International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 November 2024* ***Revised:*** *12 December 2024* ***Accepted:*** *02 January 2025*

Secure Data Transmission to Improve the Performance of Communication in Hybrid Systems

Prajakta A. Satarkar
Research Scholar, SRTMU, Nanded, MH, India.
Assistant Professor, SVERI's College of Engineering Pandharpur, MH, India.
e-mail: pasatarkar@coe.sveri.ac.in

Dr. Girish V. Chowdhary
Professor and Director, School of Computational Science, SRTMU, Nanded, MH, India.
e-mail: girish.chowdhary@gmail.com

Abstract— Light Fidelity (Li-Fi) is a way of communication using LED's with a high data rate and secures data transmission. But it has some drawbacks like data loss during shadowing and flickering of light, interference, etc. To deal with data loss we can use Hybrid Li-Fi and Wi-Fi Networks (HLWNets) by combining Li-Fi and Wireless Fidelity (Wi-Fi). Emerging HLWNets design and implementation face secure data transmission issues introduced due to Wi-Fi networks. We propose a novel comprehensive solution called Efficient Handover Protocol with Secure Data Transmission (EHPSDT).To assure the total security of data, we proposed security architecture based on Attributed-based Elliptic Curve Encryption (AECC) that ensures confidentiality and integrity. It also allows for fine-grained access control in HLWNets. Compared to other current methodologies, the proposed method minimizes overall processing overhead. The result of simulation revealed the performance of the proposed EHPSDT compared to underlying methods in terms of packet delivery ratio (PDR), average throughput, and communication overhead.

Keywords- Attribute Based Encryption, Elliptic Curve Encryption, Hybrid networks, Li-Fi, Secure transmission.

I. INTRODUCTION

The strong demand for multimedia wireless devices has prompted experts to investigate the millimeter wave frequency spectrum for multiple gigabit wireless connections. Recent advances in antenna technology, the Radio Frequency (RF)-Complementary Metal Oxide Semiconductor (CMOS) technique [1], and highly mobile baseband signal processing algorithms have made millimeter wave wireless communication a reality. The wireless communication of millimeter wave supports high data rate of gigabit per second (GBPS) has led to several applications in many critical fields such as Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), and backhaul for cellular systems [2]. The frequency range includes 28 GHz, 38 GHz, 45 GHz, 60 GHz, and even 100 GHz. Li-Fi is considered as a green form of communication since it makes use of existing lighting infrastructure for communication [3], producing radiation-free, clean communication that might be helpful for our government's Digital India plan. It aids in the transmission of information through quick tiny variations in light intensity that are imperceptible to the human eye. Governments worldwide are increasingly backing a novel solution for internet provision that sidesteps radiation and licensing constraints. This approach, known as Li-Fi, offers an alternative to traditional RF electromagnetic spectrum usage, which is hampered by congestion and regulatory hurdles. With the explosive growth of multimedia mobile devices demanding ever more data, traditional radio spectral bands have become saturated, leading to traffic bottlenecks. Li-Fi, operating within the expansive 300 THz optical spectrum and free from regulatory constraints, presents itself as a promising remedy to this congestion, offering undisturbed wireless communication capabilities [4]. The advantage of Li-Fi is that it does not interfere with Wi-Fi because it utilizes a separate frequency [5]. It enables the design of heterogeneous network HLWNets. In an interior context, heterogeneous HLWNets increase system data throughput and QoS [6]. Because Li-Fi does not affect the Wi-Fi system, the total data rate in HLWNets is higher than in separate Li-Fi and Wi-Fi systems [7].

Security is a vital concern while deploying the HLWNets. Nowadays, a substantial amount of essential information is shared and kept within wireless networks, thus it is crucial to safeguard the network itself from those who aim to benefit from all of this information [8]. Li-Fi, which transmits data via visible light, is said to be more secure than Wi-Fi due to in-built channel security. However, because of Wi-Fi's broad use, several security weaknesses in the Wi-Fi system have been discovered. These security concerns, with Wi-Fi's inability to meet the ever-increasing demand for wireless communication [9]. The malicious UEs in Wi-Fi also affect the communications in Li-Fi. Wi-Fi is prone to security breaches including a variety of concerns such: Denial of Service, Rouge Access Points, Wireless Trespasser, End Point Attacks, Data

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
***Article Received:** 25 November 2024 **Revised:** 12 December 2024 **Accepted:** 02 January 2025*

Interruption, etc. Because of the nature of the radio waves utilized in Wi-Fi, Wi-Fi connections have become unreliable and sensitive to external attacks. To make wireless networks safer, numerous security measures were included in Wi-Fi systems based on security standards [10]. These measures are still vulnerable to attacks, especially if technology advances and more individuals learn how to exploit them. Therefore, providing the appropriate security measure with an efficient handover protocol is essential for HLWNets.

We proposed a novel solution called Efficient Handover Protocol with Secure Data Transmission (EHPSDT) as the compressive solution to the challenge concerning the security in HLWNets. The EHPSDT protocol aimed to provide the QoS-efficient handover protocol with highly secured data transmissions among the UEs connected to APs. Below are the distinctive contributions that underscore the novelty of the EHPSDT protocol.

- To secure the data communications in HLWNets, we propose the lightweight cryptography approach called AECC. The data transmissions in UE-UE, UE-AP, or UE-Li-Fi cells are performed in encrypted form with optimal key management.
- EHPSDT protocol proposed to optimize the handover and load balancing functionality with security against malicious UEs.
- We conduct thorough experimental assessments to gauge the effectiveness of the EHPSDT protocol under various HLWNets conditions, juxtaposed against current solutions.

The paper is organized as follows: Background study is presented in Section 2 with research gaps analysis. Designs and proposed methodology is explained in Section 3. Section 4 has the simulation results and related discussions. Section 5 presents the conclusion with suggestions for further extensions.

II. BACKGROUND STUDY

According to the problems in HLWNets, this section presents the current solutions in brief. We reviewed ECC-based cryptography recent solutions for secure wireless data transmissions.

ECC-based Cryptography Methods

Parrilla et al. [11] introduced a compact and integrated co-processor designed for ECC and Advanced Encryption Standard (AES) functionalities, boasting minimal space utilization and offering Group-Key support. Kumar et al. [12] discussed how to deal with privacy and security concerns in 5G networks that have different types of technology mixed together. They introduced a logical architecture that combines 5G and WLAN (Wireless Local Area Network). They suggested using a method called handover authentication, which involves using ECC (Elliptic Curve Cryptography), to make sure that when devices switch between different parts of the network, they can do so securely, ensuring safe and uninterrupted internet access. Yuan et al. [13] a new management method was suggested for handling diverse networks, using a technology called Pairing-Free Identity-Based Digital Signature (PF-IBS) algorithm. This approach enhances message authentication within these networks. It's noted for being both safer and more energy-efficient compared to other methods currently used. Bettoumi et al. [14] presented an effective energy-saving approach for secure end-to-end communications based on the compression of the IPv6 header for HIP DEX packets over Low Power Wireless Personal Area Networks (6LoWPAN). ECC cryptography was used to achieve security. K.S. et al. [15] presented a multi-factor authentication using ECC based scheme for secure handover and fingerprint biometric technology considered as two factor authentication. Alagheband et al. [16] present a review of the various security measures to protect the Internet of Things (IoT)-based communications. Traditional cryptographic methods have usually been utilized in providing solutions to different IoT security such as confidentiality of data handled by IoT devices. Using the Battle Royal Optimization, Kumar et al. [17] proposed a Pairing-Free Identity-based Digital Signature (PF-IBDS) Algorithm based on Modified ECC. The research focused on secure data transfer to authenticate messages. Ullah et al. [18] provided an in-depth analysis of lightweight cryptographies for machine-to-machine communication networks based on software and hardware communication devices.

Research Motivation

In the above section, we have reviewed the works under different categories like handover efficiency and security measures. However, such works are still at the initial level of significant challenges for HLWNets. The research gaps that motivate us in this paper to propose the EHPSDT protocol are listed below.

- The current HLWNets solutions heavily relied on the default Li-Fi security approach to achieve data security and privacy preservation. As Wi-Fi in HLWNets is a vulnerable standard, it imposes several security threats on the network.
- The ECC-based solutions [11-18] recently applied to various wireless communication systems, but have not yet been implemented on HLWNets.

III. PROPOSED METHODOLOGY

Figure 1 shows the proposed EHPSDT protocol with its overall architecture and contribution, which includes block Secure Communication Phase (SCP). The EHPSDT framework aims to enhance security and performance in the presence of malicious UEs.

Secure Communication Phase (SCP)

ECC-based cryptographic operations are done to secure data transfers among UEs independent of the network to which they belong. We employed lightweight ECC-based key management approaches in conjunction with an attributed-based encryption (ABE) scheme. According to current research, the ECC-based encryption approach with public key-based message authentication exhibits robust performance and high security. To fulfill the privacy-preserving aim, we created the cryptography model known as AECC techniques. ABE accomplishes attribute-based one-to-many encryption. A cipher text may be decrypted only if the set of attributes of the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 November 2024* ***Revised:*** *12 December 2024* ***Accepted:*** *02 January 2025*

user key matches the properties of the cipher text. Only users who comply with a certain access protocol can read the cipher text in this manner. A critical security aspect of ABE is collusion resistance, which means that no user key can be extracted through collusion. ABE's characteristics make it an excellent choice for authentication in wireless communication networks. The main steps of proposed AECC framework include the system setup, keygen, encryption, and decryption. Algorithm shows the overall functionality of this proposed security model for data transmission among the source UE and destination UE.

Setup Phase $(k) \rightarrow P$: The security model deployed by Certified Authority (CA) at source UE node. It takes input security parameter k and returns the public parameter P.

ECC Keygen $(k, A) \rightarrow (Pu, Pr)$: It takes the security parameter k and corresponding UE set of attributes as input, and returns an ECC secret key and public key pair. An ECC key pair has a secrete key Pr having value from the interval $[1, n-1]$ and then public key Pu calculated as:

$$Pu = G \times Pr \quad (1)$$

Where, G denotes the basis point of an elliptic curve that yields a big prime order n. The n symbolizes the G order. To represent elliptic curve point, we use multiplication by a scalar.

Encryption Phase $(P, PP, Pu) \rightarrow CP$: It takes inputs public parameter P, Plain Packets (PP), and public key Pu and returns the Cipher packets (CP).

Keygen at Receiver $(P, Pr, A) \rightarrow C$: It takes input public parameter P, secrete key Pr, and set of attributes A.

Decryption $(P, C, CP) \rightarrow PP$: It takes input public parameter P, cipher text data CP, and decryption key C and returns the original plaintext packets at the intended receiver end.

In the above steps, the input security parameter k is source UE which generates the periodic packets. The setup phase estimates the P as the public parameter which holds the information about the size of data with its timestamp. The A is a set of attributes that consists of the ID number and IP address corresponding to each source UE. Once packets are encrypted at source UE in CP, it is traveled toward the intended destination UE. On receiving the CP, first, the security key is generated using P, Pr, and A. Finally, C is utilized to decrypt the original packet's information PP. In addition to the above steps, algorithm given below shows the signature generation and verification steps as well to perform the authentication and integrity verification of the encrypted data in the network. For authentication purposes, we designed the Elliptic Curve Digital Signature Algorithm (ECDSA) approach using small size ECC keys. In ECDSA cryptography, the public key size is typically around twice the size of the security level, which in this case is set at 128 bits, resulting in a 256-bit public key. This key is utilized for ensuring the integrity of messages sent from the source UE to the destination UE. While ECC doesn't serve as an encryption method itself, it's paired with the symmetric encryption technique AES-128, which provides 128-bit security. The messages undergo encryption using AES-128 alongside 256-bit ECC public keys.

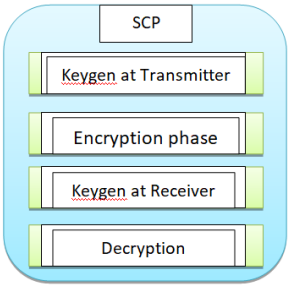

Figure 1 Architecture of secure communication phase (SCP)

Algorithm: AECC-based Secure Transmission

Inputs

$Sue: Source\ UE$
$Due: Destination\ UE$
$rt: Routing\ table$

Output

$Secure\ data\ transmission$

1. $P \leftarrow setup\ (Sue)$
2. $A \leftarrow attributes(Sue)$
3. $[Pr, Pu] \leftarrow keygen(Sue, A)$
4. $PP \leftarrow gendata\ (Sue)$
5. If $(PP \neq null)$

$$CP \leftarrow AES128(P, PP, Pu)$$

Else

discard (PP)

End If

6. $CP^{hash} \leftarrow SHA2(CP)$
7. $CP^{sign} \leftarrow ecdsa\ (CP^{hash}, Pu, Pr)$
8. $rt \rightarrow transmit\ (CP^{sign}, next_{hope})$
9. ***At Next Hope UE***
10. If $(next_{hope} \neq Due)$
11. $CP^{hash} = SHA2(CP)$
12. $stat = verify\ (CP^{hash}, Pu, Pr)$
13. If $(stat\ == 1)$

$$CP^{sign} = ecdsa\ (CP^{hash}, Pu, Pr)$$

$$rt \rightarrow transmit\ (CP^{sign}, next_{hope})$$

Else

discard (CP)

End If

14. Else, at receiver Due
15. $CP^{hash} = SHA2(CP)$
16. $stat = verify\ (CP^{hash}, Pu, Pr)$
17. If $(stat\ == 1)$

$$C \leftarrow kegen(P, Pr, A)$$
$$PP \leftarrow AES128(P, CP, C)$$

Else
discard (CP)
End If

18. Stop

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 November 2024* ***Revised:*** *12 December 2024* ***Accepted:*** *02 January 2025*

IV. Experimental Results

The study outlines the simulation analysis of the EHPSDT protocol within HLWNets, focusing on existing handover techniques. We built HLWNets-specific modules in the NS2 tool because of a lack of open-source simulation tools. The anticipated development brought the different features of the Li-Fi system to completion. The NS2 module for HLWNets offers a comprehensive AP design encompassing MAC, physical layer, UE mobility model, hybrid Li-Fi, and Wi-Fi network integration alongside handover mechanisms. Our design of HLWNets incorporates diverse UE mobility patterns and rates of light path blockage to demonstrate the efficacy of different HLWNets protocols. Since UE mobility and light path obstructions impact the frequency of handovers, this investigation highlights their influence on HLWNet performance through adjustments in their densities. On the other hand, we deployed 10% malicious UEs into each HLWNet to illustrate the efficacy of the suggested security strategy.

Additional experimental requirements involve having a virtual machine tool installed on the primary operating system, Windows 10. The guest OS Ubuntu was installed on the virtual machine. The system RAM was 8 GB, and the processor was an I5 Intel core. We built and analyzed comparable approaches LBG-shadow [19], LB-mobility [20], and LB-simulation [21] to illustrate the benefits of employing the EHPSDT protocol in HLWNets. The existing protocols were developed with considerations for mobility management, shadowing effects, and load balancing, making them closely intertwined with the EHPSDT protocol. However, none of the existing protocols have worked on security challenges in HLWNets. All four protocols are compared using measures such as average throughput, packet delivery ratio (PDR), and communication overhead. In Tables 2 and 3, you'll find the simulation parameters related to scenarios involving UE mobility and obstruction of light paths, respectively. We designed the 1000 × 1000 square foot office area, as indicated in Tables 2 and 3. Figure 2 depicts the deployment of four Wi-Fi access points and Figure 3 depicts the deployment of sixteen Li-Fi access points. The UEs, shadowing effects, and blocking objects are dispersed at random. For 200 seconds, the networks are simulated with light path barriers and UE moving around the office space at random. This section looks at the effects of UE movement and light path obstructions.

A. Investigating the Mobility Scenario through simulation

According to Table 2, HLWNets are built with UE mobility ranging from 0 to 5 m/s. The mobility of User Equipments (UEs) greatly impacts the overall performance of the network. Numerous researches on mobility effect assessments have already been provided by traditional wireless communication systems. As HLWNets represents a distinctive paradigm with UEs moving randomly, it exerts a notable influence on network performance. Even UEs with moderate movement speeds trigger frequent network handovers. As a result, effective mobility management has emerged as a critical problem for HLWNets. We present the results of simulations to analyze the impact of UE mobility on HLWNet performance utilizing protocols like LBG-shadow, LB-mobility, and LB-simulation, and EHPSDT. We also investigate the impact of malicious threats. Figures 4-6 depict the results of several HLWNet protocols for average throughput, PDR, and communication overhead performance parameters with varied mobility speeds.

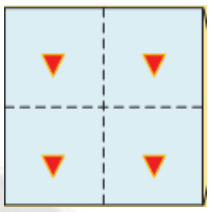

Figure 2 Indoor area with 4 Wi-Fi APs

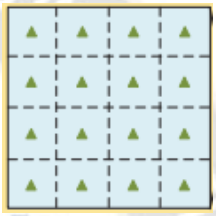

Figure 3 Indoor area with 16 Li-Fi APs

Table 2. UE mobility density scenario for HLWNets

Wi-Fi APs	4
Li-Fi APs	16
User Equipments (UE)	50
Office Area	1000 x 1000 Sq. feet
Height of office	13 feet
Transmission bandwidth	10 MHz
Simulation time	200 seconds
Frequency of Light path blockage	4 times
Mobility speed of UE	0, 1,2,3,4, and 5 m/s
Mobility model of UE	Random waypoint mobility
Optical transmission power in the Li-Fi	10 W
Modulation bandwidth of LED lamp	100 MHz
Malicious UEs	10 %

According to the data provided in Figures 4-6, raising the mobility rate of UEs significantly impacts the overall performance across all protocols. As mobility increases, average throughput decreases (Figure 4), PDR decreases (Figure 5), and communication overhead increases (Figure 6).The EHPSDT protocol improves throughput and PDR, and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 November 2024* ***Revised:*** *12 December 2024* ***Accepted:*** *02 January 2025*

minimizes communication overhead while executing network handovers, and provides security against the MIMA threats.

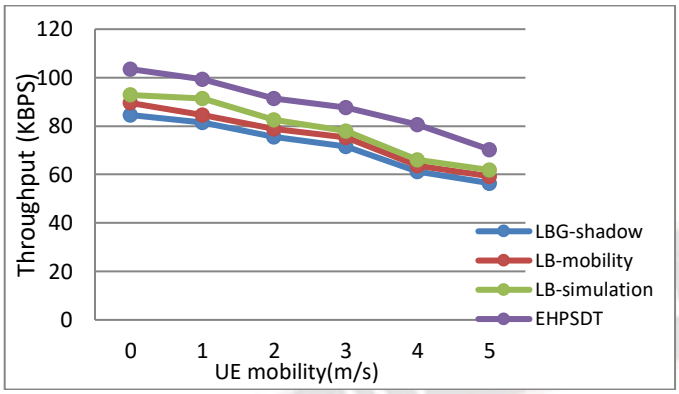

Figure 4 Throughput variation with different UE mobility rates

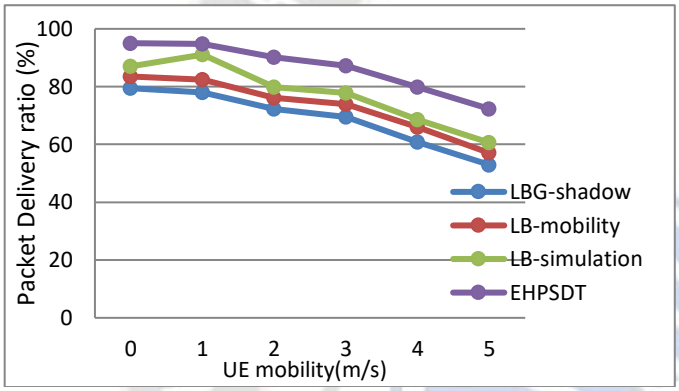

Figure 5 PDR Variation Across Different UE Mobility Rates

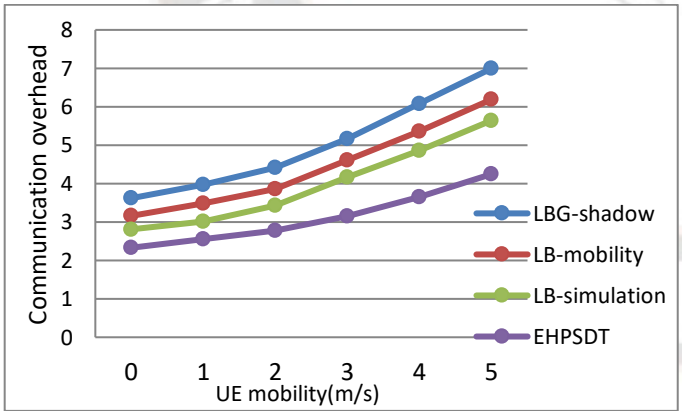

Figure 6 Communication overhead with varying UE mobility rate

Table 4 displays the average results for each protocol in this network environment. The bold numbers show the improvement in each parameter when utilizing the EHPSDT protocol. The EHPSDT protocol exhibits an increase in average throughput of around 10+ Kbps, an enhancement of approximately 9+% in Packet Delivery Ratio (PDR), and a reduction in communication overhead by about 0.83.

Table 4. Average Performance Comparison of HLWNet Protocols in Mobility Scenarios

Type of Protocol	Average Throughput (Kbps)	Average rate of packet delivery (%)	Avg. Communication overhead
LBG-shadow	71.82	68.81	5.03
LB-mobility	75.14	73.15	4.46
LB-simulation	78.75	77.45	3.95
EHPSDT	**88.81**	**86.53**	**3.12**

B. Investigating the Mobility Scenario through Mathematical model

Average throughput: The average throughput of Li-Fi and Wi-Fi Access Points (APs) is contingent upon factors such as the physical layer rate, packet size, and Signal-to-Noise Ratio (SNR). The typical formula for estimating average throughput is then employed as follows.

$$T = \left(\frac{R}{t^2 - t^1}\right) \times \left(\frac{8}{1000}\right)$$

Where R is total packets and t^2 and t^1 are simulation start and end time respectively

Packet Delivery Ratio: It represents the proportion of packets successfully received by the destination from different sources under diverse traffic conditions.

Communication overhead: Communication overhead refers to the ratio of the total number of routing packets to the overall number of data packets in the network. It's calculated as follows:

$$O = \sum_{t} \left(\frac{RT^t}{DT^t}\right)$$

Where, RT^t is aggregate count of routing packets and DT^t is cumulative sum of data packets at a specific time point "t".

V. Conclusion

The novel EHPSDT protocol proposed in this paper for hybrid Li-Fi and Wi-Fi to address the multiple challenges. The hybrid Li-Fi-based networks suffered from key challenges such as frequent handovers, UE mobility management, and lack of security in Wi-Fi communications. The EHPSDT protocol addressed the above challenges by presenting novel algorithms for handover decision-making and lightweight cryptography-based data transmission. The AECC-based cryptography algorithm provides security against the MIMA threats in the network. The simulation outcomes demonstrated the superior effectiveness of the EHPSDT protocol in comparison to the underlying protocols. The average amount of data transferred per unit of time, along with the Packet

Delivery Ratio (PDR), has seen an increase of approximately 19.91% and 14.58%, respectively. Simultaneously, the extra resources needed for communication have decreased by roughly 32.89%. The future work for the EHPSDT protocol is investigating the flickering rate analysis under different conditions. Another limitation of the proposed cryptography approach is the lack of trusted certificate authority.

REFERENCES

[1] Bhuiyan, Mohammad &Reaz, Mamun Bin Ibne. (2016). A complementary metal oxide semiconductor (CMOS) bandpass filter for cost-efficient radio frequency (RF) appliances. Journal of Engineering Research. 4. 114-127.

[2] Farooq, Umar & Rather, Ghulam. (2021). Millimeter Wave Communication Networks: Evolution, Challenges, and Potential Applications. International Journal of Service Science, Management, Engineering, and Technology. 12. 138-153. 10.4018/IJSSMET.2021050108.

[3] Manea, Viorel&Sorin, Puscoci&Stoichescu, Dan-Alexandru. (2019). Practical considerations about LiFi communications. 137. 10.1117/12.2324876.

[4] Tsonev, Dobroslav&Videv, Stefan & Haas, Harald. (2013). Light fidelity (Li-Fi): Towards all-optical networking. Proceedings of SPIE - The International Society for Optical Engineering. 9007. 900702. 10.1117/12.2044649.

[5] Li, Xuan& Zhang, Rong&Hanzo, L.. (2015). Cooperative Load Balancing in Hybrid Visible Light Communications and WiFi. IEEE Transactions on Communications. 63. 1319 - 1329. 10.1109/TCOMM.2015.2409172.

[6] Swami, Kanchan&Moghe, Asmita. (2020). A Review of LiFi Technology. 1-5. 10.1109/ICRAIE51050.2020.9358340.

[7] Jin, Fan & Zhang, Rong&Hanzo, L.. (2015). Resource Allocation Under Delay-Guarantee Constraints for Heterogeneous Visible-Light and RF Femtocell. IEEE Transactions on Wireless Communications. 14. 1020-1034. 10.1109/TWC.2014.2363451.

[8] Sharma, Pradip&Ryu, Jung & Park, Kyung & Park, Jin & Park, Jong. (2018). Li-Fi based on security cloud framework for future IT environment. Human-centric Computing and Information Sciences. 8. 10.1186/s13673-018-0146-5.

[9] Rachit, Bhatt, S. &Ragiri, P.R. Security trends in Internet of Things: a survey. SN Appl. Sci. 3, 121 (2021). https://doi.org/10.1007/s42452-021-04156-9.

[10] Mahajan, Hemant&A.Junnarkar, Dr &Tiwari, Mohit&Tiwari, Tripti&Upadhyaya, Dr. (2022). LCIPA: Lightweight Clustering protocol for Industry 4.0 enabled Precision Agriculture. Microprocessors and Microsystems. 94. 10.1016/j.micpro.2022.104633.

[11] Parrilla, L., Castillo, E., López-Ramos, J., Álvarez-Bermejo, J., García, A., & Morales, D. (2018). Unified Compact ECC-AES Co-Processor with Group-Key Support for IoT Devices in Wireless Sensor Networks. Sensors, 18(1), 251. https://doi.org/10.3390/s18010251.

[12] Kumar, A., & Om, H. (2019). Design of USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks. Digital Communications and Networks. doi:10.1016/j.dcan.2019.07.003.

[13] Yuan, E., Wang, L., Cheng, S., Ao, N., &Guo, Q. (2020). A Key Management Scheme Based on Pairing-Free Identity Based Digital Signature Algorithm for Heterogeneous Wireless Sensor Networks. Sensors, 20(6), 1543. https://doi.org/10.3390/s20061543.

[14] Bettoumi, B., &Bouallegue, R. (2021). LC-DEX: Lightweight and Efficient Compressed Authentication Based Elliptic Curve Cryptography in Multi-Hop 6LoWPAN Wireless Sensor Networks in HIP-Based Internet of Things. Sensors, 21(21), 7348. https://doi.org/10.3390/s21217348.

[15] K. S., S., Rangasamy, J., S. Kamath, S., & Lee, C.-C. (2021). ES-HAS: ECC-Based Secure Handover Authentication Scheme for Roaming Mobile User in Global Mobility Networks. Cryptography, 5(4), 35. https://doi.org/10.3390/cryptography5040035.

[16] Alagheband, M.R., Mashatan, A. Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives. J Supercomput (2022). https://doi.org/10.1007/s11227-022-04586-1.

[17] Kumar, V., Ray, S. Pairing-Free Identity-Based Digital Signature Algorithm for Broadcast Authentication Based on Modified ECC Using Battle Royal Optimization Algorithm. Wireless PersCommun 123, 2341–2365 (2022). https://doi.org/10.1007/s11277-021-09244-y.

[18] Ullah, Shafi& Raja MohdRadzi, Raja Zahilah& Khan, Ilyas&Alshehri, Ali &Yazdani, Tulha. (2022). Types of Lightweight Cryptographies in Current Developments for Resource Constrained Machine Type Communication Devices: Challenges and Opportunities. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3160000.

[19] Wang, Y., Wu, X., & Haas, H. (2017). Load Balancing Game With Shadowing Effect for Indoor Hybrid LiFi/RF Networks. IEEE Transactions on Wireless Communications, 16(4), 2366–2378. doi:10.1109/twc.2017.2664821

[20] Wu, X., & Haas, H. (2019). Load Balancing for Hybrid LiFi and WiFi Networks: To Tackle User Mobility and Light-path Blockage. IEEE Transactions on Communications, 1–1. doi:10.1109/tcomm.2019.2962434

[21] Ullah, S., Rehman, S. U., & Chong, P. H. J. (2021). A Comprehensive Open-Source Simulation Framework for LiFi Communication. Sensors, 21(7), 2485. doi:10.3390/s21072485.