GAN-Assisted Secret Key Generation Against Eavesdropping In Dynamic Indoor LiFi Networks

Elmahedi Mahalal*, Muhammad Ismail*, Zi-Yang Wu†, Mostafa M. Fouda‡§, and Zubair Md Fadlullah¶
*Department of Computer Science, Tennessee Technological University, Cookeville, TN, USA,
†College of Information Science and Engineering, Northeastern University, Shenyang, China,
‡Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID, USA,
§Center for Advanced Energy Studies (CAES), Idaho Falls, ID, USA,
¶Department of Computer Science, Western University, London, ON, Canada,
Emails: {emahalal42, mismail}@tntech.edu, wuziyang@ise.neu.edu.cn, mfouda@ieee.org, zfadlullah@ieee.org

***Abstract*—This paper explores the vulnerability of wireless secret key generation (WSKG) to eavesdropping in a dynamic indoor light-fidelity (LiFi) network. It analyzes the channel impulse response (CIR) similarities of two moving user equipments (UEs) across scenarios with two, four, and eight UEs. We observe that as the number of UEs increases, the similarity in CIR also rises, due to the proximal movement patterns among UEs. Specifically, the similarity rate peaks at 70% when eight UEs enter the room; it then drops to 24% during the wandering phase and rises again to 80% as UEs exit the room. Consequently, an eavesdropper among the eight UEs is able to generate 27% of a legitimate UE's secret key, it significantly reduces the key's complexity, decreasing the number of possible keys that need to be tested to break the encryption and making it easier to predict the remainder of the key. To mitigate this issue, we introduce a novel approach that utilizes a generative adversarial network (GAN) to artificially manipulate the CIR, thereby reducing the effectiveness of eavesdropping by adding noise into the observed CIR. This method effectively reduces the CIR similarity to a negligible 1%, thus ensuring the integrity of WSKG against eavesdropping threats.**

***Index Terms*—Wireless secret key generation, LiFi, indoor, deep learning, generative adversarial networks.**

I. Introduction

With the expansion of wireless networks, security threats grow in both complexity and frequency, making the protection of communications against unauthorized access increasingly critical, such in radio networks [1] or light-fidelity (LiFi) networks [2]. Encryption fundamentally safeguards communications, ensuring their confidentiality, integrity, and authentication [3].

To ensure data security, encryption is vital, which in turn requires secure key exchange mechanisms. However, quantum computing poses a significant threat to traditional factorization-based methods, such as Diffie-Hellman, which can be easily compromised [4]. Given this vulnerability, there's a need for alternative approaches to key exchange. One promising solution is to extract encryption keys directly from the properties of the wireless channel. This method does not rely on computational complexity, thus bypassing the vulnerabilities exposed by quantum technologies. Instead, it exploits the randomness of the wireless channel to securely generate and exchange keys [5].

In this, cryptographic key generation from wireless channels emerges as an innovative alternative, suited for the evolving needs of future wireless networks [6]. Nevertheless, assessing the resilience of wireless secret key generation (WSKG) to passive eavesdropping attacks is crucial for validating the reliability of this security technique [7].

A. Related works

The authors in [8] explore the secret key capacity from correlated wireless channels, focusing on factors like sampling delay, eavesdropper's location, and channel qualities demonstrated as signal-to-noise ratio (SNR). Their research suggests that optimal key capacity can be achieved by tuning parameters such as sampling delay and pilot length, providing practical guidelines for secure key generation in the presence of eavesdroppers. Another study, [9], introduces a method for generating keys in static scenarios through randomness and advanced processing, showing high key generation rates. They apply semantic security measures approaches to set upper limits on the successful eavesdropping based on mutual information metrics. Additionally, [10] investigates cooperative key generation against correlated eavesdropping, proposing a jamming scheme that significantly improves security, especially at high SNRs. The authors in [11] propose a key generation scheme that maximizes secret key capacity using IRS. It designs and optimizes IRS elements to improve the SNR for legitimate users while degrading the channel quality for eavesdroppers, thereby enhancing security against eavesdropping.

Limitations Current research on WSKG in dynamic Li-Fi networks, particularly in environments with user movement, is lacking. The study in [12] achieved a key generation rate (KGR) of only 5 bits/s with a high key disagreement rate (KDR) of 40%, due to channel non-reciprocity issues, indicating efficiency gaps. Further [13] improved these figures to an 8% KDR and 89 bits/s KGR using deep learning, but did not address eavesdropping risks. Most research on passive attacks focuses on stationary settings in lower frequencies, overlooking the impact of user mobility and room layouts on WSKG in 5G and higher frequencies. There is also a notable

This work was supported by NSF award #2138234. Dataset generation was supported by the TNTech HPC cluster funded by NSF award #2127188.

absence of studies exploring defensive measures against these challenges.

B. Contribution

This paper addresses the challenge of WSKG in LiFi networks in dynamic environments, where the downlink (DL) operates in visible-light (VL) and the uplink (UL) operates in infrared (IR). Through extensive analysis, we demonstrate how variations in UE density can elevate channel correlation between UEs, thereby facilitating key overlap and increasing the vulnerability against passive eavesdropping attacks.

To address this problem, our contributions are the following:

- We conduct a detailed analysis that highlights the CIR similarity between two UEs by examining their mobility in time and space across varying density of UEs (2, 4, and 8) in a nine desks office layout. The spatial and temporal analyses reveal a notable CIR similarity spike—65-85%—as users walk next to the entry and exit space. However, throughout the other regions of the room space, this similarity doesn't dip below an average of 25%. This finding indicates that an eavesdropper could potentially exploit these CIR similarities to gain access to the same statistical properties as a legitimate user. With access to the same WSKG algorithm, it's conceivable that an eavesdropper could regenerate 27% of the user's key, introducing a significant vulnerability.
- We have identified areas within the room that exhibit high CIR similarity. To mitigate potential eavesdropping in these zones, we propose a generative adversarial network (GAN) defense technique. This approach employs GAN to inject artificial noise directly into the eavesdropper's CIR within these defense zones, effectively minimizing CIR similarity to less than 1% and eliminating the risk of key duplication.

The rest of this paper is organized as follows: Section II introduces the system model. Section III describes the deep learning-based WSKG framework. Section IV provides an analysis of multi-UE CIR similarity. Section V discusses the proposed GAN-based artificial noise generation method to counter passive attacks and presents performance results. Finally, Section VI concludes the paper.

II. SYSTEM MODEL

This section presents an overview of the indoor setup, the human mobility model, and the channel modeling approach.

A. Indoor Setup

The indoor configuration is a 5m × 5m × 3m office layout, equipped with nine desks each measuring 1m in length and 0.75m in width, and 1.3m high. The LiFi network is ensured by four access points (APs), which are placed on the ceiling and distributed uniformly as illustrated in Fig. 1. The human body is abstracted as a cuboidal figure with dimensions of 1.8m × 0.2m × 0.45m, simulating an average human body mass of 70kg. This model allows for a maximum walking speed of 2.1m/s and acceleration up to 1m/s^2. Movements are sampled every 100 milliseconds to accurately capture the dynamics of human mobility. In this simulation, all room surfaces, including the human figure, are assumed to act as blockers to direct line of sight (LOS) communication.

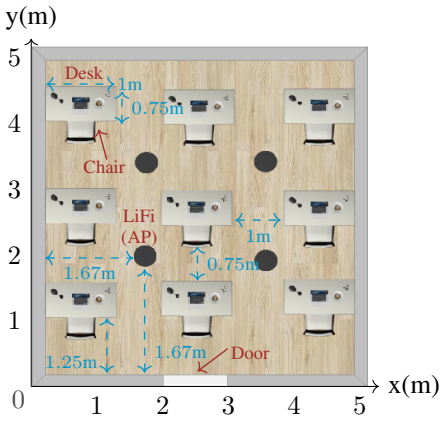

Fig. 1: Office room setup showing the distribution of desks and LiFi APs.

B. Mobility Model

Previously in [14], we introduced an indoor human mobility model that effectively simulates human movements on two distinct scales. Firstly, the *macro scale*, which determines the instants time and destinations target of human movement. Secondly, the *micro scale*, which details the fine-grained patterns of the movement between start and destination points. At the *macro scale*, we employed a semi-Markov renewal process to emulate the return regularity and truncated Lévy walk. At the *micro scale*, we incorporated algorithms for the shortest path navigation, dynamic steering behavior, and the orientation of UEs. The mobility model has been validated in [14] against empirical data gathered using the Phyphox mobile application.

C. Channel model

The LOS impulse response is expressed as

$$h^{(0)}(t,\tau) = \begin{cases} \dfrac{A_R}{d_0^2(t)} \dfrac{(m+1)}{2\pi} \cos^m \psi(t) \cos\theta(t) \\ \times T_S\left(\theta(t)\right) \delta\left(\tau - \dfrac{d_0(t)}{c}\right), \\ \qquad \text{if } 0 \le \theta(t) \le \Psi \\ 0, \quad \text{if } \theta(t) > \Psi \text{ or ray is blocked,} \end{cases} \tag{2}$$

A_R represents the sensor area, ψ and Ψ the angle of irradiance and the receiver's field-of-view (FoV), respectively, c is the speed of light, $T_S(\theta)$ transmission response of the optical system (assumed to be 1), and $d_0(t)$ is the LOS transmission distance. In addition, the mode number m relates to the half-power angle $\Phi_{1/2}$ through $m = -\ln 2 / \ln \cos \Phi_{1/2}$. $\cos\theta(t) = u_\theta^{UL}(t) \cdot u_\theta^{DL} / (\|u_\theta^{UL}(t)\| \|u_\theta^{DL}\|)$. A ray is considered blocked if it intersects any surface, including furniture or the user's body. The channel model in equation (2) applies to both VL and IR.

III. Deep Learning-Enhanced Key Generation Strategy

The non-reciprocity caused by the difference in bands of IR and VL poses a challenge to generate similar keys between the UE and the AP, thus it causes an increased KDR and decreased KGR [12]. In addition, the user mobility, the environmental interactions, and the absence of precise channel models make It crucial to employ a data-driven approach for mitigating the non-reciprocity and optimizing the KDR and KGR [13].

a) WSKG Procedure: The process starts with simulating indoor human mobility as detailed in section II-B. This simulation considers the presence of obstacles such as furniture and human bodies to determine if they obstruct the communication link between the UE and the AP. It then verifies if the incoming signal falls within the receiver's FoV. For the unblocked signals and within the FoV, the CIR is computed according to (2) and then used to extract a secret key through steps that include; channel probing, cumulative-distribution-function (CDF)-based quantization, secure sketch method for information reconciliation and privacy amplification through SHA-256 from the SHA-2 family [15]. These steps are illustrated and detailed in [13], except for the privacy amplification, it is incorporated in this work because of the presence of potential eavesdroppers.

b) Dataset Generation and Stacked-LSTM Model: Utilizing the high-performance computing (HPC) cluster at Tennessee Technological University, we generated UL and DL CIR datasets. This data collection, based on 1000 mobility traces per user for $2, 4,$ and 8 users density, and 120 CIR per scenario.To learn the channel characteristics between the UE and AP and to minimize the keys mismatch between them, we have developed a stacked long short-term memory (LSTM) model. By employing Backpropagation-through-time (BPTT) and a grid search for hyperparameter tuning, we achieved optimal configuration of two hidden LSTM layers; the first with 56 hidden units and $\tanh$ activation function, while the second uses 72 hidden units and Sigmoid. The input layer takes the shape of the UL CIR , where the output layer uses Softmax across 2^V neurons (V is the quantization level), trained using a 0.001 learning rate and the Adam optimizer. This model learns how to select quantization thresholds at the AP using the UL CIR that are the same selected at the UE by minimizing categorical cross-entropy. Detailed methodologies for data preprocessing and model optimization are provided in [13].

IV. Multi-UE CIR similarity

In the following sub-sections, we will explore the temporal and spatial CIR similarities, as well as the potential for key leakage, between two UEs-legitimate and eavesdropper-when they are the only ones present, as well as in scenarios with 4 UEs and 8 UEs. This analysis aims to understand how user density affects communication security and channel characteristics.

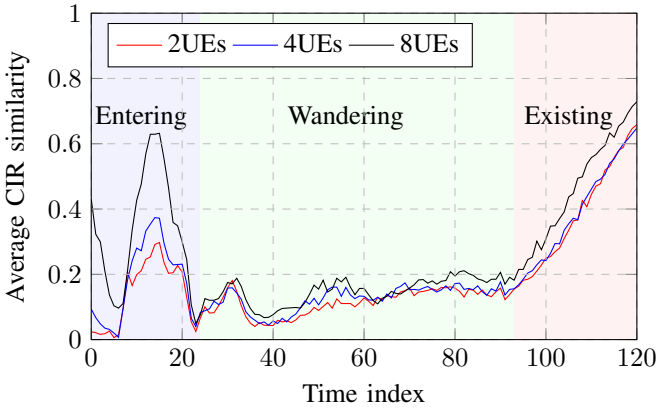

Fig. 2: Average CIR similarity between the legitimate and the eavesdropper over time for 2, 4, and 8 UEs density during entering, wandering, and existing stages, in nine desks room layout.

a) Temporal analysis: First we study the CIR similarity between the legitimate and the eavesdropper by performing a point-by-point comparison between their CIRs, then we take the average over all the 1000 scenarios. Fig. 2 illustrates the average similarity of CIR under different user densities: 2, 4, and 8 UEs. This analysis captures three key spaces of user mobility: *entering*, *wandering*, and *existing* the room.

Key observations from the figure include:

- Increasing UE density from 2 to 8 leads to a significant rise in CIR similarity, particularly evident whenever the UEs wander in the entering and existing areas with up to a 30% increase. This trend ensures closer proximity among UEs increase CIR similarities.
- User mobility areas impact CIR similarity:
  - The entering phase sees a notable peak in similarity, especially at higher 8 UEs density, indicating similar channel experiences as users initially move into the room.
  - During the wandering phase, similarity fluctuate but remains distinct, reflecting the diverse paths and positions UEs step within the room.
  - The exiting phase marks a consistent increase in similarity, more so with greater UE numbers, as users converge towards the exit, aligning their channel conditions more closely.

We have conducted a statistical analysis over a four-month period, assessing user traffic patterns within a room layout same to that depicted in Fig. 1. Our findings indicate an average occupancy of 5 UEs at any day. However, it is important to note that the room has the potential to accommodate a larger, more crowded environment, which significantly elevates security concerns. The observed high CIR similarity in both the entry and exit areas results in extensive key overlap between legitimate users and potential eavesdroppers. Moreover, during periods of user movement in the room, there is a 20% similarity which is not negligible. This overlap substantially compromises the security of the

key. Advanced AI models employed by eavesdroppers could potentially predict the remaining segments of the key, which further the security risks. Given these findings, we strongly need a thorough mitigation against such eavesdropping risks.

b) Spatial analysis: Our analysis is visualized through three heatmaps, each depicting the average CIR similarity between the legitimate UE and the eavesdropper located at various positions within the room, shown in Fig. 3. These heatmaps are generated for varying numbers of UEs 2 in Fig. 3 (a), 4 in Fig. 3 (b), and 8 in Fig. 3 (c) to explore the spatial dynamics of CIR similarity.

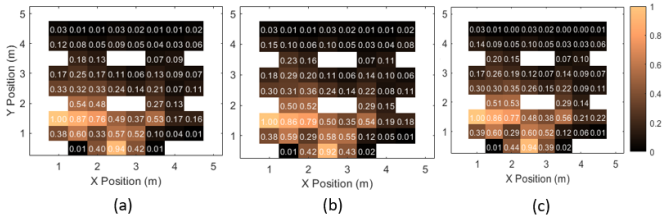

Fig. 3: The areas depicted represent the average CIR similarity between the legitimate UE and the eavesdropper under different conditions: (a) with only the two UEs present, (b) in the presence of 4 UEs, and (c) in the presence of 8 UEs.

Key observations from our study include:

- Specific locations, such as the area near the (1.5 m,1.5 m) coordinate, consistently exhibit high CIR similarity. This indicates that UEs near the first AP, such as those near the door, share similar channel characteristics. To explain why the area under the first AP shows the highest similarity, we consider that the UE initially connects to this AP, then a handover only occurs if the signal is totally lost, (threshold 1 as noted in [12]), which accounts for the observed similarity in this area. Additionally, some areas show 100% CIR similarity, contrasting with temporal analysis results. This is because, in spatial similarity, values are clustered to represent specific areas.
- CIR similarities do not simply cluster but spread across the area under the second AP with coordinate (4 m,1 m) as number of UEs increase from 4 to 8 shown in Fig. 4(b) and Fig. 4(c), respectively. This distribution might initially show a weak increase in CIR similarity; however, a closer analysis reveals a significant overall increase—15% in CIR similarity. This spread in CIR similarity concludes that an increase in UE density leads to a spread of CIR similarity around the room.

This analysis demonstrates the relationship between user density and spatial positioning in shaping CIR similarity within indoor environments. Specific locations consistently exhibit high CIR similarity, this insight highlights areas where eavesdropping mitigation should be intensified, rather than uniformly deploying it across the entire room.

c) Key leakage: As detailed in Sections II and III, we generate secret keys for all users within the room environment. We then examine the similarity across 240 consecutive bits between two UEs for varying user densities: 2, 4, and 8 UEs over the 1000 scenarios, this number of bits is enough for encryption as described in [16]. The findings are presented in TABLE I.

TABLE I: Key leakage for different UEs.

Number of UEs	2 UEs	4 UEs	8 UEs
Key Leakage (%)	10.32	11	27

This analysis reveals a clear trend: as the number of UEs in the room increases, so the key leakage rate increase. Specifically, within this room, the introduction of 8 UEs leads to a key leakage rate of 27%, highlighting the risk of key compromise with increased number of users. These results demonstrate the key generation process's sensitivity to both the number of users and their spatial distribution, underscoring the need for robust security measures to defense the WSKG in dense user environments.

V. GAN-BASED ARTIFICIAL NOISE GENERATION AGAINST PASSIVE ATTACKS

GANs can model the complex statistical properties of the legitimate UE's CIR. After training, the GAN can generate synthetic noise that mimics our environmental and system CIR characteristics but does not replicate any real UE's CIR. This ensures that the eavesdropper cannot derive useful information from intercepted signals. Using actual CIR data can lead to privacy issues, as it involves handling and manipulation of real UE data. The traditional reversed CIR method might not be as effective in dynamic environments where CIR characteristics can change rapidly due to user movement or other environmental factors and easy to reverse-engineer [17]. GANs can continuously learn and adapt to new environmental conditions in real-time, making the noise generation more robust against changes, once trained, GANs can generate noise for different scenarios without needing to re-collect and process new user data which is the case in tradition reverse methods. Furthermore, artificial noise generated by GANs can be designed to be less predictable and harder for eavesdroppers to filter out or reverse-engineer compared to simple inverse CIR broadcasting. In this work, we deploy a GAN to generate synthetic noise in the zone of high CIR similarity. The GAN first extensively learns and models the inverse of the legitimate UE CIR, then it generates the artificial noise. The GAN architecture comprises two components: a generator (G) that creates synthetic data from random source of noise, and a discriminator (D) tasked with distinguishing real data from the generator's synthetic output. Their interaction forms a minimax game, described by a specific objective function: the generator aims to fool the discriminator into mistaking synthetic data for real, while the discriminator learns to identify the generator's fake data more accurately. Finally the GAN generates an artificial reversed legitimate UE CIR. This synthetic CIR is broadcast within the defense zone, effectively disrupting the eavesdropper's ability to match or mimic the legitimate UE's signal, thereby mitigating the risk of eavesdropping and enhancing overall communication security.

After extensive hyperparameter optimization, we finalized the architectures for both components of our GAN, designed specifically for optimal synthetic CIR scenario generation.

The generator model consists of a feedforward neural network with three layers: the first and second layers have 128 and 256 neurons, respectively, both using ReLU activation, and the final layer has 127 neurons with tanh activation, mapping outputs to the -1 to 1 range for synthetic CIR scenario generation. Conversely, the discriminator uses a 1D convolutional neural network (CNN) with 128 filters and ReLU activation, followed by a flattening step and a dense output layer with sigmoid activation for binary classification of the CIR scenarios as real or fake.

A. Results

In our approach, we consider the second UE as an eavesdropper and utilizing the results from Section IV.B we deploy a GAN model within the first AP. By introducing this artificial noise into the eavesdropper's intercepted signals, we achieve a significant decrease in signal similarity, dropping to below 1% in scenarios involving 8 UEs.

This outcome demonstrates the artificial noise technique's efficacy, especially in dense UE environments. It leads to a notable decrease in eavesdropping success, showcasing negligible CIR similarity and effectively null key leakage, maintaining a 0% leakage rate as illustrated in Fig.4. This evidence points to the GAN-generated noise as a powerful tool for safeguarding communications against eavesdropping attempts in complex wireless environments.

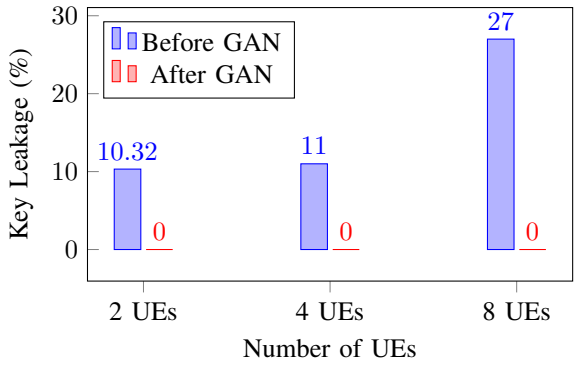

Fig. 4: Key Leakage for different UEs: before and after GAN utilization

VI. Conclusion

In this study, we investigated the CIR similarity in an indoor LiFi environment and assessed the vulnerabilities of secret key generation in the presence of user mobility. Our simulations captured significant similarities in CIR between two UEs, especially as users entered or exited the room, with peak similarities ranging from 70% to 80%.

Our findings revealed a potential for substantial key leakage, with up to 27% under high user density scenarios. To address this vulnerability, we introduced a GAN-based method for generating artificial noise, which successfully reduced CIR similarity to about 1%, effectively nullifying the key leakage.

The implementation of GAN for noise generation marks a significant advancement in securing dynamic LiFi networks. By manipulating CIRs to impede eavesdroppers, we ensure robust key generation even in scenarios of high user density and mobility. Future work could explore the scalability of this method across different network configurations and further refine the AI models to adapt to varying environmental complexities.

References

[1] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5g mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[2] H. Abumarshoud, M. D. Soltani, M. Safari, and H. Haas, "Realistic secrecy performance analysis for lifi systems," *IEEE Access*, vol. 9, pp. 120 675–120 688, 2021.

[3] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1093–1111, 2019.

[4] S. P. Jordan and Y.-K. Liu, "Quantum cryptanalysis: Shor, grover, and beyond," *IEEE Security Privacy*, vol. 16, no. 5, pp. 14–21, 2018.

[5] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 6–11, 2019.

[6] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for iot security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[8] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Communications Letters*, vol. 21, no. 4, pp. 961–964, 2017.

[9] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[10] P. Xu, J. Yang, G. Chen, Z. Yang, Y. Li, and M. Z. Win, "Physical-layer secret and private key generation in wireless relay networks with correlated eavesdropping channels," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 985–1000, 2024.

[11] Y. Liu, K. Huang, S. Yang, J. Yang, and X. Sun, "Secret key generation for intelligent reflecting surface assisted wireless communication networks with multiple eavesdroppers," in *2021 International Conference on Advanced Computing and Endogenous Security*, 2022, pp. 1–6.

[12] E. Mahalal, M. Ismail, Z. Wu, and M. M. Fouda, "Characterization of secret key generation in 5G+ indoor mobile LiFi networks," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022.

[13] E. Mahalal, M. Ismail, Z.-Y. Wu, M. Fouda, Z. Md Fadlullah, and N. Kato, "Robust deep learning-based secret key generation in dynamic lifi networks against concept drift," in *IEEE CCNC*, 2024.

[14] Z.-Y. Wu, M. Ismail, J. Kong, E. Serpedin, and J. Wang, "Channel characterization and realization of mobile optical wireless communications," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6426–6439, 2020.

[15] National Institute of Standards and Technology. (2015) Secure hash standard (shs). U.S. Department of Commerce. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[16] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, "Advanced encryption standard (aes)," 2001-11-26 2001.

[17] S. Li, N. Li, X. Tao, Z. Liu, H. Wang, and J. Xu, "Artificial noise inserted secure communication in time-reversal systems," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6.