technique called Optical Camera Communications (OCC) is described in [18]. OCC allows the use of huge unregulated bandwidth in the optical domain spectrally located between microwave and X-ray wavelengths, as shown in **Figure 1**. In such a system, an image sensor and a camera are used

to demodulate the transmitted signal which has been modulated according to on–off keying (OOK). Currently available devices are smart devices equipped with LED flash and cameras. This provides a pragmatic form of an Optical Wireless Communication (OWC) where LED projectors to provide the Visible Light spectrum (VLC) component and a camera as the receiving module, building a transceiver pair.

The OCC system uses commercial LED lighting sources that include, LED-based infrastructure lighting, LED flashes, LED tags, displays, laser diodes, image patterns, some current generation projectors. The major driving forces of OCC deployment are the widespread availability of visible light (VL) LEDs and the possibility of utilizing the camera in the smart devices to decode LED modulated data. Therefore, these LED infrastructures can be used for data transmissions using on–off keying (OOK).

A typical OCC system is shown in **Figure 2**, where a camera is used as a receiver, which consists of an imaging lens, image sensor, and readout circuit.

7.4 Optical camera communication architecture

Optical communication comprises a LED, Infra-Red, or Lazier projector and a high-speed camera embedded in a mobile phone. The projector projects a beam of light to the direction of the camera. The camera has an embedded CMOS image sensor capturing the projected beam. The beam on/off projection duration and frequency is according to an encoding pattern agreed with the receiving camera. The receiving camera records in a video the projection session and saves it in its internal storage. The recorded projection is decoded into bits, where for an "on" beam the corresponding decoding bit is set to "1", otherwise it is decoded as "0". The video in

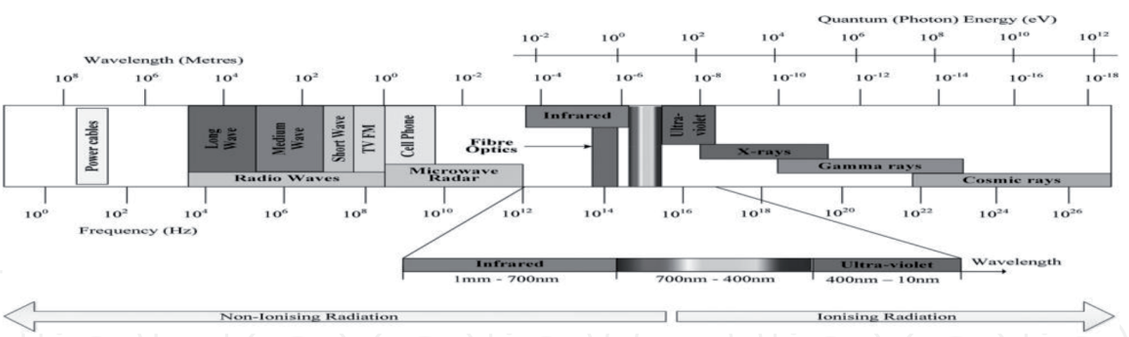


Figure 1.
Electromagnetic spectrum range.

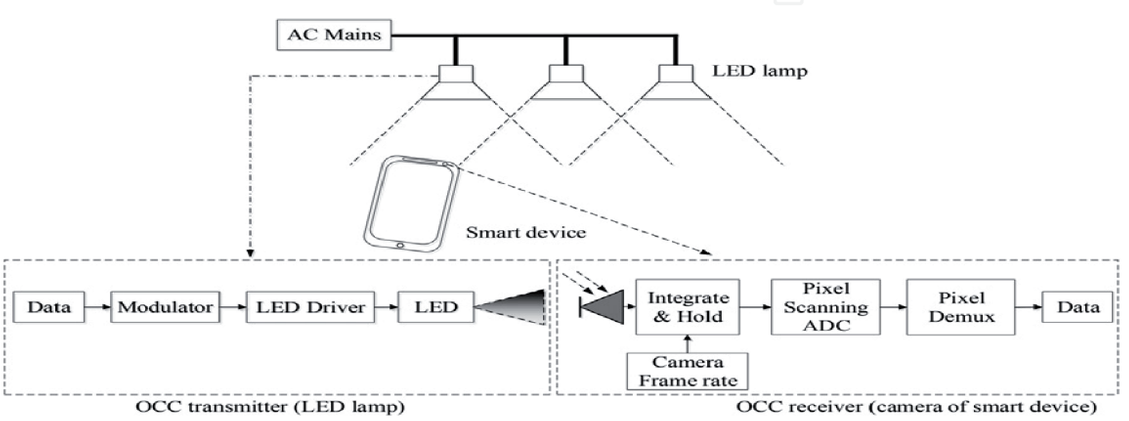


Figure 2.
A schematic view of the OCC system.

the camera can be further transmitted to the target receiver through a public network connection. The beam may be visible (normal lighting) or invisible (Infra-Red and Lazier). The illumination duration and frequency are so fast that a human eye is not able to follow and quote it. When the CMOS image sensor is operated, images are captured. These images are the source for extracting data by decoding it. **Figure 3** depicts the three phases of the received signal processing. The left image is the originally recorded beam impact, the image to the right is the original image after it was crystallized, and the third image to the right describes the final stage of the process. The third image is the input for decoding the beam stream into a bit string.

Figure 4 depicts the encoding process, starting from processing the image and translating it into a sequence of a signal chart (the top chart). The bottom chart depicts the final bit sequence.

7.5 System architecture

The objective of this work is to securely exchange keys utilizing optical communication, where the LED transmits, and the camera collects it. The idea is to modulate the information in a way that cannot be decoded only by processing the received

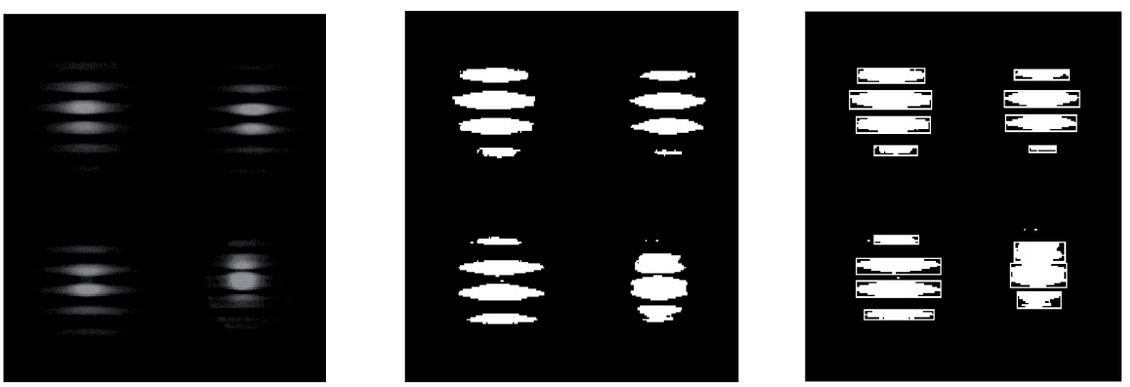


Figure 3.
Three phases of fringe signal processing.

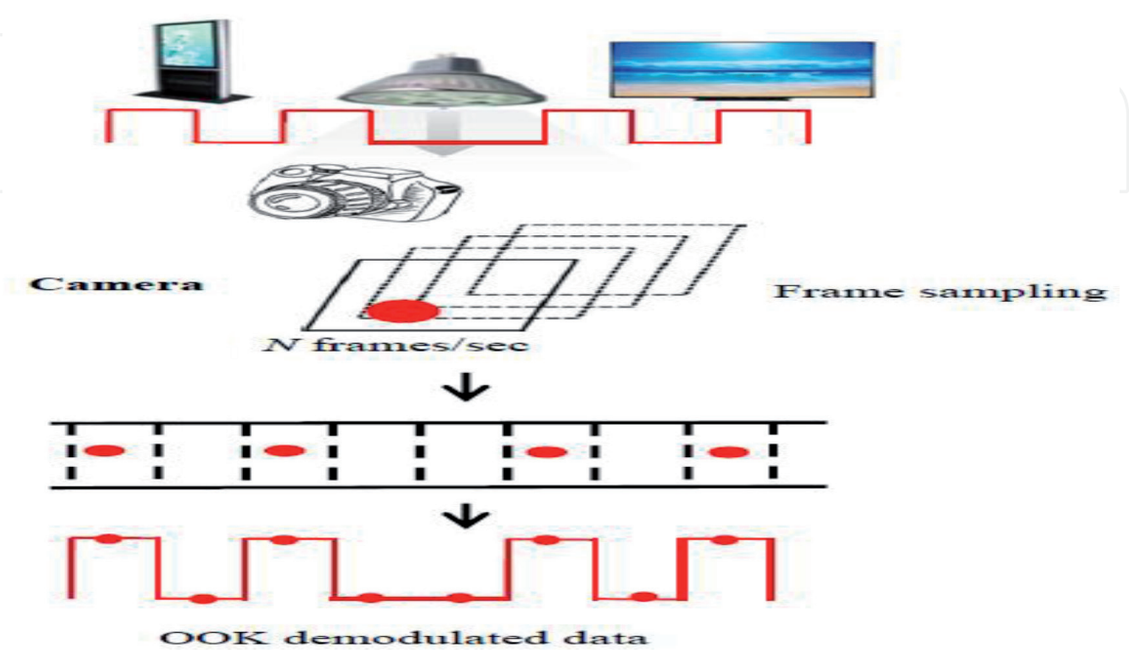


Figure 4.
Optical camera communication architecture.

signals. **Figure 5** illustrates the basic idea of the optical-based communication approach. The source computer generates an encrypted key. The key is translated to optical signals, which are projected by the LED projector to the targeted camera, embedded into a mobile device. The camera captures the optical signals and records it as a video movie. For authentication and accuracy, the video movie is signed by a standard electronic signature and the signed video is encrypted and transmitted via VPN to the target mobile device, which then projects the original signed-video to the target computer. The target computer decrypts the received video signals into a sequence of bits and thus the encrypted key reaches the target computer. We may consider moving the mobile device itself towards the target computer avoiding the key transmission.

Figure 6 outlines the 6 stage process. In stage 1, the key is generated and transformed into a LED code in stage 2, and then in stage 3, it is projected to the receiver camera. In stage 4, the received video is transferred to the target computer and in stage 5, the images are decoded into the encryption key. In step 6, the original key is discovered and forwarded for further use.

Figure 7 depicts the messaging protocol between the mobile and the computer.

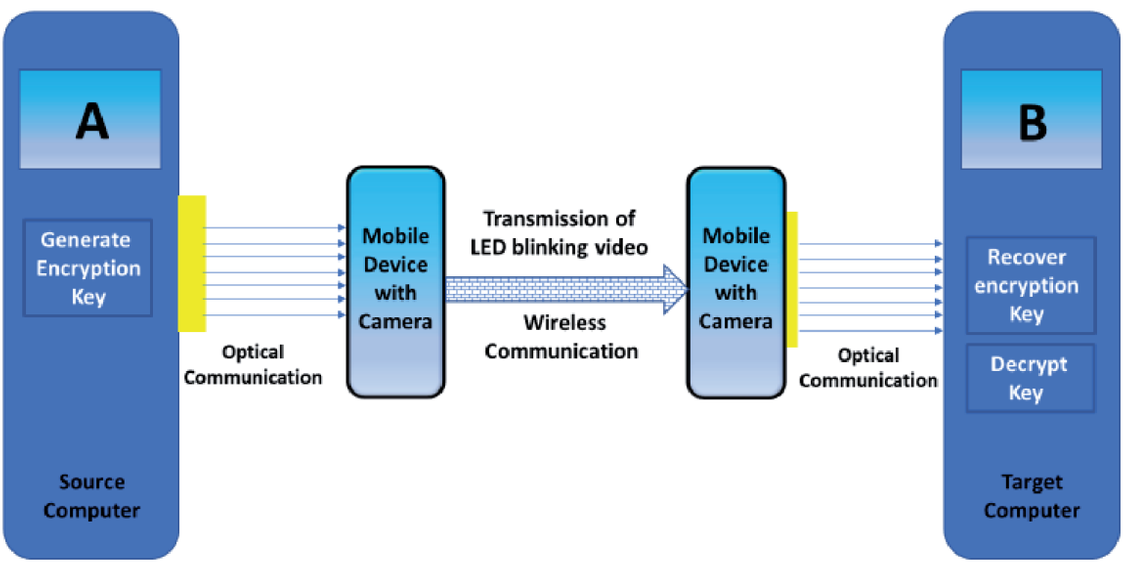


Figure 5.
High level secured key transmission system.

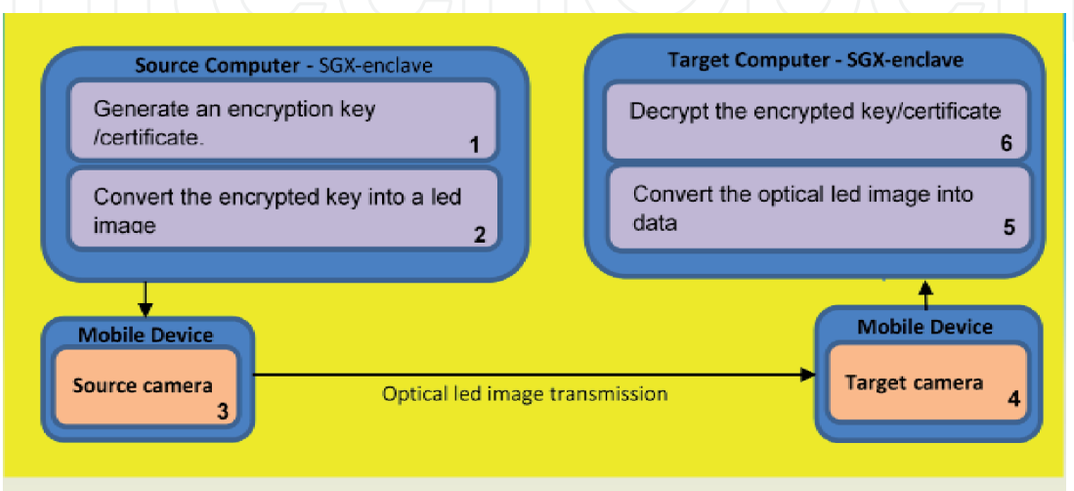


Figure 6.
Optical-based key transmission stages.

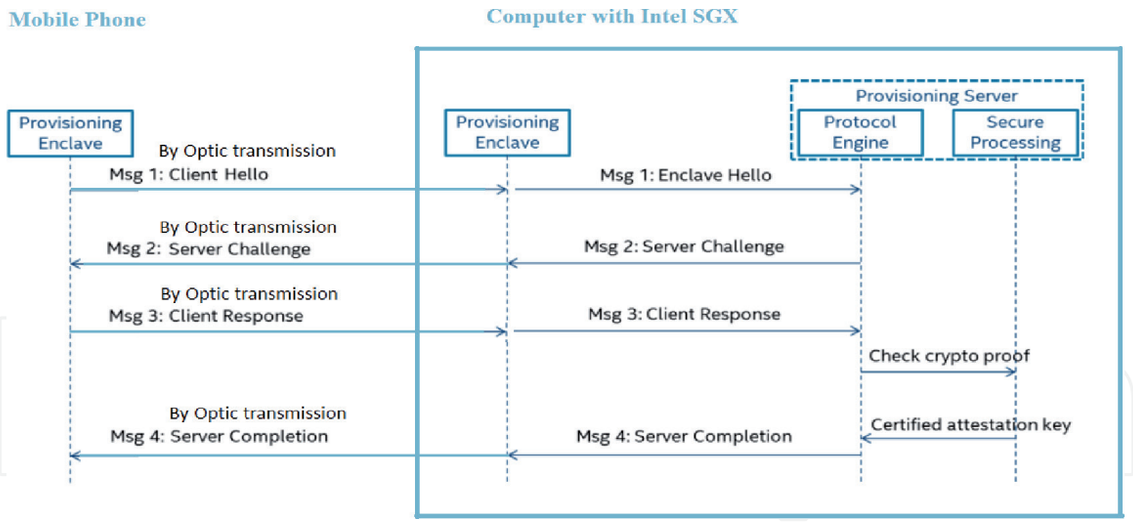


Figure 7.
Provisioning message flow protocol.

This way of transmitting optical signals instead of a bit-string, adds to the key exchange security level comparing to other solutions. However, the transmitted content is much more than a bit string. The practical impact is reasonable based on a moderate frequency of key changes and the availability of high capacity and high-speed communication.

7.6 Experiment and results

For the experiment we used a USB connected blinking LED device controlled by an Arduino code and an embedded Linkit ONE hardware. The encoding/decoding is simple, "1" bit is set when the LED blinks, and "0" otherwise. The key is transmitted to the USB device, the *Serial.exe* program receives it and converts it into an ASCII code. Before starting the key transmission, a unique bit string is sent. A developed application accepts the sequence of the blinking LED, processes it to produce a bit sequence, and converted into an ASCII code. A lit LED is processed by the OpenCV image processing such that each non-white pixel turns to 0 while white remains 255. Then, all pixels are summed up. If the sum is 0, the LED remains "off", and the output is a "0" bit. Otherwise, the output is a "1" bit.

We ran the entire cycle. The key was generated in a secured environment, then transmitted a bit string to the USB blinking device. The mobile phone camera recorded the video of the blinking sequence. The mobile phone signed, encrypted, and transmitted the blinking LED video, the receiver mobile device in the target location, accepted the blinking video, and transformed it into a bit string. We experimented with the "a b c d" key transferred between a host with an optical USB device and a smartphone with a camera. **Figure 8** depicts the output of the "abcd" transmission where lines 3, 6, 9, 12, and 15 represent the output "abcd" respectively.

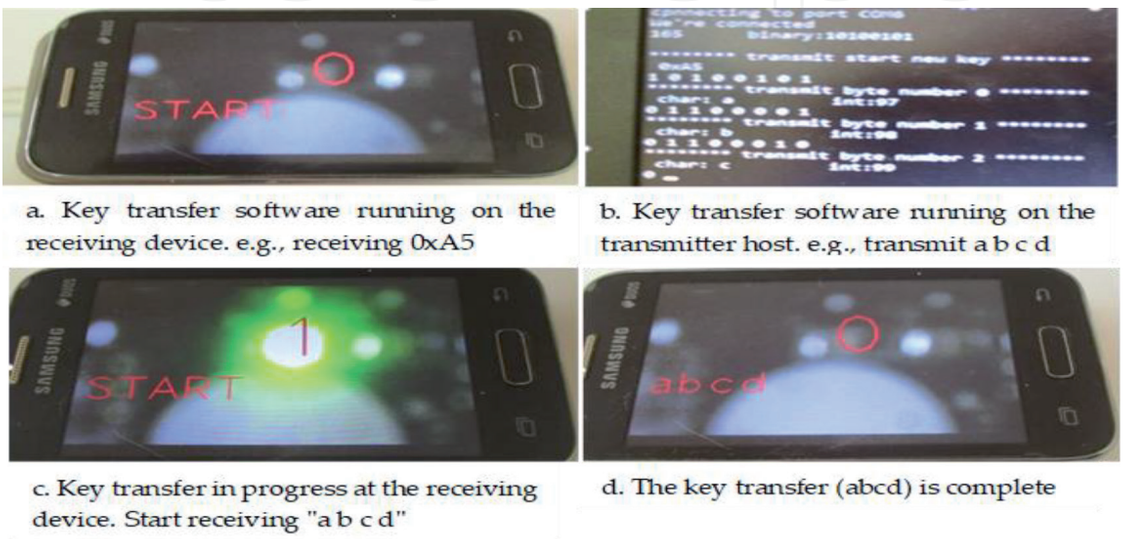
Figure 9 depicts the key transmission example "abcd" used in the experiment. The four images have been taken during the live key transmission stages.

In image a, the starting special bit string has been accepted by the mobile device connected to the sending computer. Image b shows the sender computer screenshot during the key transmission to its associated mobile device. Image c is the mobile-screen accepting the "abcd" key, and image d depict the acceptance of the transmitted key.

In this section, we introduced a complete cycle of secured key exchange using a form of optical communication. We described the hardware components and

```
******** transmit start new key ********
 0xA5
1 0 1 0 0 1 0 1
******** transmit byte number 0 ********
 char: a          int:97
0 1 1 0 0 0 0 1
******** transmit byte number 1 ********
 char: b          int:98
0 1 1 0 0 0 1 0
******** transmit byte number 2 ********
 char: c          int:99
0 1 1 0 0 0 1 1
******** transmit byte number 3 ********
 char: d          int:100
0 1 1 0 0 1 0 0
```

Figure 8.
Example of the key transmission.



a. Key transfer software running on the receiving device. e.g., receiving 0xA5

b. Key transfer software running on the transmitter host. e.g., transmit a b c d

c. Key transfer in progress at the receiving device. Start receiving "a b c d"

d. The key transfer (abcd) is complete

Figure 9.
Captured images of the live key transmission stages.

software of the conducted experiment. This demonstrates the applicability of an Optical Communication (OC) assisted method for secured key distribution [18].

8. Summary and conclusions

In this chapter, we outlined advancements in the Optical Communications subject matter. We focused on OC main improvements, transmission channel, and method, bandwidth, speed, and security. We concluded the chapter with detailed unique use of OC for key transmission required for symmetric cryptography. OC technology is still at its development and growth stage. We expect it to continue its fast growth and be implemented in many more domains, transforming our lives to be much more convenient, safe, and automated.

Comment: Due to the comprehensiveness and wide-ranging scope, this chapter outlines just part of the advancements in OC leaving issues such as underwater OC [19] and Machine learning for OC [1] out of scope.

Author details

Menachem Domb
Computer Science Department, Ashkelon Academic College, Ashkelon, Israel

*Address all correspondence to: dombmnc@edu.aac.ac.il

IntechOpen

References

[1] F. Musumeci et al., "An Overview on Application of Machine Learning Techniques in Optical Networks," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1383-1408, Second quarter 2019, DOI: 10.1109/COMST.2018.2880039.

[2] Mehtab Singh, Jyoteesh Malhotra, M.S.Mani Rajan Vigneswaran Dhasarathan Moustafa H.Alyc Performance evaluation of 6.4 Tbps dual-polarization quadrature phase-shift keying Nyquist-WDM super-channel FSO transmission link: Impact of different weather conditions, Elsevier, Alexandria Engineering Journal, Volume 59, Issue 2, April 2020, Pages 977-98

[3] A.Mansour, R.Mesleh, M.Abaza, New challenges in wireless and free-space optical communications, Elsevier, Optics and Lasers in Engineering, Volume 89, February 2017, Pages 95-108

[4] M. S. Bashir and M. R. Bell, "The Impact of Optical Beam Position Estimation on the Probability of Error in Free-Space Optical Communications," in IEEE Transactions on Aerospace and Electronic Systems, vol. 55, no. 3, pp. 1319-1333, June 2019, DOI: 10.1109/TAES.2018.2869506

[5] Alien wavelength technique to enhance Garr optical network, Paolo Bolletta, Massimo Carboni, Andrea Di Peo, Americo Gervasi, Lorenzo Puccio, Gloria Vuagnin, Cornell University, arXiv:1805.05811v1 [cs.NI], 2018

[6] Alan E.Willner1, Yongxiong Ren1, Guodong Xie1, Yan Yan1, Long Li1, Zhe Zhao, JianWang, Moshe Tur, Andreas F. Molisch and Solyman Ashrafi, High-capacity free-space optical and radio-frequency communications using orbital angular momentum multiplexing, doi.org/10.1007/978-3-030-26118-4_26, ISBN978-3-030-26117-7, ISBN978-3-030-26118-4, Springer, Cham, 2019

[7] S. Donati and V. Annovazzi-Lodi, "From order to chaos and back: Recent advances in optical cryptography of transmitted data," 2013 International Conference on Advanced Optoelectronics and Lasers (CAOL 2013), Sudak, 2013, pp. 1-6, DOI: 10.1109/CAOL.2013.6657507.

[8] F. Futami, K. Tanizawa, and K. Kato, "Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications," J. Lightwave Technol. 38, 2774-2781 (2020)

[9] Chowdhury, M.Z.; Shahjalal, M.; Hasan, M.K.; Jang, Y.M. The Role of Optical Wireless Communication Technologies in 5G/6G and IoT Solutions: Prospects, Directions, and Challenges. MDPI and ACS, Appl. Sci. 2019, 9, 4367

[10] Celik, A., Shihada, B., & Alouini, M.-S. (2019). Optical wireless data center networks: potentials, limitations, and prospects. Broadband Access Communication Technologies XIII. DOI:10.1117/12.2507643

[11] D. Kraus, E. Leitgeb, T. Plank and M. Löschnigg, "Replacement of the Controller Area Network (CAN) protocol for future automotive bus system solutions by substitution via optical networks," 2016 18th International Conference on Transparent Optical Networks (ICTON), Trento, 2016, pp. 1-8, DOI: 10.1109/ICTON.2016.7550335.

[12] Petkovic M., Narandzic M. (2019) Overview of UAV Based Free-Space Optical Communication Systems. In: Ronzhin A., Rigoll G., Meshcheryakov R. (eds) Interactive

Collaborative Robotics. ICR 2019. Lecture Notes in Computer Science, vol 11659. Springer, Cham. https://doi.org/10.1007/978-3-030-26118-4_26

[13] Denis P. Naughton, Robert Bedington, Simon Barraclough, Tanvirul Islam, Doug Griffin, Brenton Smith, Joe Kurtz, Andrey S. Alenin, Israel J. Vaughn, Arvind Ramana, Igor Dimitrijevic, Zong Sheng Tang, Christian Kurtsiefer, Alexander Ling, Russell Boyce, Design considerations for an optical link supporting inter-satellite quantum key distribution, Optical Engineering, 58(1), 016106 (2019). https://doi.org/10.1117/1.OE.58.1.016106, 9 January 2019

[14] S. Arai, S. Mase, T. Yamizato, T. Yendo, T. Fujii, M. Tanimoto, and Y. Kimura, Feasible Study of Road-to Vehicle Communication System using LED Array and High-Speed Camera, 15th World Congress on Intelligent Transport Systems and ITS America's 2008 Annual Meeting, Nov. 2008, pp. 1-12.

[15] P. Luo, Z. Ghassemlooy, H. L. Minh, X. Tang, H-M. Tsai, Undersampled Phase Shift ON-OFF Keying for Camera Communication, WCSP 2014, Oct 2014, pp. 1-6. IEEE

[16] R. D. Roberts, Space-time forward error correction for dimmable undersampled frequency shift ON-OFF keying camera communications (CamCom), Fifth International Conference on Ubiquitous and Future Networks (ICUFN), pp: 459-464, July 2013.

[17] N. Liu, J. Cheng, J. F. Holzman, Undersampled differential phase shift on-off keying for optical camera communications with phase error detection, 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE Xplore, July 2017

[18] Domb, M.; Leshem, G. Secured Key Distribution by Concatenating Optical Communications and Inter-Device Hand-Held Video Transmission. MDPI and ACS Style Appl. Syst. Innov. 2020, 3, 11.

[19] Schirripa Spagnolo, G.; Cozzella, L.; Leccese, F. Underwater Optical Wireless Communications: Overview. Sensors 2020, 20, 2261