Journal of Ubiquitous Computing and Communication Technologies (ISSN: 2582-337X)
www.irojournals.com/jucct/

Ensuring Privacy in Wireless Channels with Physical Layer Security: A Survey of Encryption Strategies

S. Revathi[1], M Abisri[2], C. Aparna[3], G. Lidhuna[4]

[1]Assistant Professor, Department of Computer Science and Engineering, Erode Sengunthar Engineering College (Autonomous) Thudupathi, Erode, Tamilnadu, India

[2,3,4] Final Year, Department of Computer Science and Engineering, Erode Sengunthar Engineering College (Autonomous) Thudupathi, Erode, Tamilnadu, India

E-mail: [1]revathiesec25@gmail.com, [2]abisrim161202@gmail.com, [3]caparna003@gmail.com, [4]lidhuna8032003@gmail.com

Abstract

This paper reviews various encryption strategies designed to enhance privacy in wireless communication, with a focus on leveraging physical layer security. Exploring techniques that utilize inherent wireless channel features for secure communication, the survey presents the strengths and challenges of each method. The aim is to provide a straightforward overview for researchers, practitioners, and decision-makers, about the evolving landscape of encryption methods in wireless channels for improved privacy. Furthermore, it discusses how these physical layer key generation techniques can be integrated with advanced technologies by providing a suggested model by combining the Machine learning and the Multi authority ciphertext-policy attribute-based encryption (CP-ABE) to ensure privacy in wireless channels.

Keywords: Conventional cryptographic algorithms, cryptographic solutions, Multi authority ciphertext-policy attribute-based encryption, Wireless channel

DOI: https://doi.org/10.36548/jucct.2023.4.006
Received: 18.12.2023, received in revised form: 14.01.2024, accepted: 30.01.2024, published: 08.02.2024
© 2023 Inventive Research Organization. This is an open access article under the Creative Commons Attribution-Non-commercial International (CC BY-NC 4.0) License

1. Introduction

The wireless channel functions as the unseen foundation of our modern interconnected society, facilitating the smooth transmission of information and communication over long distances without the limitations of physical cables. This complex medium serves as the pathway for electromagnetic waves carrying signals for voice, data, and multimedia. The wireless channel, known for its dynamic and often unpredictable nature, plays a central role in various technologies such as mobile communications, Wi-Fi networks, satellite links, and more. But the data transmission through the wireless network is often affected by the many security issues like eaves dropping, Man-in-the-Middle Attacks, Jamming, Spoofing, Physical Layer Attacks, Signal Interception and Replay Attacks, Wireless LAN Vulnerabilities, Device Misconfiguration, Physical Location Tracking etc. Handling these security problems in wireless channels requires the implementation of robust encryption, authentication protocols, intrusion detection systems, and secure configurations. As physical layer security is very much essential to address the above-mentioned security issues that are inherent in wireless channel, the proposed study aims to review the physical layer encryption methods of the wireless channel.

1.1 Physical Layer Encryption

In today's age, where the smooth transfer of data and information is crucial, the protection and confidentiality of wireless communications have gained utmost importance. Physical layer encryption, an advanced and inventive technique for securing wireless communication, plays a crucial role in achieving this objective. Unlike conventional encryption methods that function at higher protocol layers, physical layer encryption focuses on securing the data at the fundamental layer of wireless transmission. By utilizing the inherent properties of radio signals to encode and safeguard information, this method offers strong resistance against different types of eavesdropping and interference. Physical layer encryption, also known as physical layer security or secure communication at the physical layer, is the process of safeguarding communication channels by taking advantage of the physical properties of the communication medium itself. Unlike standard encryption approaches, which focus on hiding information through algorithms and cryptographic keys, physical layer encryption uses the natural features of the transmission medium to enhance security.

Encrypting wireless communications in real-time is a crucial aspect of safeguarding the transmission of sensitive data in our increasingly interconnected world. As wireless technology continues to progress, it becomes imperative to employ robust encryption techniques to ensure the confidentiality and integrity of the exchanged information. One highly secure approach is the utilization of a one-time pad (OTP) and key generation. When implemented correctly, this method offers an invulnerable encryption scheme, preventing unauthorized individuals from intercepting or deciphering the transmitted data. This article provides an in-depth study about the different physical layer security available

In today's interconnected world, where wireless communication is prevalent, it is crucial to ensure the confidentiality and integrity of data transmitted through the airwaves. Physical Layer Security, an innovative approach to safeguarding wireless communications, plays a vital role in this endeavor. Unlike traditional cryptographic methods that primarily focus on securing data in higher network layers, physical layer security utilizes the unique characteristics of the wireless channel itself to protect information. This makes it an indispensable tool in defending against eavesdropping and cyber threats. In this article, we will explore the concept of physical layer security, its fundamental principles, the advantages it offers, and its potential to revolutionize wireless communication security as well as suggest a physical layer encryption to address the security issues

The proposed study in order to address the security issues of wireless channel that exhibit dynamic and scalable characteristics, suggests an multiauthority cipher text attribute based encryption combined with the machine learning offering a fine-grained access control in wireless networks, collaborative key generation for enhanced security, adaptability to heterogeneous devices and attributes ensuring a flexible management.

1.2 Objective

- To study the physical layer encryption method that are used in the wireless channel communication
- To suggest a proposed work flow on the multiauthority CP-ABE and machine learning
- To discuss the advantages of the suggested method and the future progress of the research.

2. Related Study

In research, propose a novel practical approach to achieve perfect secrecy for wireless communication using the one-time pad method. This method does not employ the conventional cryptographic method used at the upper layers of a wireless network, instead offers an enhanced security by avoiding the vulnerabilities associated with computational complexity. It also takes into consideration the potential impact of future advancements in Quantum computing. Additionally, the authors address the challenge of establishing a shared key in symmetric security systems, where securing the channel and sharing the key are interdependent. Given the widespread use of wireless communication in various information technology applications, ensuring security and privacy has become a critical concern. The inherent broadcast nature of wireless communication exposes it to eavesdropping, necessitating the inclusion of robust security measures [1].

This article presents an innovative encrypted scheme for the transmission of the data using an “intelligent reflecting surface” (IRS) by generating secret keys. The authors demonstrate that by employing a simple random phase shifting of the IRS elements, perfectly secure one-time pad (OTP) communications can be achieved. An optimal time slot allocation technique is developed for both the IRS secret key generation and the encrypted data transmission phases in order to maximize the secure transmission rate. Furthermore, a Poisson point process (PPP)-based theoretical definition of the key generation rate is derived for real-world settings in which the channel state information (CSI) of eavesdroppers is not known. The IRS technology's low cost, excellent spectrum efficiency, and energy efficiency make it a promising option for upcoming mobile communication systems. The IRS reconfigures the electromagnetic propagation environment to improve wireless device communication performance by dynamically altering the phase shifts of passive reflecting materials. The production of secret keys via IRS is still substantially unexplored, despite the fact that prior research in IRS-assisted networks has mostly concentrated on beamforming and artificial noise vectors [2]. In this paper [3], a method for securely transmitting the data between the ground control station (GCS) and the unmanned aerial vehicles (UAVs) and is laid out. The focus is on achieving maximum security while dealing with limited computational resources. The authors demonstrate that using OTPS for encryption is a feasible method under these situations. This technique leverages one-time pads demonstrated total cryptographic security and quick encryption speed. Furthermore, it uses the memory reserved for the one-time pad

not just to store gamma sequences but also to store encrypted data. The development of mobile robotic systems, particularly UAVs, is a highly promising and significant area of research in intelligent control systems. Ensuring the security of data transmission within UAV groups and between UAVs and GCSs is a critical concern.

The paper [4] introduces the concept of Physical layer key generation (PKG) as a method to generate shared secret keys in real-time by utilizing the radio channel's inherent randomness. However, the of is propagation environments heavily influence the PKG effectiveness. To address this, the authors propose the use of reconfigurable intelligent surfaces (RIS) to control the wireless environment and enhance the performance of PKG. In contrast to previous studies, this paper investigates both the positive and negative impacts of PKG with the RIS scheme. The constructive aspect explores the potential applications of RIS in static and wave-blockage environments for future wireless systems. Experimental results in a static setting show that RIS can greatly boost the entropy of the secret key, resulting in a key generation rate (KGR) of 97.39 bit/s and a bit disagreement rate (BDR) of 0.083. PKG offers a promising solution for establishing symmetric keys in wireless communication networks without the need for complex ciphers, making it suitable for ubiquitous connectivity.

In this paper [5], the concept of steganography, which has been utilized for concealing information over the course of history. In the field of cryptology, the information that needs to be concealed is encrypted. Both of these areas of study are extensively employed in the domain of secure communication. The research focuses on digital image steganography, a specific application of steganography, where we have developed and implemented a technique to hide text within selected images. To accomplish this, we initially employ the discrete Haar wavelet transform to obtain the low bands of the images, which will be used to conceal the data. The text to be hidden is then encrypted using the one-time-pad algorithm. The encryption key is transmitted to the recipient through a transmission layer based on a Highly Secured Information Exchange Algorithm. This algorithm utilizes a randomly generated key pool that is maintained by both the sender and the receiver. For each message, a random key starting point is generated by selecting a key from the pool. A significant condition for a one-time pad is that there should be no key repetition; this is ensured by the size of the pool and the randomness of the selection procedure. Using the least significant bit approach, the resulting cipher text and the key starting point indicator are hidden within the

low bands of the images. Information security has been achieved through a variety of approaches that have been tried and tested throughout human history.

3. Existing System

This article describes a novel encryption strategy for modulated signals in the physical layer known as a onetime pad (OTP). The method uses a wireless channel to ensure secure connection. By simulating the OTP encryption process for bit sequences, we demonstrate the essential conditions for flawless encryption of modulated signals and provide a thorough proof. Furthermore, we provide a detailed approach for implementing this scheme in a wireless system. Because the plaintext in this scenario is represented by modulated signals rather than bit sequences, we use high-level quantized channel estimate samples as secret keys and create encryption methods suited for QAM and PSK signals.

4. Proposed System

A proposal is made for providing a physical layer security in the wireless communication channel. The suggested method put forth tries to enhance the security and the privacy in data transmission against many security issues such as eavesdropping and unauthorized access, man-in-the-middle attacks, jamming and denial of service (DOS), spoofing and impersonation, physical layer attacks, interference and signal interception, quantum threats, location privacy etc that arise in the physical layer of the wireless channel. The method put forth combines the machine learning with the multiauthority ciphertext-policy attribute-based encryption to address the dynamic and complex challenges inherent in wireless communication environments, offering a flexible, adaptive, and holistic approach to physical layer security. This integration enhances the capabilities of ABE systems, making them more responsive to real-time conditions and better equipped to mitigate evolving security threats.

4.1 Multiauthority Ciphertext-Policy Attribute-Based Encryption

This section details the general work flow of the Multiauthority Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The multiple-authority ciphertext process begins with system parameter generation, followed by the distribution of public parameters to all involved authorities. Each authority generates a private key and a master key for the attributes it

manages. The relevant authorities receive the attribute set from the user, generate a private key for the user, and distribute it to the user. The data owner defines an access policy based on attributes, encrypts the data using the access policy, and generates a ciphertext. The data owner encrypts the data with the ciphertext based on the access policy, using the public parameters from all relevant authorities for encryption. When a user possessing a private key request a decryption key from the authorities, the authorities collaborate to generate a decryption key for the user. The user then decrypts the ciphertext using the generated decryption key [6,7,11].

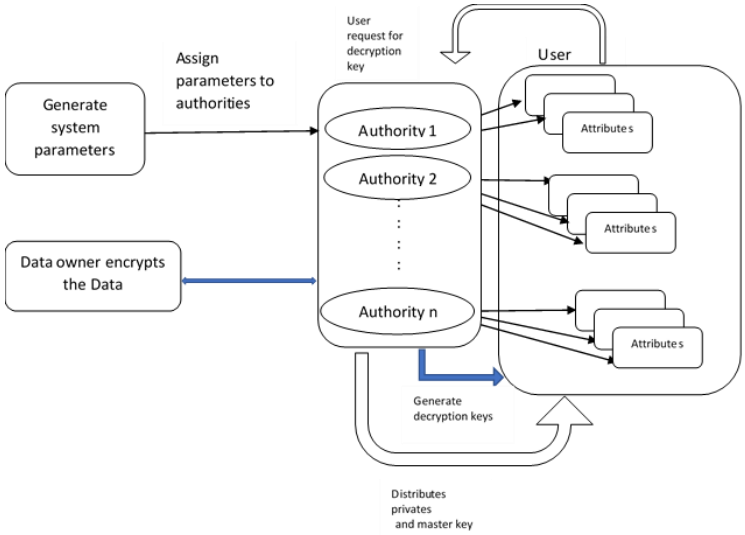

Figure 1. Flow Diagram of Multiauthority CP-ABE

4.2 Machine Learning with Multiauthority CP-ABE

The integration of Multi-authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE) with machine learning (ML) for wireless communication offers several advantages. It combines the strengths of attribute-based encryption with the adaptive decision-making capabilities of ML, providing dynamic access control, predictive key generation, anomaly detection for security monitoring, adaptive attribute management, optimized key generation parameters, user authentication enhancements, and continuous learning for security enhancement. In a wireless channel environment, where conditions and users' roles may change frequently, ML models can analyze patterns in user behavior, device characteristics, and network conditions to dynamically adjust and ensure adaptive and

context-aware security. ML can also predict users' attribute requirements based on historical usage patterns, allowing for proactive key generation [8,12].

Given the diverse security threats in wireless communication, ML-enhanced Multi-authority-CP-ABE provides a proactive defense mechanism against unauthorized access or malicious activities. ML's capability to detect anomalous patterns in user behavior or access requests contributes to this proactive defense. ML-driven attribute management ensures that access policies remain aligned with the current context, even if the capabilities of devices or users' roles change. ML algorithms can optimize key generation parameters based on real-time network conditions, device capabilities, and user behaviors, enhancing the overall efficiency and performance of Multi-authority-CP-ABE. Moreover, ML's ability to continuously learn from new data makes the system adaptable to emerging security threats in the wireless channel. This combined approach ensures a robust security framework. The flow chart in figure.1 shows the generalized workflow for integrating ML with multiauthority CP-ABE for the physical layer security in a wireless channel [9,10].

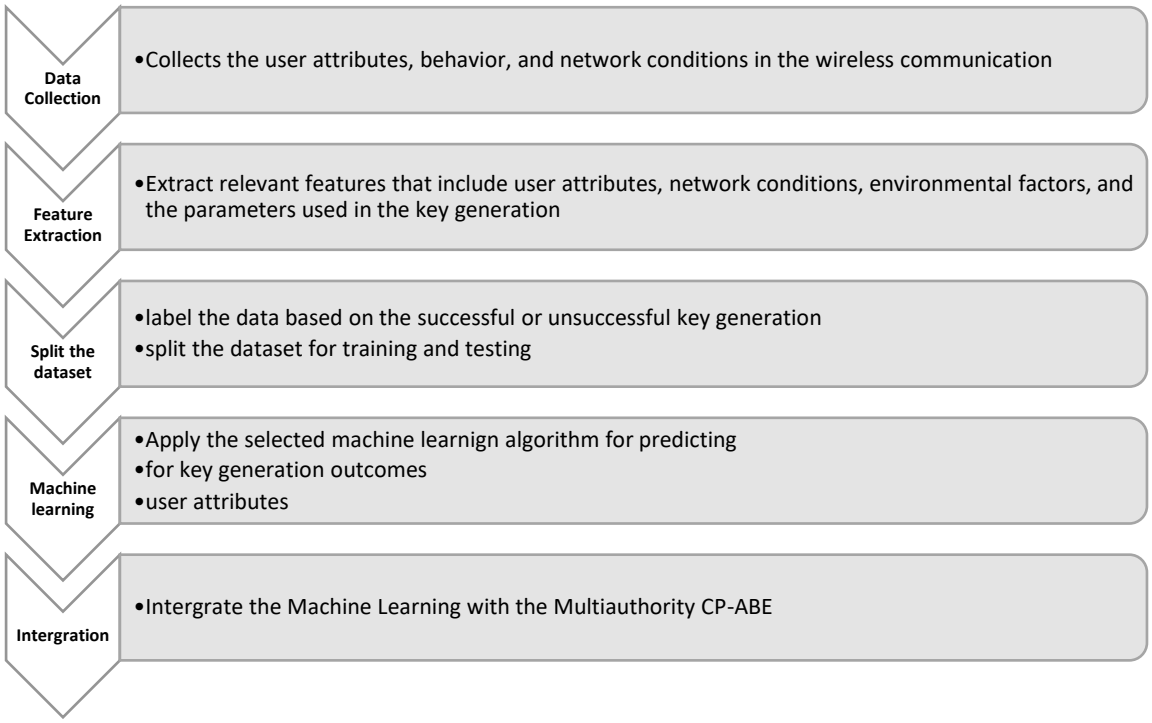

Figure 2. General Work Flow of ML with multiauthority CP-ABE

5. Future Progress

Further we would like to proceed with the implementation of the suggested model, but before going with the implementation, a comparative analysis of different supervised machine learning methods combination with the multiauthority CP-ABE is likely to be performed to identify the best methods that are suitable with the process of encrypting. Further in the future work the selection of the appropriate machine learning that are to be combined with the multiauthority CP-ABE and the criteria for selecting the ML models, its working in prediction of key generation outcomes, user attributes, detection of abnormal behaviours will be discussed clearly with the Implementation of Multiauthority-CP-ABE for generating cryptographic keys based on predicted attributes and contextual information provided by ML models.

6. Conclusion

In wireless networks, maintaining privacy in wireless channels is essential for communication security—especially when physical layer security is taken into account. A thorough encryption strategy becomes essential when the wireless landscape changes due to a variety of devices, dynamic user behaviors, and evolving security risks. In order to improve security and adaptability, this survey studies encryption techniques of the physical layer and suggests an Multi-authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE) and its combination with Machine Learning (ML) to address the challenges posed by the evolving wireless landscape while ensuring robust security and user privacy. The future work of the research would proceed with the implementation of the suggested method.

References

[1] X. Liu, H. Zhai, Y. Shen, B. Lou, C. Jiang, T. Li, S. B. Hussain, and G. Shen, ‘‘A Practical Method to Achieve Perfect Secrecy: Encryption Wireless Communication on the Fly Using One Time Pad and Key Generation,’’ IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 13, no. 13, pp. 414–427, 2020.

[2] Y. T. Solano-Correa, F. Bovolo, L. Bruzzone, and D. Fernandez-Prieto, ‘‘OTP Encrypted Data Transmission: Random Shifting Intelligent Reflecting Surface,’’ IEEE Transactions on Geoscience and Remote Sensing, vol. 58, no. 3, pp. 2150–2164, Mar. 2020.

[3] Y. J. E. Gbodjo, D. Ienco, and L. Leroux, ‘‘Creating a Perfectly Secure Data Transmission Channel Between Unmanned Aerial Vehicle and Ground Control Station Based on One-Time Pads: A Method,’’ IEEE Geoscience and Remote Sensing Letters, vol. 7, no. 2, pp. 307–311, Feb. 2020.

[4] S. D. Fabiyi, H. Vu, C. Tachtatzis, P. Murray, D. Harle, T. K. Dao, I. Andonovic, J. Ren, and S. Marshall, ‘‘Constructive or Destructive? Reconfigurable Intelligent Surface for Physical Layer Key Generation,’’ IEEE Access, vol. 8, pp. 22493–22505, 2020.

[5] Z. Li, G. Chen, and T. Zhang, ‘‘Highly Secured Hybrid Image Steganography with an Improved Key Generation and Exchange for One-Time-Pad Encryption Method,’’ IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 13, no. 13, pp. 847–858, 2020.

[6] Li, Jin, Qiong Huang, Xiaofeng Chen, Sherman SM Chow, Duncan S. Wong, and Dongqing Xie. "Multi-authority ciphertext-policy attribute-based encryption with accountability." In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 386-390. 2011.

[7] Muller, Sascha, Stefan Katzenbeisser, and Claudia Eckert. "On multi-authority ciphertext-policy attribute-based encryption." Bulletin of the Korean Mathematical Society 46, no. 4 (2009): 803-819.

[8] Ancy, P. R., and Addapalli VN Krishna. "Machine Learning Techniques for Resource-Constrained Devices in IoT Applications with CP-ABE Scheme." In Congress on Intelligent Systems, pp. 557-566. Singapore: Springer Nature Singapore, 2022.

[9] Zhou, Xianfei, Kai Xu, Naiyu Wang, Jianlin Jiao, Ning Dong, Meng Han, and Hao Xu. "A secure and privacy-preserving machine learning model sharing scheme for edge-enabled IoT." IEEE Access 9 (2021): 17256-17265.

[10] Kurniawan, Agus, and Marcel Kyas. "Securing machine learning engines in IoT applications with attribute-based encryption." In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 30-34. IEEE, 2019.

[11] Baba, K. Sai, A. Sandeep Kumar, and B. Tarakeswara Rao. "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks." International Journal of Computer Applications 132, no. 17 (2015).

[12] Porwal, Shardha, and Sangeeta Mittal. "Implementation of Ciphertext Policy-Attribute Based Encryption (CP-ABE) for fine grained access control of university data." In 2017 Tenth international conference on contemporary computing (IC3), pp. 1-7. IEEE, 2017.