IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Enhancement in Free Space Optical Communication:A Review

V. M. Gursale[1], S. S. Patil[2], A. B. Kakade[3]

Research Scholar, Rajarambapu Institute of Technology, Sakharale, Islampur, Sangli (M. S.), India[1]

Assistant Professor, Rajarambapu Institute of Technology, Sakharale, Islampur, Sangli (M. S.), India[2]

Associate Professor, Rajarambapu Institute of Technology, Sakharale, Islampur, Sangli (M. S.), India[3]

Abstract: In recent year, technology development has taken place in communication standards such as fourth generation (4G) or fifth generation (5G) and we are experiencing a rapid growth in information and communication technologies. Moreover, the demand of higher data rates has been increasing with development in technology. Free Space Optic (FSO) connections are becoming an enchanting alternative for copper, RF and fiber optic communication techniques, in terms of speed, costing, distance and mobility. Higher data rate demands higher data security as well as reliability. Optical communication security is important not only at the management layer but also at the physical layer. The following article focuses on enhancements in FSO communication techniques to improve the reliability of the FSO link and data security. Line of Sight (LOS) is maintained using Fine Tracking System which uses 4-quadrant detector (4QD), the user data security can be achieved by implementing quantum cryptography, and a secure physical network can obtained by using Acousto-optic Deflectors (AOD).

Index Terms: Acousto-optic deflector; Free space optic; Physical layer security; Data link layer security; User data security; quantum cryptography; Fine tracking system.

I. INTRODUCTION

At present, the three primary transport media used for communication purposes are copper line used for about 90% of communication, microwave radio link used for about 6% communication purposes and optical fiber for almost 4% of the communication [8]. Copper lines are becoming incapable option for future communication demands due to low data rate and linear increase in price in accordance with the capacity. Alternatively, optical fiber can support large data rates but need high initial investments and the maintenance cost. The conventional radio frequency (RF) technology has been widely used and studied for the communication purposes. RF links provide wireless connectivity between two nodes hence supports mobility. These links however have limited data rates and are also vulnerable to interference and security problems. As the frequency for the signal increases, it is increasingly curbed by distance and weather conditions. Moreover the spectrum license part adds to the cost.

Free Space Optical (FSO) Communication, also known as Optical Wireless Communication (OWC), is a promising technology aimed to fulfill the next generation demands such as high data rates, low interference, ease of implementation and maintenance, etc. FSO offers higher data rates, ultra-low channel interference, simplified implementation and lower power consumption. An FSO link utilizes the free space between pair of laser-photo detector transceivers to transfer data. The FSO operates at beam wavelength ranging from 350 nm to 1550 nm hence making system immune to interference, license free and can support higher capacity. Hence FSO system can be implemented to establish optical link of several gigabits per second over a distance of few kilometers [2]. As FSO and Optical fiber communication operate with similar wavelengths, FSO and optical fibers can be easily integrated in the network, thereby making this communication system more robust. These advantages of FSO bring upon an alternative for traditional RF based wireless communication; however this system has intrinsic difficulties such as Line of Sight (LOS) misalignment. FSO link can be setup only when the two nodes are in the line of sight and also up to the weather conditions, such as fog and precipitation, affecting beam scattering of the transportation beam.

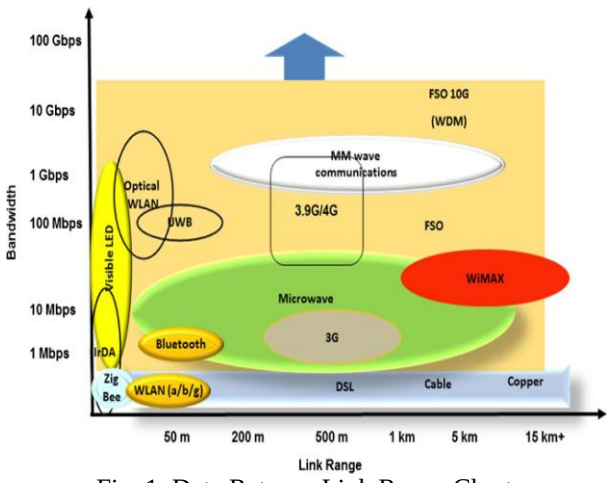

Fig. 1. Data Rate vs. Link Range Chart

DOI 10.17148/IJARCCE.2016.51213

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

FSO can use ultra-violet (UV), infra-red (IR) or visible light communication (VLC) for both indoor and outdoor environment, including underwater communication environment [19,20]. LOS is the best alternative to achieve higher data rates at lower bit error rate with reliable transmission. However, LOS link is deficient to mobility and liable to blocking due to obstacles, particularly in indoor environment. Indoor VLC, uses 380 nm to 780 nm range of optical wavelength and can be used as an alternative to indoor IR (780 nm to 950 nm) technology.

Extensive use of Wavelength Division Multiplexing (WDM) has made optical networks capable to transfer huge traffic in terms of Tb/s [11]. Terrestrial FSO communication is a LOS technology that operates at 850 nm, 1300 nm, and 1550 nm wavelengths. The short range FSO link (500 m) mainly used for urban area is an alternative for conventional RF links to provide high speed broadband access to home and offices. Full duplex FSO system can provide 1.25 Gb/s data rate between two static nodes over a range of 3.5 km. Number of very high data rates have been reported using FSO system by applying 80 Gb/s wavelength division multiplexing, 320 (8x40) Gb/s over 212 m, 1.6 (16x100) Tb/s, and so on.

Features of FSO communication
- No spectrum license required
- Virtually unlimited bandwidth
- Extensive link range (up to 5km)
- Green technology
- Low power consumption
- Reduced interference
- High Scalability and Re-configurability
- Higher security and authentication
- Cost efficient (price per bit)

II. MINIMIZING ATMOSPHERIC EFFECTS

The FSO communication requires an accurate line of sight between the two nodes between which communication is to be done. Atmospheric turbulences, storms, fog, etc affect the line of sight on a large extent. Atmospheric turbulence misaligns the LOS as the nodes for FSO communication are placed at high altitude platforms hence fast blowing wind may disturb the alignment of the nodes. Fog, on the other hand, consists of water molecules causing the beam to disperse in the fog, due to which the diffraction angle of the beam substantially changes as compared to clear LOS and fog [17,18].

To overcome this limitation of FSO communication system, a self-tracking control system can developed to maintain alignment between the pair of transceiver [4]. An accurate alignment can be maintained using acquisition, pointing and tracking system. The system consists of two structures, a Course Pointing Assembly (CPA) and a Fine Pointing Assembly (FPA) [4]. CPA consists of course tracking sensor using a Charged Coupled Device (CCD), 2-axis gimbals mechanism and controller.

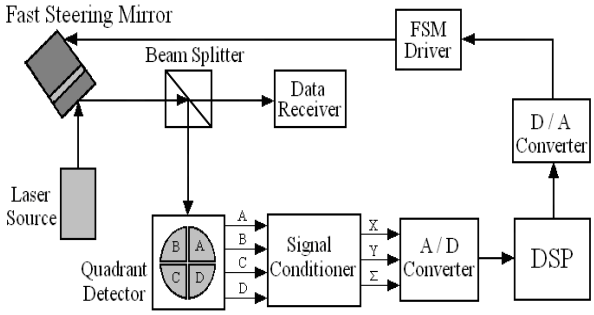

Fig. 2. Experimental Setup of Fine Pointing Assembly

The experimental setup of Fine Pointing Assembly (FPA) subsystem consists of fine tracking sensor using a 4-Quadrant Detector (4QD), a Fast Steering Mirror (FSM), a controller for FSM, Signal conditioner and Processor. The beam splitter is used to split the incoming beam in two directions; one beam is focused on photo detector of the receiver system whereas the second beam is focused on 4QD. The 4QD measures the position error of the beam and generates an error signal which is given to signal conditioner. The signal conditioner then gives the analog signal to analog to digital converter (ADC) in DSP and the DSP then generates a digital signal to drive the FSM. The digital signal is converted into analog signal and then given to driver of FSM.

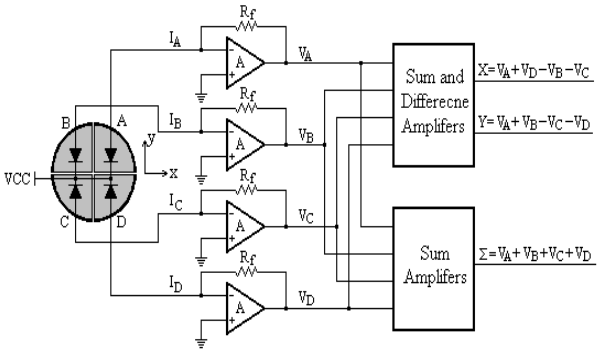

Fig. 3. Operating Principle of 4QD

The 4QD and signal conditioner working principle can be explained with reference with the Fig. 3. The photodiodes A, B, C and D, representing 4 quadrants, are separated by small equal gaps. The photo diodes A, B, C and D convert the incoming light into currents I_A, I_B, I_C, and I_D and further these currents are converted into voltages V_A, V_B, V_C and V_D using Op-amp circuit. Ideally the currents or voltages of photo diodes must be equal in reference with laser beam or spot, distributed uniformly on all the photo diodes as shown in Fig. 4. (a). If there is misalignment in the nodes then the beam spot will be distributed non-uniformly over the photodiodes as shown in Fig. 4. (b).

The spot displacement along x-axis and y-axis is shown in Fig. 4. (b). and is determined by the relative change between the four current outputs and then can be removed by fine tracking control loop. The currents and voltages are used to determine E_x and E_y, called as pointing error, as follows [4];

DOI 10.17148/IJARCCE.2016.51213

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

$$E_x = K_x \frac{(I_A+I_D)-(I_B+I_C)}{I_A+I_B+I_C+I_D} = K_x \frac{(V_A+V_D)-(V_B+V_C)}{V_A+V_B+V_C+V_D} \quad (1)$$

$$E_y = K_y \frac{(I_A+I_B)-(I_C+I_D)}{I_A+I_B+I_C+I_D} = K_y \frac{(V_A+V_B)-(V_C+V_D)}{V_A+V_B+V_C+V_D} \quad (2)$$

Where, K_X and K_Y are correlation coefficient of x-axis and y-axis direction respectively.

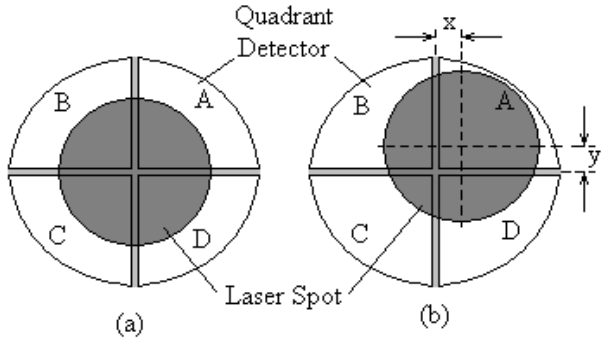

Fig. 4. Relative Positions of Beam Spots
(a) Spot is centered on the 4QD
(b)Spot is not centered on the 4QD

The E_X and E_Y error signals, by (1) & (2), are feed to the DSP processor which processes the data and then sends control signal to the FSM driver so that the beam spot may be aligned to the center of the 4QD and hence on the photo detector of the receiver hence making a reliable data reception at receiver.

III. USER DATA SECURITY

The second most important characteristic of FSO communication is the data security. As the communication between two nodes is done by transmitting a light beam in free space hence it can be easily deflected or accessed by the attacker. Moreover the traditional encryption techniques can be broken using computers with such capabilities and hence and gain access to the data that is being transmitted. Thus the data security in the network was weak in terms of encryption, as the encryption algorithms can easily be broken by sequential computers.

Hence there was a need of more sophisticated encryption algorithm to be developed. Several methods for network security are studied in [11]. Quantum Cryptography is one of the most sophisticated techniques used for encryption of optical data. Quantum cryptography follows the quantum mechanism principle, such as Heisenberg's uncertainty principle, in relevance to that, in an optical cryptographic system an attacker or eavesdropper would disturb the quantum state of photon thus varying the polarization, phase and wavelength proportion. Anurbane scheme to transmit a secret code using sequence of randomly polarized photons from which an encryption key is generated, is called quantum cryptography. Thus if the quantum state of photon is disturbed then the key generated will decrypt the data to a non-useful data hence providing a secure system. The key generation and distribution method is known as quantum key distribution (QKD).

In quantum cryptography, the ciphered text, known as "quantum cipher text", is generated by the quantum key. However, photons are subjected to nonlinear dielectric environment, attenuation, and scattering and reflections discontinuities. Conversely, multiple photons deliver lower security against eavesdropping as few photons can be mined from the stream. Thus there is a tradeoff between protection of data and quality of reception.

Till date numerous quantum cryptographic algorithms have been proposed such as the Greenberger-Horne-Zelinger [12], Bostroem and Felbinger [13], and Cai [14] which are examined and found to have liabilities to eavesdropping [15]. However, these liabilities may be used as means to authenticate or nullify network security method and hence should be carefully examined. Several vulnerabilities of quantum cryptography method as discussed in [16] are:

- There are no single optical sources with controllable single photon rate generation and controllable photon polarization.
- As photons propagate through media, polarization state of photon tends to change.
- A very long random bit sequence is required to guarantee a decent encryption.
- Imperfectly coupled single photon source or fiber will suffer attenuation which may cause photon loss and thus increase quBit Error Rate (qBER).

IV. ACOUSTO-OPTIC DEFLECTOR

The user data security deals with the encryption of signal at the data link layer of the OSI reference model whereas physical network security deals with the physical layer i.e. the lower most layer of the OSI reference model. A proposed novel security mechanism and hardware design for beam transmission in physical layer of a FSO communication is discussed in [7]. The transmitter in FSO sends consecutive packets through diverse beam paths between transmitter and receiver using acousto-optic deflector (AOD) [7]. As the beam radius and intensity is raised the probability of eavesdropping increases. Hence AODs are deployed at transmitter to change the beam profile.

An acousto-optic device is a column of optically transparent medium tapered at one end by a piezoelectric transducer producing an internal strain in the column. As the wave propagates through the medium of column it causes cyclic deviation in the refractive index, this is achieved as the acoustic wave produces regions of compression in the crystal lattice followed by the relaxed lattice. The variations are periodic, causing medium to act as diffraction grating, resulting diffraction of portion of an incident beam [9].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

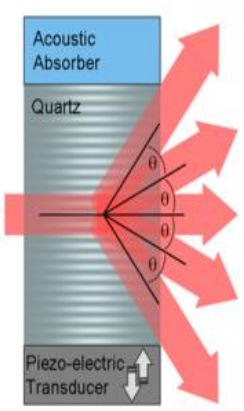

Fig. 5. AOD with Incidence Angle Normal to Surface

The Bragg angle or diffraction angle of the AOD column depends on the frequency of piezoelectric transducer, optical wavelength of incident beam, velocity of acoustic wave, and refractive index of the column in normal state. The angle of diffraction or Bragg angle is represented by θ_B [10];

$$\theta_B = \frac{\lambda f_s}{2N_a V_s}$$

The Bragg angle changes as the angle of incidence changes and is given by;

$$\theta_B = \theta_B + \theta_i$$

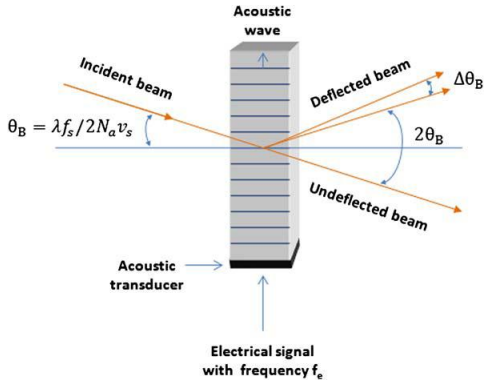

Fig. 6. AOD with angle of incidence θ_i

The angle of incidence of the incident beam is equal to the Bragg angle as shown in fig. 6. Hence the Bragg angle or the diffraction angle at the output is given by $2\theta_B$. Where, λ is optical wavelength in air, N_a is the refractive index, f_s and v_s are the frequency and velocity of acoustic wave travelling through AOD.

V. PHYSICAL NETWORK SECURITY

Consider a long distance terrestrial FSO link is established using single-mode semiconductor laser as transmitter and photo detector as a receiver. The distance between the transmitter and receiver is considered as D hence the beam travels distance D from transmitter to receiver in free space.

A narrow beam is transmitted from the transmitter and passed through free space and received by the receiver, the beam while travelling in free space experiences divergence, denoted by θ, due to optical diffractions in free space as shown in Fig. 7.

The transmitted beam in Fig. 7 is shown by the blue cone which is the data that actually reaching at the receiver whereas the brown cone shown around the blue cone is the wastage of signal and is unavoidable as it is caused due to atmospheric diffraction. The laser is encrypted and also follows the flow control protocol as discussed in section III hence if the attacker intrudes or disturbs the signal in blue then the transmission will stop and the data will not be decrypted by the attacker.

However, attacker can settle a sensing device in the divergence region of transmitted beam i.e. in the brown cone. The gray cone in Fig. 7 shows the attacker sensing the signal from the diffracted beam without disturbing the signal. Hence, this increases the opportunity of eavesdropping in case of long transmission links. Thus to overcome this disadvantage a proposed novel physical layer design is developed to improve the security of the system [7].

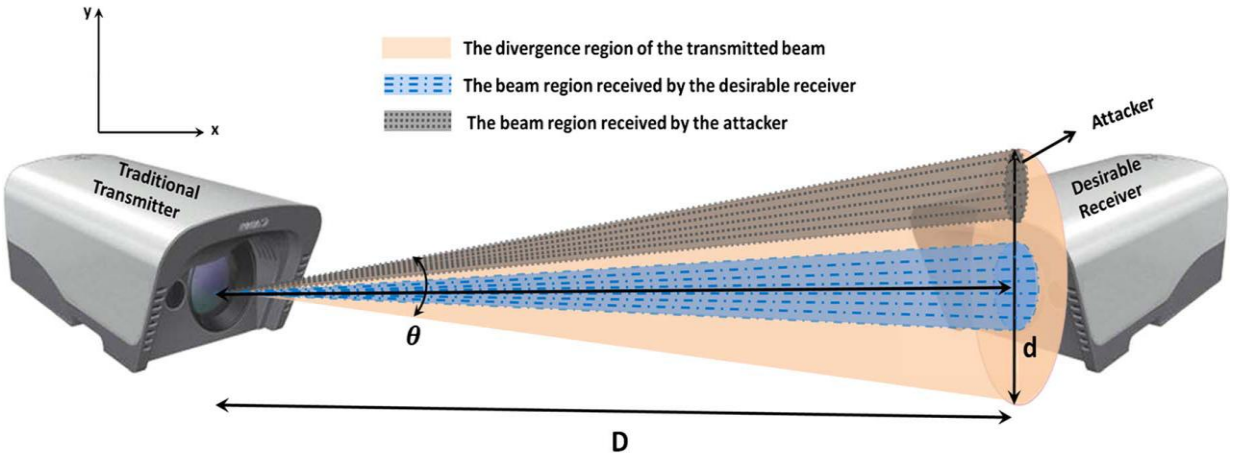

Fig. 7. Conventional FSO Link

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

In the proposed novel [7] design of physical layer, the beam transmission is done through different paths, i.e. the packets of data is transmitted from transmitter to receiver via successive different paths between transmitter aperture (TA) and receiver aperture (RA) using acousto-optic deflector (AOD). In contrast to traditional transmission, the optical transmitter transmits N consecutive packets through N dissimilar paths between TAs and RAs as shown in fig. 8(a), where the divergence θ causes the two light paths to overlap each other hence complete data can only be recovered at the overlapping part.

Fig. 8 (b) shows the beam paths through which the data is transmitted in the link. The relevant data can be obtained only in area A_1 i.e. only at the central aperture (CA) whereas the receiver aperture (RA) receive phase shifted data with allowable phase shift, used only for the detection of eavesdropping. The outer part of the overlapped signal is out of phase and hence cannot be decoded as it requires the quantum key generated using phase, polarization and wavelength of the beam.

Thus even the attacker receives the overlapped data the difference between the phases will not allow to decode the data, however, to access the decodable data the attacker has to move the sensing device to area A_1 which will first detected by RAs and then the transmission will be stopped and hence protecting the transmission from eavesdropping. The FSO transceiver based on AOD has a more complicated structure than as shown in the simplified structure in Fig. 9. In Fig. 9 two beam paths are used to transmit the packets through the link. It consists of three AODs of which AOD 1 is the most significant AOD as it is responsible to form two beam paths from a single laser source. Combination of convex- concave lenses is used to guide the beams to the TAs where another AOD is used to provide the transmission path in free space. The received beam is then passed through partial mirror which reflected the received beam completely but doesn't affect the transmission beam. Then the received beam is passed through beam splitter which splits the beam in two, one given to PD of the receiver to obtain the data and second given to 4QD which is used for fine tracking of the system as explained in section II. The controller, computer and drive circuit also controls the AODs at the TAs which gives the accurate beam path. Thus fine tracking is obtained using the assembly.

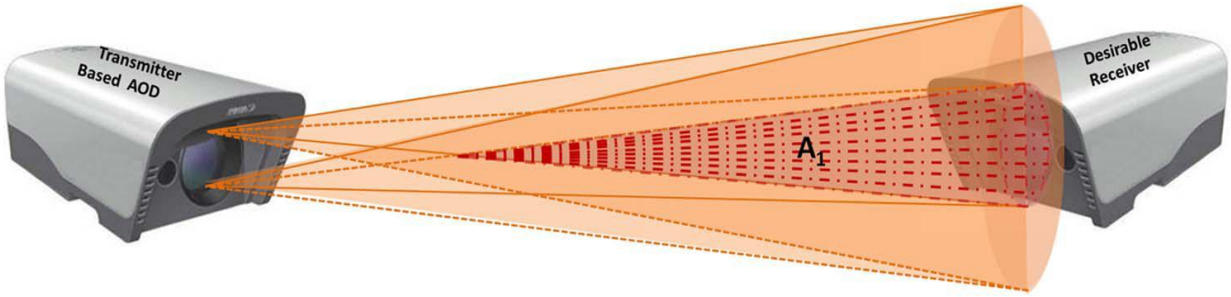

Fig. 8 (a) General Schematic of a FSO link based on AOD

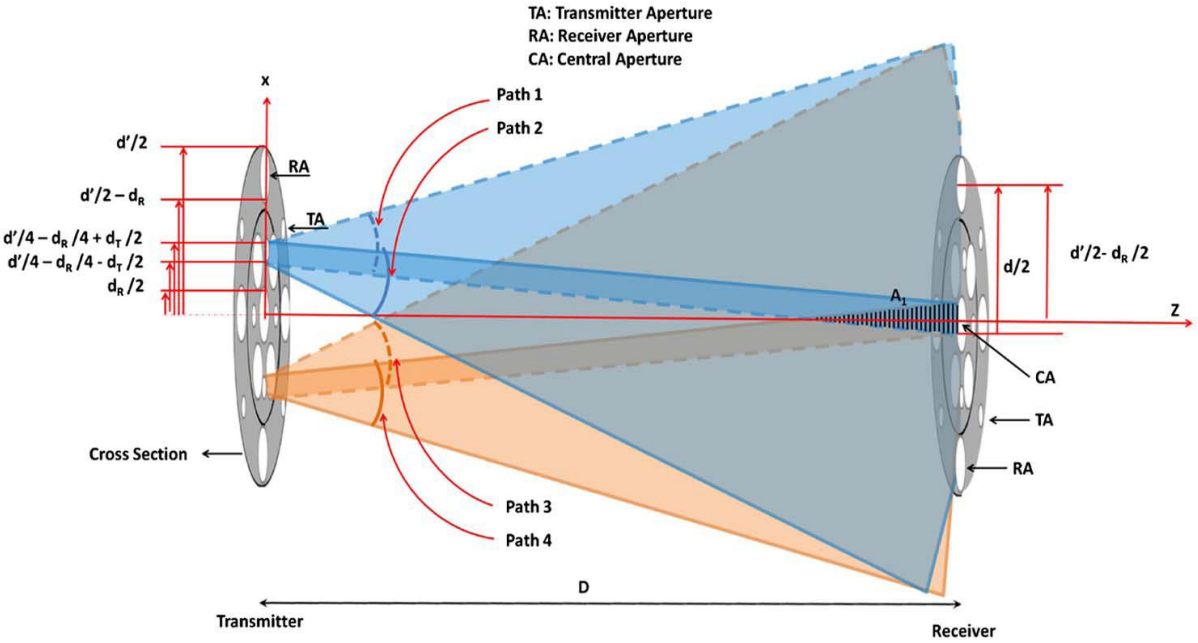

Fig. 8 (b) Four Beam Path between two TAs and RAs with overlapping area A_1

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

The number of different transmission paths in every time slot can be increased by increasing the number of AODs at the TAs of the transmitter. To construct different beam paths between the transmitter and receiver, AOD2 and AOD3 are used. In every time slot, one of the AODs or one of the TAs is chosen to send the beam. AOD1 is positioned at focal length of convex lens 1 to convert the arrived beam into collimated beams with optical axis I as shown in Fig. 9. When the parallel beam travels straight through the partial mirror BS1 and passes through the concave lens, it diverges from the axis I. As the focal points of concave lens and convex lens 2 are same, when the diverged beam passes through convex lens 2 it causes the beam to propagate again in parallel with the optical axis I and is incident on AOD2 or AOD3 depending on beam path selected [7].

When a beam is received through the RA of the structure the beam is reflected and the split to control the alignment and to decode the data as explained earlier. As a result, fine tracking is achieved and data security is also increased by transmitting through different beam paths.

VI. CONCLUSION

The enhancement in FSO communication technique is achieved by categorizing the enhancement requirements and finding the individual solution for each enhancement. The requirement and maintenance of LOS can be achieved by using fine tracking system which used 4-quadrant detector to detect the beam alignment and FSM to adjust the beam at center of 4QD. The controller generates signals so that the two nodes of FSO link are maintained in the accurate alignment. Secondly the user data security is enhanced by using quantum cryptography, in which the key is generated using the polarization, phase and wavelength of the photon call as quantum key distribution (QKD) technique, as the conventional encryption techniques can be easily broken if attacker has access to high speed sequential computers.

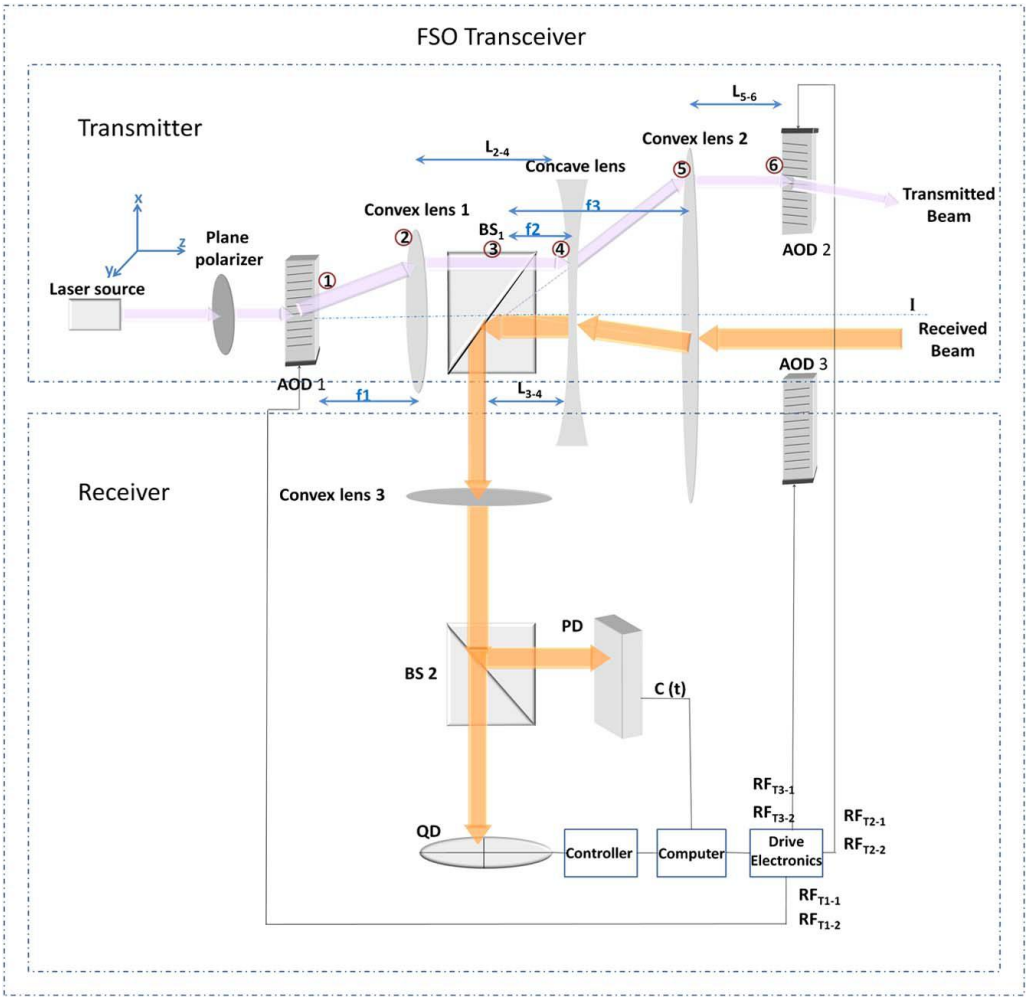

Fig. 9. FSO Transceiver using AOD

Lastly the enhancement in physical layer security is done using AODs by which the transmission is achieved by sending the data through different beam paths at different time slots. The different beam paths are directed towards the receiver such that the overlap just before it reaches the CA of the receiver. Even if the attacker has access to the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

overlapped beam other than CA, the quantum encryption cannot be detected as the phase change will occur at any point other than CA. Thus enhanced secure and reliable FSO is achieved by integrating the three categorical solutions as mentioned in section V.

REFERENCES

[1] Z. Ghassemlooy, S. Arnon, M. Uysal, Z. Xu, and J. Cheng, "Emerging Optical Wireless Communications- Advances and Challenges," IEEE Journal on Selected areas in Communication, vol. 33, no. 9, pp 1738-1749, Sep. 2015.
[2] C. Haoshuo, H. P. A. Van den Boom, E. Tangdiongga, and T. Koonen, "30-Gb/s Bidirectional transparent optical transmission with an MMFaccess and an indoor optical wireless link," IEEE Photon. Technol. Lett.,vol. 24, no. 7, pp. 572–574, Apr. 2012.
[3] V. V. Nikulin, R. Khandekar, J. Sofka, and G. Tartakovsky, "Acousto-optic pointing and tracking systems for free-spacelaser communications," Proc. SPIE, vol. 5892, Aug. 2005.
[4] H. Zhen and S. Zhengxun, "Modeling of fine tracking sensor for fress space laser communication system," IEEE Photonics and Optoelectronics Conference, pp 1-4, 14-16 Aug. 2009.
[5] Y. Li, N. Pappas, V. Angelakis, M. Pioro, and D. Yuan, "Optimization of Free Space Optical Wireless Network for Cellular Backhauling," IEEE Journal on Selected areas in Communication, vol. 33, no. 9, pp 1841-1854, Sep. 2015.
[6] S. V. Kartalopoulos, "Security in advanced optical communication networks," in Proc. IEEE Int. Conf. on Communications (ICC), June 2009.
[7] M. Eghbal and J. Abouei, "Security Enhancement in Free-Space Optics Using Acousto-optic Deflectors," IEEE/OSA J. Opt. Commun.Netw., vol. 6, no. 12, pp. 684-694, Aug. 2014.
[8] O. Tipmongkolsilp, S. Zaghloul, and A. Jukan, "The evolution of cellular backhaul technologies: Current issues and future trends," IEEE Commun.SurveysTuts., vol. 13, no. 1, pp. 97–113, 1st Quart. 2011.
[9] A. M. Kiruluta and V. M. Ristic, "Acousto-optic devices: Application to the reconstruction of spatially sampled data in magnetic resonance imaging," Can. J. Elect. & Comp. Eng., Vol. 21, No. 4, pp 145-148, 1996.
[10] I. C. Chang, "Acousto-optic devices and applications," IEEETrans. Sonics Ultrason., vol. SU-23, no. 1, pp. 2–21, Jan. 1976.
[11] S. V. Kartalopoulos, "Quantum Cryptography for Secure Optical Networks," in Proc. IEEE Int. Conf. on Communications(ICC), pp 1311-1316, 24-28 June 2007.
[12] X. Li, "A quantum key distribution protocol without classical communication", quant-ph/020950, Sept. 6, 2002
[13] K. Bostroem and T. Felbinger, "Ping-pong coding", quant-ph/020940, September 5, 2002.
[14] Q-Y. Cai, "Deterministic Secure Direct Communication Using Ping-pong Protocol without Public Channel", quant-ph/0301048, January 13, 2003.
[15] D. R. Kuhn, "Vulnerabilities in Quantum Key Distribution Protocols", quant-ph/0305076, May 12, 2003.
[16] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm and T. Lörunser, "Practical quantum key distribution with polarization entangled photons", Optics Express, vol. 12, no. 16, 2004, pp. 3865-3871.
[17] W. Jian, "Propagation of a Gaussian-Schell beam through turbulent media," J. Mod. Opt., vol. 37, no. 4, pp. 671–684, 1990.
[18] J. Wu and A. D. Boardman, "Coherence length of a Gaussian-Schell beam and atmospheric turbulence," J. Mod. Opt.,vol. 38, no. 7, pp. 1355–1363, 1991.
[19] J. R. Barry, J. M. Kahn, E. A. Lee, and D. G. Messerschmitt, "Highspeed nondirective optical communication for wireless networks," IEEE Netw., vol. 5, no. 6, pp. 44–54, Nov. 1991.
[20] M. Uysal and H. Nouri, "Optical wireless communications—An emerging technology," in Proc. 16th ICTON, pp. 1–7, Jul. 6–10, 2014.