International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 08 | Aug - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Security Enhancement in Optical Wireless Visible Light Communication

Naresh Kumar Meena[1], Ashutosh Kumar Singh[2], Chandan Kumar[3]

[1,2,3]*ECE Department, Dr. Rammanohar Lohia Avadh University, Ayodhya, Uttar Pradesh, India*

Abstract - Since the development of remote applications and benefit, the request for a secure and quick information exchange association requires unused innovation arrangements competent to guarantee the finest countermeasure against security assaults, it is one of the foremost promising unused remote communication innovation, due to the plausibility of utilizing natural counterfeit lights as information exchange channel in free-space. The broadcast nature of VLC makes it fundamental to consider the security of fundamental transmissions. Physical layer information communication and security beneath the channel has ended up a raising concern for communication analysts and due to the victory of physical layer security (PLS) in making strides the security of radio-frequency (RF) remote systems, expanding such PLS techniques to VLC frameworks has been of incredible intrigued. By analysing some cases of the conceivable busybody dangers that can happen in these frameworks, this offers novel bits of knowledge into the vulnerabilities of state-of-the-art PLS plans for VLC frameworks, counting distinctive channel models, input disseminations, arrange arrangements, precoding/signalling techniques, and mystery capacity and data rates and beneath VLC the tall level security and security overhauling arrangements are educated and moderated a period.

***Key Words*:** Visible Light, Physical layer security, Multi User, Spread-spectrum, security performance.

1. INTRODUCTION

With the fast advancement of present day science and innovation, the sum of modern information and data has expanded, which makes the constrained radio recurrence (RF) range assets indeed scarcer. Subsequently, expanding the communication speed and spreading the communication range has ended up an successful way to unravel the issue. With the approach of the enormous information time, the utilize of routine differing qualities innovation and keen radio wire innovation can now not meet communication necessities. The multiple-input multiple-output (MIMO) innovation can enormously progress the space asset utilization of the framework and increment the transmission rate and transmission capacity without expanding the framework transfer speed. The next-generation communications framework points to realize tall unearthly and vitality proficiency, moo idleness, and enormous network since of the broad development of broadcast communications frameworks. Web of Things (IoT) frameworks produce a enormous sum of information transmitted through a organizing framework interfacing bounty of communicating computing gadgets and thus the security of information is exceptionally major concern. In differentiate to radio recurrence remote communication, which needs specialized hardware to find a benefit range, VLC benefit regions are promptly identifiable. In spite of the fact that remote suppliers are conveying extra get to framework by implies of modern cells and WiFi conclusion focuses, the restriction is getting to be abuse of existing RF range. This shows as dispute and obstructions, and comes about in an increment in inactivity and a diminish in arrange throughput – a "spectrum crunch". To reduce this issue, unused approaches to realize bigger potential capacity at the remote connect are required and optical innovations counting unmistakable light communication (VLC) are great.

VLC innovation given with Driven gadgets is characterized by tall zone unearthly effectiveness, unlicensed wide transmission capacity, tall security and dual-use nature. VLC utilizes unmistakable light, the range of which ranges from 400 THz to 700 THz and is permit free; thus, VLC can be misused for high-speed indoor remote communication. VLC offers extra points of interest. On the one hand, since obvious light cannot enter an murky divider, a VLC framework can offer tall security at the physical layer. Be that as it may, in huge open spaces, such as libraries, open-plan workplaces, and conference corridors, it is still conceivable for a malevolent client to listen stealthily a VLC transmission. In spite of the fact that an verification prepare comparable to Wired Comparable Protection (WEP) and WiFi Ensured Get to (WPA) would be conceivable indeed for a VLC framework, such a strategy forces huge signaling and computational overhead and was appeared to be breakable; in this way, it would not be secure.

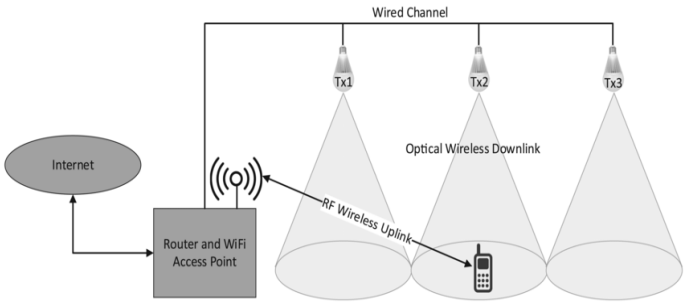

Fig -1: RF and VLC network architecture.

As one of numerous arrange security approaches, physical layer security (PLS) may be a set of strategies that empowers a transmitter and a genuine collector to safely communicate by utilizing the arbitrariness of the channel between the transmitter and the receiver. PLS can be considered to be the foremost secure strategy of communicating, for illustration, in a normal wiretap demonstrate, PLS hypothesis lingerie that secure communication is conceivable when the capacity of the expecting communication channel is higher than that of the spying channel.

In RF frameworks, different PLS transmission methods that permit way better flag gathering at an aiming collector by utilizing different radio wires were proposed, and their data theoretic security exhibitions were analyzed [5]. Too, spurred by the PLS plans of the RF frameworks, various variations of PLS methods securing indoor VLC frameworks were

moreover proposed, such as zero-forcing, vigorous beamforming, manufactured sticking, and light emanating diode (Driven) choice, generalized space move keying (GSSK) balance, etc. However numerous inborn characteristics of VLC frameworks are distinctive from RF frameworks like as the channel, physical properties of the transmitting and getting gadgets, and the flag limitations. Subsequently, it is fundamental to require these contrasts under consideration when fitting PLS strategies to VLC frameworks.

A number of examinations considered these special properties. For case, considered the achievable mystery rates beneath limitations on the input flag adequacy for single-input single-output (SISO) and multiple-input single-output (MISO) scenarios and considered different input flag disseminations to extend the mystery rate. Essential examinations of PLS ordinarily treat a demonstrate whereby a single dynamic sticking gadget or passive eavesdropper is show within the framework, and the area and/or channel properties related with the third-party gadget are expected to be known. In reality, it may be the case that the areas and number of listening in gadgets are not known. Moreover, VLC spies utilize distinctive collector designs than authentic clients in an exertion to captured the flag. The physical highlights of the VLC handset components empower the spy to increase its recipient capability and overcome numerous of the existing PLS strategies.

In light of the current state-of-the-art in VLC technology, the main goal of this article is to argue that the majority of PLS studies for VLC undertaken in recent years were considering naive assumptions that excessively favor the system designer and to offer novel insights into the vulnerabilities of current PLS schemes for VLC systems. Here, we begin by explaining the fundamental differences in the security environments in RF and VLC systems. In another section, a few examples showing that an eavesdropper can break existing PLS techniques are examined.

2. VULNERABILITIES OF TRANSMISSION SECURITY

A few of the famous points of interest of VLC frameworks over RF frameworks is the higher security that VLC frameworks give. This can be essentially acquired from to the reality that light does not enter through dividers. In any case, security issues emerge normally in VLC frameworks due to their open and broadcast nature. Particularly, VLC frameworks may well be as helpless as their RF counterparts when their hubs are sent in open ranges and/or when there are large windows within the scope regions. Hence, security for VLC frameworks is as imperative because it is for RF frameworks. Thus, since VLC is considered as a promising innovation for 5G systems and beyond, and since vigorous end-to-end security is one of the basic necessities of the another era systems, security ought to be profoundly examined within the VLC setting.

Security in remote communication frameworks, counting 5G remote systems, may be improved by presenting physical layer security (PLS) strategies. In truth, PLS procedures have been connected to a wide extend of RF applications in an exertion to progress the generally framework security by complementing existing cryptography-based security strategies. The potential of PLS stems from its capacity to use highlights of the encompassing situations through advanced encoding methods at the physical layer. In fact, PLS plans can be connected within the same soul to VLC frameworks. Compared with RF, VLC has an unlicensed and free of charge optical transfer speed. This makes exceptionally tall information rate communication conceivable and for all intents and purposes fulfills the 1-10 Gb/s/m3 key-performance pointer (KPI) related with following era organize. Besides, since the optical band does not cover with existing RF groups, there's no electromagnetic obstructions with those frameworks.

The greatly tall request for data-rate in another era systems depicted so distant, clearly postures major challenges in terms of security and protection. Due to the tall computation complexity, existing security plans are not appealing. The following era communication innovation has as of late set up as security has got to be considered at each person layer but the strongest security may be accomplished within the physical layer. VLC is predicted as a key enabler innovation to attain quick remote communications. Proficient plans ought to coordinated physical-layer security into existing confirmation and cryptography components for assist securing remote systems. The another era of low-power sensors systems is an region where physical layer security can give magnificent focal points in terms of the number of computations than cryptography. It appears that the proposed engineering can improve the device's cybersecurity by executing a physical layer standalone security arrangement on VLC systems.

From the perspective of information security, PLS is essential for VLC systems that have channel openness and signal broadcasting characteristics. Some improved channel coding schemes that can be used as PLS coding have been proposed. A finite-length punctured low-density parity-check (LDPC) codes to achieve security against eavesdroppers and reliability for legitimate users, a multilevel coding scheme is specifically considered to reduce the increasing security gap by several dB. A decoding algorithm for soft-input soft-output run-length-limited (RLL) codes based on OOK and reed-solomon (RS) codes to address the low data transmission efficiency in PLS-VLC system, experimental results show that their approach has lower error rates compared to eavesdropper with hard-input hard-output RLL decoder and soft-input hard-output RLL decoders. Leveraging the properties of polar codes that are sensitive to channel differences and bound to channel quality, and proposed a polar codes construction scheme for a time-division duplex (TDD) wireless communication system based on the channel quality indicator (CQI), where the frozen bit structure is determined by the instantaneous gains of the legitimate links. However, this method requires the full channel reciprocity of the TDD mode to ensure the transmitter and the legitimate receiver obtain the same channel state information (CSI) of the legitimate link without using a feedback channel. Polar codes can reduce hardware design complexity compared to other PLS techniques, such as beamforming and jamming.

The Obvious Light Communication situation comprises of a transmitter, a genuine collector and an spy. Moreover determined closed-form lower and upper bounds on the mystery capacity of the amplitude-constrained wiretap channel. The achievable mystery rates for the MISO channel and zero-forcing is gotten utilizing the bar shaping procedure and is an fitting methodology for secure transmission over MISO VLC channels and proposed a down to earth vigorous pillar shaping conspire which impressively progresses worst-case mystery rates.

3. THE INTEGRATED CONTRIBUTIONS AND SYSTEM OUTLINES

Against the over portrayal, it presents a comparative ponder of existing procedures, and propose future inquire about headings that join a few practical framework plan parameters. Particularly, most of the inquire about done on PLS-VLC can be classified as either data theoretic, i.e., mystery capacity, achievable mystery rate and capacity-equivocation locale; or flag processing-based, i.e., precoding, beamforming, get to focuses (APs) choice and optimization. A bound together diagram of all PLS-VLC related considers that have been distributed so distant and addresses a few key highlights of VLC frameworks the highlights considered within the examinations are:

1) The characteristics of the VLC channel.
2) The input dispersion: ceaseless versus discrete.
3) The handset plan: models of the transmitter/ collector.
4) The number of true blue clients and unauthorized recipients.
5) The accessibility of the channel state data (CSI).
6) The geometry of the communication environment.
7) The sort of signaling plot utilized: precoding, fake commotion, spatial balance, etc.

Whereas combining the over highlights, four sorts of VLC frameworks can be considered, which are single-input-single yield (SISO), multiple-input-single-output (MISO), multiple-input-multiple-output (MIMO) and half breed RF/VLC. For each sort, both cases of single dynamic client (AU) and different AUs are considered and the impact of the number and CSI of the spies (EDs) on the mystery execution is additionally examined. Besides, a few open investigate issues are proposed to encourage progress the state-of-the-art of VLC advances. Without a doubt, VLCs can offer moo inactivity communications and a range of a few orders of size more noteworthy than conventional communications.

The proceeded think about by the scholarly community and the remote gadget industry have distinguished modern openings utilizing optical recurrence groups. LiFi employments frequencies over 10 GHz, which comes about in more complex arrange framework with littler cells. In a few circumstances, the VLC channel comprises basically of as it were the LOS; in that case, the optical signals will not be subject to blurring. In this way, the nonattendance of blurring, combined with the reality that in VLC frameworks the wavelength of the optical signals is much littler than the getting PDs permits these frameworks to supply exact and dependable situating administrations with centimeter-level precision. The plausibility of deciding the position of the recipient with a certain exactness may be a highlight that produces VLC/OWC exceptionally curiously from a cybersecurity point of see and gives an advantage to authentic recipients over assailants. The tall execution given by VLC may, in a few cases, corrupt quickly in case the collector pivots or moves; at that point there would be a misfortune of flag. An arrangement to this issue can be advertised by reconfigurable brilliantly surfaces (RIS).

The engineering of the proposed coordinates PLS-VLCP framework is appeared in Fig. 2. At the transmitter side, the HSHLC line coding conspire is proposed to coordinated and at the same time transmit the high-speed communication information signals and low-speed situating information signals. Firstly, the high-speed communication information is encoded by polar codes to create communication code words with brief run-length. At the same time, the low-speed situating information is encoded by the interleaves two of five (ITF) codes to produce situating code words without sequential bit “0” or “1”. At that point, the HSHLC encoder utilizes the contrasts in transmission rate, image period, and line coding structure of the two code words to typify them with image period coordinating, whereas embedding emolument images (CS) to meet the coding prerequisites of the situating images transmission.

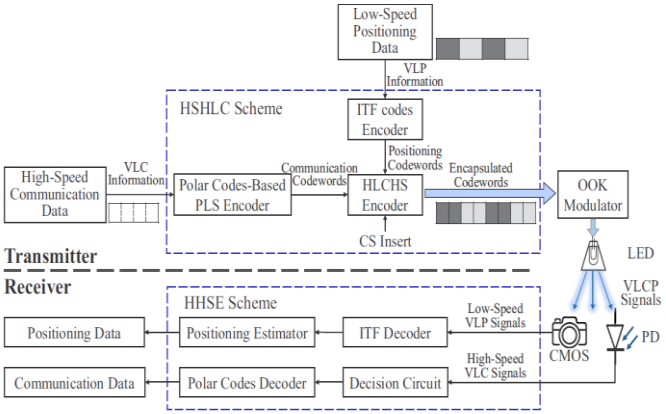

Fig -2: The architecture of the proposed integrated PLS-VLCP system.

At long last, the typified code words are transmitted as an coordinates VLCP signals by the Driven after OOK tweak. At the collector side, we planned the HHSE conspire combining two diverse sorts of PD gadgets with opposite recurrence reactions to partitioned and get the VLCP signals. For the high-speed communication information signals, we utilize a high-bandwidth PD to change over it into electrical signals and re-establish it into transmitted information. As for the low-speed situating information signals, we utilize a CMOS picture sensor with a rolling screen to capture it as a periphery picture and calculate the receiver's position through the pinhole camera show.

To realize PLS communication, proposed a polar codes-based PLS FEC coding plot for communication information encoding utilizing the mystery capacity of the VLC channel demonstrate based on the exactness position of both the transmitter and collector. The polar codes-based PLS encoder can be specifically cascaded with the HSHLC encoder, consistently coordination the VLC data with the VLP data. Furthermore, the coding-based plot can streamline the PLS communication framework and does not meddled with the transmission of the coordinates signals compared to other PLS plans such as beamforming and sticking that require complex equipment plan or flag control.

4. METHODOLOGIES AND FINDINGS

In this, studied the writing of PLS for VLC frameworks taking after the common rules for conducting efficient writing survey that's displayed in. To begin with, the state of the craftsmanship of PLS concept from data hypothesis and security building focuses of see. At that point, the state of the craftsmanship of VLC innovation. At last, distinguished the convergences between the writing of PLS and VLC. Our main objective is to supply an in-depth examination of the PLS strategies utilized for securing VLC frameworks whereas highlighting their qualities and shortcomings. Moreover pointed at distinguishing crevices in current inquire about and

propose ranges for advance examinations. Here recognized PLS methods that were embraced for securing VLC frameworks.

A PLS-VLCP exploratory framework was realized encourage to assess the down to earth execution of the proposed conspire, essentially centering on the integration execution of communication and situating, as well as the PLS communication execution beneath blunder control.

A. OWC and VLC Innovations:

Over the a long time, analysts have distributed numerous papers on OWC and VLC, proposing modern tweak plans and comparing the execution with classical RF communications. More as of late, there have been commitments selecting VLCs as an empowering innovation for next-generation remote communications. Without a doubt, VLCs can offer moo idleness communications and a range of a few orders of greatness more noteworthy than conventional communications. The proceeded consider by the scholarly world and the remote gadget industry have recognized modern openings utilizing optical recurrence groups. Taking after this drift, in later a long time, have created Light-Fidelity (LiFi) that expands the concept of VLC to attain high-speed, secure, two-way remote communications. LiFi employments frequencies over 10 GHz, which comes about in more complex arrange foundation with littler cells. In a few circumstances, the VLC channel comprises primarily of as it were the LOS; in that case, the optical signals will not be subject to blurring. In this way, the nonattendance of blurring, combined with the reality that in VLC frameworks the wavelength of the optical signals is much littler than the receiving PDs permits these frameworks to supply exact and solid situating administrations with centimeter-level exactness. The plausibility of deciding the position of the collector with a certain exactness is a include that creates VLC/OWC exceptionally curiously from a cybersecurity point of see and gives an advantage to authentic recipients over assailants. The tall execution given by VLC may, in a few cases, corrupt quickly on the off chance that the collector turns or moves; at that point there would be a misfortune of flag. A arrangement to this issue can be advertised by reconfigurable cleverly surfaces (RIS). Surfaces made of metal or fluid precious stone might be powerfully designed to coordinate the transmitted light flag to the moving recipient.

B. Sticking as A Security Apparatus:

Mystery capacity is characterized as the greatest transmission rate achievable at whatever point the eavesdropper's channel perceptions are noisier than the authentic user's channel. Hypothetical comes about have appeared that mystery can be made strides by misusing channel varieties. Other commitments utilize sticking to meddled with remote communications, misuse sticking as a apparatus for progressing security in agreeable systems, utilize neighborly sticking as a effective instrument to extend mystery of remote frameworks. Since these plans are basically appropriate in a portable environment, a channel-independent convention called iJAM was presented. With this convention, the sender transmits two times each image, and the collector arbitrarily jams complimentary tests over the two images. This strategy has a few shortcomings in terms of communication throughput since it cuts the information rate by half. In expansion, it has security shortcomings since an foe that watches two successive transmissions might revamp the message by comparing and expelling the stuck bits. WBPLSec overcomes these issues.

C. Incognito Channel Communications:

Cryptographic conventions are the classical implies for ensuring information from unauthorized get to. Tragically, there are cases in which encryption is unseemly; in these cases the utilize of offbeat communication channels can be of offer assistance. We seem say that clandestine channels are elective apparatuses to ensure security of advanced communications through data covering up. Able to utilize them for different legitimate and non-legitimate purposes. In a few cases, we are able utilize clandestine channels to move forward arrange security, whereas in other cases, to breach it. Government and companies can utilize these channels to secure their communications, cyber-criminals can abuse this innovation within the same way. For occasion, it is proposed utilizing undercover channels to balk organize security arrangements by building up unused communication ways. The quality of this approach is the embodiment of data in an existing medium, to dodge any adjustment of standard conventions. Any framework that employments TCP/IP can advantage of covered up communications that transmit data through systems without activating Interruption Discovery Frameworks (IDS).

D. VLC Security:

VLC has picked up noteworthy intrigued due tall data-rate, vigor against obstructions, and moo fetched of LEDs and PDs. By their nature, indoor VLCs are restricted, for illustration, by the room's dividers where the communication is taking put. On the one hand, this could restrain communication by making it vital to introduce other light sources to engender communication between distinctive hotspots. On the other hand, it offers a significant advantage in terms of security and protection. In hone, VLCs offer way better PLS and protection than RF frameworks since light waves cannot pass through dividers, making it about outlandish to interfere into delicate structures by picking up the wireless flag. Numerous commitments within the paper propose VLC-based PLS arrangements to upgrade security of remote communication frameworks. In an illustration; there light concentrated and reflections are combined with the channel estimation to improve security of VLC in IoT.

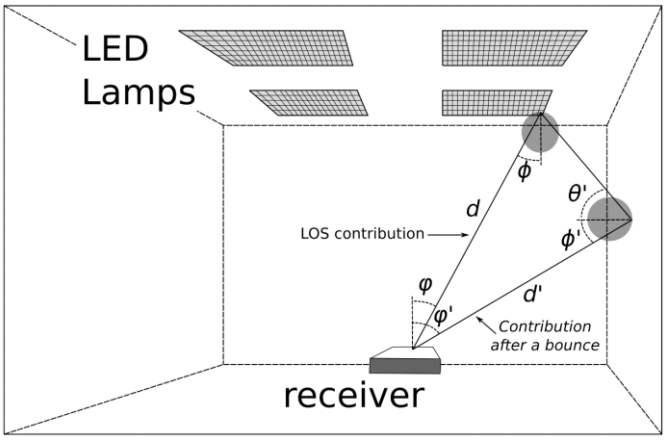

Fig -3: VLC environment with LOS contribution.

An curiously set of commitments examined arrangements utilizing sticking to move forward security of VLCs. For occasion, proposed inviting sticking to anticipate spying. Some

place too proposed other sticking plans to move forward the execution of PLS in VLC frameworks. In such an indoor VLC plot, they accepted to have numerous LEDs mounted on the room's ceiling.

The Driven closest to the authentic collector will transmit the data whereas the others will make a light obstructions towards the aggressor to diminish its SINR. From another viewpoint, depending on the recipient innovation, camera-based VLC employments a camera as a collector rather than PDs to secure versatile communications. In expansion, other commitments appear how utilizing VLCs can have a high directional pick up that produces interferences of data transmission exceptionally improbable, making the joins more secure than we would have with conventional RF communications. Among the inquire about commitments in PLS for VLCs, it is additionally worth specifying those that utilize multiple-input multiple-output transceiver-based beamforming strategies to make secure communication zones. Other analysts have set a physical layer encryption strategy based on optical OFDM to reinforce the secrecy of VLC frameworks. This strategy performs a complex encryption operation on OFDM signals that make it safe to measurable and brute constrain assaults. The utilize of RIS is considered a unused zone of inquire about to move forward VLC security. These reconfigurable surfaces can be utilized in at slightest three ways: energetic multipath tuning, creating sticking, and pillar directing to the genuine collector.

VLC is considered a key enabler innovation for quick remote communications. Such a kind of communication misuses the worldview transmitting whereas enlightening. The accessibility of this free range makes an opportunity for moo taken a toll broadband communication that seem reduce range blockage. This think about appears that WBPLSec, a watermark based VLC with a sticking recipient, can improve devices' cybersecurity by actualizing a physical layer standalone security arrangement. We computed closed-form expressions for the presence of the mystery capacity and of its blackout likelihood for a adjusted wiretap channel. Our approach offers true blue collectors the plausibility to form a secure locale that ensures private communication between them and the transmitters. In this way, abusing this daze full-rate convention, a authentic recipient can, for illustration, trade a mystery shared key with a neighboring gadget within the same room by misusing VLCs. Additionally, in case the aggressor was outside the security locale made by, the communication may be listened stealthily; in this case, sender may still figure out on the off chance that it is in a sticking scope zone and choose not to transmit at all.

We assessed the strength of our approach by considering assailants with persistent get to to remote systems and with the plausibility of moving unreservedly inside rooms. We moreover considered that attackers' capabilities might alter depending on their position generally to the security locale of intrigued. In such a situation, we anticipate assaults just like the followings:

Listening in: This assault points at latently sniffing the communication to analyze it in a moment minute to compromise future communication.

Message Infusion Assault: The objective of this assault is to send a customized and pernicious message to collector to compromise the communication between sender and recipient.

Replay Assault: This assault points to reuse a already transmitted and sniffed message in progressive communication to duplicate the true blue transmission.

Message Alteration: In this case, the objective is to alter the message amid transmission.

WBPLSec can without a doubt relieve these assaults. Privacy of messages is gotten much obliged to the sticking stage, which permits as it were sender to know the sticking focuses and subsequently to reproduce the message. This property permits anticipating listening stealthily. Replay assurance is guaranteed since sender has haphazardly chosen and annihilated a portion of the message, and with each consequent communication, it'll have diverse data and the misshaped bits will too be diverse. This property will anticipate any endeavor by collector to reuse an ancient message and in this way maintain a strategic distance from message infusion and replay assaults. Keenness of sent messages is ensured since a interesting watermark for each transmission is included and in case the assailant tries to alter the watermarked message, sender would take note an abnormal increment within the number of mistakes amid the extraction of the watermark itself. This property avoids message adjustment assaults.

At long last, it is fundamental to note that the proposed calculation is in reverse congruous with the innovation utilized by VLCs. Collector can embed the watermark utilized as it were by it that actualizes WBPLSec; something else, in the event that the recipient does not actualize this calculation, the watermark will not be utilized, and the sticking will not be transmitted. Sender, for his portion, does not expect to know receiver's position, and so when sender jams, this impedances is emanated indistinguishably completely different bearings making accurately a secure locale where sender can communicate with recipient when sender Eve is inside this region. Conceivable improvements of this work may include strategies of focusing on the light beam such that sticking is concentrated in regions of the room where the aggressor is most likely to be found.

5. CONCLUSION

Given in this paper a comprehensive and comparative survey of all PLS procedures detailed within the writing that point to improve the security of VLC frameworks. The detailed methods cover both data theoretic and flag preparing perspectives of VLC frameworks. Diverse sorts of VLC frameworks were considered, counting SISO, MISO and MIMO VLC frameworks, as well as crossover RF/VLC frameworks. In expansion, we considered the effect of different VLC highlights on the mystery execution, counting the input signaling plans, the geometry and parameters of the organize, the number of authentic recipients and meddlers, and the CSI accessibility at the transmitting hubs. We have appeared the potential of a few PLS strategies in upgrading the mystery execution of VLC frameworks. Such methods may incorporate the utilize of discrete input signaling, the utilize of manufactured commotion when the CSI of the EDs isn't accessible as well as the utilize of transfer and crossover VLC/RF frameworks. We too recorded a number of open investigate issues that have incredible potential for progressing the state-of-the-art of security for VLC frameworks. The mystery execution of VLC framework can be altogether progressed in different and unmistakable scenarios through well outlined PLS strategies. What has been finished so distant within the totality of the investigate works on security for VLC frameworks, though being crucial and

unique, it serves as a beginning point for creating reasonable PLS methods custom fitted to real-world settings in an exertion to bring the arrangement of VLC-based frameworks (such as LiFi) closer than ever.

REFERENCES

1. Arfaoui, MA, Soltani, MD, Tavakkolnia, I, Ghrayeb, A, Safari, M, Assi, CM & Haas, H 2020, 'Physical Layer Security for Visible Light Communication Systems: A Survey', IEEE Communications Surveys and Tutorials, vol. 22, no. 3, 9070153, pp. 1887-1908. https://doi.org/10.1109/COMST.2020.2988615.
2. Haggar Cho, S.; Chen, G.; Coon, J.P.; Xiao, P. Challenges in Physical Layer Security for Visible Light Communication Systems. Network 2022, 2, 53–65. https://doi.org/10.3390/network2010004.
3. Tang, J.; Chen, G.; Coon, J.P. Secrecy Performance Analysis ofWireless Communications in the Presence of UAV Jammer and Randomly Located UAV Eavesdroppers. IEEE Trans. Inf. Forensics Secur. 2019, 14, 3026–3041.
4. Yin, L.; Haas, H. Physical-Layer Security in Multiuser Visible Light Communication Networks. IEEE J. Sel. Areas Commun. 2018, 36, 162–174.
5. Cho, S.; Chen, G.; Coon, J.P. Enhancement of Physical Layer Security With Simultaneous Beamforming and Jamming for Visible Light Communication Systems. IEEE Trans. Inf. Forensics Secur. 2019, 14, 2633–2648.
6. Cho, S.; Chen, G.; Coon, J.P. Securing Visible Light Communication Systems by Beamforming in the Presence of Randomly Distributed Eavesdroppers. IEEE Trans. Wirel. Commun. 2018, 17, 2918–2931.
7. Cho, S.; Chen, G.; Coon, J.P. Zero-Forcing Beamforming for Active and Passive Eavesdropper Mitigation in Visible Light Communication Systems. IEEE Trans. Inf. Forensics Secur. 2021, 16, 1495–1505.
8. Yesilkaya, A.; Cogalan, T.; Erkucuk, S.; Sadi, Y.; Panayirci, E.; Haas, H.; Poor, H.V. Physical-Layer Security in Visible Light Communications. In Proceedings of the 2020 2nd 6GWireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
9. Cho, S.; Chen, G.; Coon, J.P. Cooperative Beamforming and Jamming for Secure VLC System in the Presence of Active and Passive Eavesdroppers. IEEE Trans. Green Commun. Netw. 2021, 5, 1988–1998.
10. Arfaoui, M.A.; Ghrayeb, A.; Assi, C.M. Secrecy Performance of Multi-User MISO VLC Broadcast ChannelsWith Confidential Messages. IEEE Trans. Wirel. Commun. 2018, 17, 7789–7800.
11. Abdelhady, A.M.; Salem, A.K.S.; Amin, O.; Shihada, B.; Alouini, M.S. Visible Light Communications via Intelligent Reflecting Surfaces: Metasurfaces vs Mirror Arrays. IEEE Open J. Commun. Soc. 2021, 2, 1–20.
12. S. Pergoloni, A. Petroni, T.-C. Bui, G. Scarano, R. Cusani, and M. Biagi, "ASK-based spatial multiplexing RGB scheme using symbol-dependent self-interference for detection," Opt. Express, vol. 25, no. 13, pp. 15 028–15 042, Jun 2017.
13. S. Soderi, "Acoustic-based security: A key enabling technology for wireless sensor networks," International Journal of Wireless Information Networks, 2019.
14. S. Soderi, L. Mucchi, M. H¨am¨al¨ainen, A. Piva, and J. H. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver." Trans. Emerging Telecommunications Technologies, vol. 28, no. 7, 2017.
15. M. Katz, M. Matinmikko-Blue, and M. Latva-Aho, "6Genesis Flagship Program: Building the Bridges Towards 6G-Enabled Wireless Smart Society and Ecosystem," in 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM), Nov 2018, pp. 1–9.
16. B. Aazhang, P. Ahokangas, H. Alves, M.-S. Alouini, J. Beek, H. Benn, M. Bennis, J. Belfiore, E. Strinati, F. Chen, K. Chang, F. Clazzer, S. Dizit, K. DongSeung, M. Giordiani, W. Haselmayr, J. Haapola, E. Hardouin, E. Harjula, and P. Zhu, Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper), 09 2019.
17. E. Calvanese Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 42–50, Sep. 2019.
18. L. Cheng, W. Viriyasitavat, M. Boban, and H. Tsai, "Comparison of Radio Frequency and Visible Light Propagation Channels for Vehicular Communications," IEEE Access, vol. 6, pp. 2634–2644, 2018.
19. A. Al-Kinani, C. Wang, L. Zhou, and W. Zhang, "Optical wireless communication channel measurements and models," IEEE Communications Surveys Tutorials, vol. 20, no. 3, pp. 1939–1962, thirdquarter 2018.
20. "IEEE Standard for Local and metropolitan area networks–Part 15.7: Short-Range Optical Wireless Communications," IEEE Std 802.15.7-2018 (Revision of IEEE Std 802.15.7-2011), pp. 1–407, April 2019.
21. Shi, G.; Cheng,W.; Gao, X.; Wei, F.; Zhang, H.;Wang, Q. Enhancing Security in Visible Light Communication: A Tabu-Search-Based Method for Transmitter Selection. Sensors 2024, 24, 1906.
22. Zheng, G.; Gong, C.; Xu, Z. Constrained Partial Group Decoding with Max–Min Fairness for Multi-Color Multi-User Visible Light Communication. IEEE Trans. Commun. 2019.
23. Lai, X.; Fu, Z.H. A Tabu Search Approach with Dynamical Neighborhood Size for Solving the Maximum Min-Sum Dispersion Problem. IEEE Access 2019.
24. Chen, Y.; Gao, S.; Tu, G.; Chen, D. Group-Based LED Selection for Generalized Spatial Modulation in Visible Light Communication. IEEE Commun. Lett. 2021.
25. Cho, S.; Chen, G.; Coon, J.P. Securing Visible Light Communication Systems by Beamforming in the Presence of Randomly Distributed Eavesdroppers. IEEE Trans. Wirel. Commun. 2018.
26. Obeed, M.; Salhab, A.M.; Alouini, M.; Zummo, S.A. On Optimizing VLC Networks for Downlink Multi-User Transmission: A Survey. IEEE Commun. Surv. Tuts. 2019.
27. Yapıcı, Y.; Güvenç, I. NOMA for VLC Downlink Transmission with Random Receiver Orientation. IEEE Trans. Commun. 2019.
28. Shi, G.; Aboagye, S.; Ngatched, T.M.N.; Dobre, O.A.; Li, Y.; Cheng,W. Secure Transmission in NOMA-Aided Multiuser Visible Light Communication Broadcasting Network with Cooperative Precoding Design. IEEE Trans. Inform. Foren. Sec. 2022.
29. Morant, M.; Trinidad, A.; Tangdiongga, E.; Koonen, T.; Llorente, R. Experimental Demonstration of mm-Wave 5G NR Photonic Beamforming Based on ORRs and Multicore Fiber. IEEE Trans. Microw. Theory Tech. 2019.
30. Cho, S.; Chen, G.; Coon, J.P. Zero-Forcing Beamforming for Active and Passive Eavesdropper Mitigation in Visible Light Communication Systems. IEEE Trans. Inf. Forensics Secur. 2021.
31. Zhang, F.; Wang, F.; Zhang, J.; Zuo, T. SVM aided LEDs selection for generalized spatial modulation of indoor VLC systems. Opt. Commun. 2021.
32. Yang, Y.; Yang, Y.; Chen, M.; Feng, C.; Xia, H.; Cui, S.; Poor, H.V. Joint LED Selection and Precoding Optimization for Multiple-User Multiple-Cell VLC Systems. IEEE Internet Things J. 2022.
33. Naser, S.; Sofotasios, P.C.; Bariah, L.; Jaafar, W.; Muhaidat, S.; Al-Qutayri, M.; Dobre, O.A. Rate-Splitting Multiple Access: Unifying NOMA and SDMA in MISO VLC Channels. IEEE Open J. Veh. Technol. 2020.
34. Aboagye, S.; Ndjiongue, A.R.; Ngatched, T.M.N.; Dobre, O.A.; Poor, H.V. RIS-Assisted Visible Light Communication Systems: A Tutorial. IEEE Commun. Surveys Tuts. 2023.
35. Shi, G.; Li, Y.; Cheng, W.; Dong, L.; Yang, J.; Zhang, W. Accuracy analysis of indoor visible light communication

localization system based on received signal strength in non-line-of-sight environments by using least squares method. Opt. Eng. 2019.

36. D. Shi, X. Zhang, L. Shi, A. Vladimirescu, W. Mazurczyk, K. Cabaj, B. Meunier, K. Ali, J. Cosmas, and Y. Zhang, "On improving 5g internet of radio light security based on led fingerprint identification method," Sensors, vol. 21, no. 4, p. 1515, 2021.
37. Z. Liu, D. Shi, S. Oukemeni, and X. Zhang, "Alexnet-based visible light communication devices fingerprint extraction and authentication in broadcast systems," in 2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), pp. 01–05, IEEE, 2022.
38. M. Zhu, Y. Wang, X. Liu, Z. Qi, X. Chen, and J.-Y. Wang, "Physical layer security performance analysis for relay-aided visible light communication system," IEEE Photonics Journal, vol. 15, no. 3, pp. 1–9, 2023.
39. X. Deng, S. Mardanikorani, Y. Wu, K. Arulandu, B. Chen, A. M. Khalid, and J.-P. M. G. Linnartz, "Mitigating led nonlinearity to enhance visible light communications," IEEE Transactions on Communications, vol. 66, no. 11, pp. 5593–5607, 2018.
40. D. Shi, X. Zhang, Z. Liu, X. Chen, X. Liu, J. Wang, J. Song, and A. Vladimirescu, "Physics-based modeling of gan mqw led for visible light communication systems," IEEE Transactions on Electron Devices, vol. 71, no. 1, pp. 337–342, 2024.
41. W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6g: A comprehensive survey," IEEE Open Journal of the Communications Society, vol. 2, pp. 334–366, 2021.
42. N. Chi, Y. Zhou, Y. Wei, and F. Hu, "Visible light communication in 6g: Advances, challenges, and prospects," IEEE Vehicular Technology Magazine, vol. 15, no. 4, pp. 93–102, 2020.
43. D. Shi, X. Zhang, A. Vladimirescu, L. Shi, Y. Huang, and Y. Liu, "A device identification method based on led fingerprint for visible light communication system," in Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1–7, 2020.
44. B. Aazhang et al., "Key drivers and research challenges for 6g ubiquitous wireless intelligence," tech. rep., White Paper, Sep 2019.
45. V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6g era," IEEE Access, vol. 9, pp. 142314–142327, 2021.
46. B. Khorsandi et al., "D1.3, targets and requirements for 6g - initial e2e architecture, hexa-x," tech. rep., Feb 2022.
47. IEEE International Network Generations Roadmap, "Security and privacy," 2022.
48. L. Xie, L. Peng, J. Zhang, and A. Hu, "Radio frequency fingerprint identification for internet of things: A survey," Security and Safety, vol. 3, p. 2023022, 2024.
49. J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio frequency fingerprint identification for device authentication in the internet of things," IEEE Communications Magazine, 2023.