Cross-Layer Authentication and Physical Layer Authentication in Internet-of-Things: A Systematic Literature Review

Mahsa Mohaghegh
School of Engineering, Computer, and Mathematical Sciences
Auckland University of Technology
Auckland, New Zealand
Email: mahsa.mohaghegh@aut.ac.nz

Vicky Ngo
School of Engineering, Computer, and Mathematical Sciences
Auckland University of Technology
Auckland, New Zealand
Email: vicky.ngo@autuni.ac.nz

***Abstract*—This research presents a comprehensive analysis of physical layer and cross-layer authentication schemes in the context of the Internet of Things (IoT) through a systematic literature review. The study evaluates the methods, as well as strengths and weaknesses of existing techniques in defending against prominent security threats, including eavesdropping, impersonation, and brute-force attacks. The findings underscore the challenges faced by physical layer authentication due to variations in features, rendering it unreliable despite its ability to offer enhanced security with minimal computational resources. In contrast, the integration of physical layer techniques into cross-layer authentication methods demonstrates promising results in mitigating these challenges. Despite such integration being one of the most common approaches to cross-layer authentication, we also evaluate other approaches that does not involve physical-layer authentication. There is also an emphasis on the fact that although hypothesis testing yields optimistic outcomes, assessing the impact on communication network latency, delay, and overhead in actual testbeds is essential.**

***Index Terms*—authentication, cross-layer, physical layer, Internet-of-Things**

I. Introduction

One of the key aspects of IoT security is authentication, a process that verifies the identity of devices, users, and nodes within the network [1]. Many IoT devices do not have sufficient resources for traditional cryptographic authentication schemes, which were designed for main-powered, high-processing and/or large memory devices. This highlights the importance of lightweight authentication schemes for IoT with low computational requirements while still maintaining high security [2]. Additionally, because IoT networks vary greatly based on their usage, authentication schemes should also be compatible across different network types.

Physical layer authentication and cross-layer authentication schemes have been found to provide high security while maintaining low latency in the communication network, which is an important feature for IoT. Physical layer authentication utilises the physical characteristics of the devices, which given their uniqueness should be sufficient for identifying legitimate and malicious devices [3]. Because such features are difficult to imitate, physical layer authentication can provide effective authentication with minimal computational resources required.

Meanwhile, cross-layer authentication refers to the usage of different authentication elements at different layers. For example, it is possible to combine authentication elements from the physical layer with those from the application layer, or traditional cryptographic techniques. Because cross-layer authentication is slightly more resource-demanding than physical layer authentication, there is also a need to address this demand without impeding network latency and communication.

However, a significant relationship exists between physical layer authentication and cross-layer authentication. Therefore, conducting a comprehensive literature review encompassing current authentication schemes within both these approaches would be highly advantageous. To the best of our knowledge, this is the first literature review to cover both physical layer authentication and cross-layer authentication, as well as the relationship between the two approaches. The contributions of our research are as follows:

- Provide a systematic literature review of existing authentication schemes and their techniques within both physical layer and cross-layer authentication approaches.
- Identify the techniques' strengths in authentication and abilities to defend against attacks such as eavesdropping, impersonation, and brute-force.
- Discusses the relationship between physical layer authentication and cross-layer authentication, as well as the need for evaluation of such schemes in actual testbeds to better understand the impacts on communication latency and authentication performance, aside from hypothesis testing.

This study is structured as follows. Section II introduces the systematic literature review method. Section III and Section IV present the existing techniques in physical layer authentication and cross-layer authentication respectively. Finally, Section V discusses our findings, while Section VI presents our conclu-

sion.

II. Methodology

A systematic literature review (SLR) is conducted to review existing research on physical-layer authentication and cross-layer authentication since 2013. Our SLR seek to answer the following research questions:

- RQ1: What are the current approaches to physical-layer authentication and cross-layer authentication in Internet-of-Things?
- RQ2: What are the advantages and disadvantages of using physical-layer authentication versus using cross-layer authentication?
- RQ3: In which use cases should one approach be preferred over another?

A. Search Process

Our search engines include ACM Digital Library, IEEE, ScienceDirect, in addition to Scopus and Springer. Additionally, we then conduct a secondary search in Google Scholar to ensure that as many relevant papers have been included. An example of our search string is:
(cross-layer OR physical layer) AND (authentication).

B. Inclusion & Exclusion Criteria

We included research on either cross-layer authentication or physical-layer authentication for IoT between 2013 and 2023 inclusive. The authentication techniques, evaluation criteria, results, as well as use cases, were then examined. Papers that are not relevant to the topic of cross-layer or physical layer authentication are excluded, such as research on protocols or cross-layer designs. Additionally, we exclude demo abstract papers as such papers are too short to provide sufficient information on the respective authentication schemes, which makes it difficult to evaluate.

III. Physical Layer Authentication in IoT

A physical layer authentication scheme can be understood as a receiver authenticating the transmitter based on the physical features of the signals. Because physical features are more difficult to impersonate or clone, this approach can effectively discern between benign and malicious nodes. Most importantly, physical layer authentication would also create the opportunity to construct a two-factor authentication system, where authentication mechanisms could exist at both the physical layers and those at upper layers [3].

Compared to conventional cryptographic approaches which require heavy computation, physical layer authentication schemes in IoT allow faster and more lightweight authentication while having low complexity, latency, and computation [4], [5]. These characteristics make physical layer authentication more suitable for edge devices with low computational power. On another hand, physical layer authentication may have low authentication reliability due to feature variation and environmental factors such as noise.

Table I present physical layer authentication techniques in IoT. Physical layer authentication is typically classified into two types: Transmitter-based and channel-based authentication [6]. Note that the transmitter-based approach identifies legitimate and malicious transmitters through fingerprinting, while channel-based authentication uses inherently unique channel characteristics.

A. Transmitter-based Authentication Techniques

The transmitter-based physical layer authentication mainly identifies a transmitter by analyzing captured radio frequency as fingerprint features [5], [6]. We have found most transmitter-based authentication techniques to involve fingerprint embedding. Particularly, [7] generated authentication sequence to watermark preamble chips for authentication in IoT. [3] proposed three different authentication schemes (PLA-SIT, PLA-SAT, PLA-TDM) based on different ways in which signals can be tagged using either shared or unique authentication tags. The study found that for non-orthogonal multiple access systems, the PLA-SAT approach is best assuming no colluded users and ignoring authentication accuracy fairness. Otherwise, the PLA-SIT approach is best. Finally, [12] considers the generation of a unique PHY-ID for cross-layer authentication, in addition to a PHY-IBC-based key protection for an end-to-end communication system.

B. Channel-based Authentication Techniques

Communication channels between transmitters and receivers in different places possess different channel characteristics, such as space-variability, uniqueness, time-variation, and reciprocity. These unique channel characteristics can be used to identify legitimate and illegal nodes. Examples of such characteristics are received signal strength (RSS), channel impulse response (CIR), channel state information (CSI), and channel frequency response (CFR) [5]. However, other physical layer signatures could still be used for authentication.

[8] creates physical layer signature through spatially and temporally correlated channel attributes within the coherence time interval. This signature can be used as a message authentication code to prove the packet's authenticity. [11] utilise transmitter-specific frequency offset estimation for authentication, however, the false alarm and detection probabilities of the proposed authentication scheme were only derived analytically based on the theories of statistical signal processing, and composite hypothesis testing. [4] proposes a deep learning-based multi-user authentication scheme which uses channel state information to detect spoofing attacks in wireless networks. Meanwhile, [13] protects authentication responses generated by AKA with physical layer authentication using a fault-tolerant hash method.

IV. Cross-Layer Authentication in IoT

Cross-layer authentication scheme can be understood as authentication spanning across two or more layers. As many schemes involve adding additional authentication on top of physical layer authentications, cross-layer authentication can also be said to be an improvement of physical layer authentications.

TABLE I
PHYSICAL LAYER AUTHENTICATION TECHNIQUES IN IOT

Scheme	Year	Approach	Method	Strengths
[7]	2023	Transmitter-based	Watermarking preamble chips with generated authentication sequence in replace of partial pseudorandom noise code chips.	Improved frame detection rate and successful rate.
[8]	2022	Channel-based	Using physical layer signature as a message authentication code to ensure authenticity.	Support high packet authentication detection probability at small signal-to-noise ratios.
[9]	2022	Channel-based	Using trusted third party known as a server (anonymizer) to authenticate the transmitter and receiver by incorporating different physical layer security.	Improves privacy of transmitted messages.
[10]	2021	Channel-based	Using channel amplitude for authentication	Probabilities of transmission, security outage, connection outage, joint security-connection outage
[6]	2020	Channel-based	Authentication technique based on the uncloneable wireless channel characteristics for handover authentication scenario.	Authentication accuracy
[3]	2020	Transmitter-based	Proposed three authentication schemes using authentication tags for non-orthogonal multiple access systems.	Authentication accuracy, reliability
[11]	2020	Channel-based	Use maximum likelihood estimator to obtain frequency offset estimation. The authentication scheme is based on the transmitter-specific frequency offset and false alarm and detection probabilities	Authentication accuracy.
[4]	2019	Channel-based	Deep learning based multi-user authentication scheme which can also discriminate legitimate and malicious nodes, and attackers for MEC system.	Authentication rate
[12]	2018	Transmitter based	Integrate PHY-ID with existing, well-established asymmetric cryptography-based authentication schemes with novel PHY-IBC-based key protection schemes.	Authentication performance, resistance to the upper-layer computation-based impersonation attacks
[13]	2017	Channel-based	Responses generated by Authentication and Key Agreement (AKA) protocol is used as a key for physical layer authentication	Lower false alarm rate and missing rate, less communication overhead, improving communication efficiency.

The PHY-AUTH column in Table II refers to whether the cross-layer authentication scheme also involves physical layer authentication. Particularly, we have found that many cross-layer authentication schemes involve adding upper-layer authentications or cryptographic techniques before or after physical layer authentication. Note that in a dynamic environment, physical layer authentication has unreliable performance [15]. Furthermore, due to feature variation and environmental factors such as noises, physical layer authentication may not guarantee robust authentication reliability either [19]. Although physical layer authentication can provide low computational overhead and low time latency, having additional layers for authentication on top would allow for higher authentication accuracy, and thus security, meanwhile maintaining low computational overhead and latency. This balance is an important benefit of cross-layer authentication, which has been a priority in current research in this area.

As for the approaches that do not directly involve physical layer authentication, we found that [17] had proposed an authentication scheme where only necessary attributes are selected for authentication, thus reducing latency. Meanwhile, [22] employs the radio trusted zone database concept to reduce authentication recurrence, however, it does not elaborate on how such a system can be built. Instead, the study assumes the existence of the trusted database as part of their analysis. [25] monitor physical characteristics, namely packet error rate and received signal strength indicator, to make authentication decisions. [26] utilises an ID-based authentication scheme with anonymous signature generation for authentication, however, it has also been discovered to be vulnerable to private key reveal attack [27], [28]. Particularly, the private key could be recovered just by eavesdropping. [27] proposed an improvement on this authentication scheme.

Additionally, the usage of cross-layer authentication has also allowed for the defence of attacks such as eavesdropping, impersonation, brute-force, and traceability attacks. We also found that most cross-layer authentication schemes are validated through hypothesis testing, where attributes such as authentication probabilities are analytically derived. On top of hypothesis testing, some research also used a simulation or testbed to evaluate their proposed authentication schemes.

V. DISCUSSION

Our literature review described the current research into physical layer authentication and cross-layer authentication in the past 10 years. Particularly, we summarise the advantages and disadvantages of the two approaches in Table III.

Through our literature review, we found cross-layer authentication to be superior to physical layer authentication. While physical layer authentication can either use unique physical characteristics or embedding authorisation code to ensure security of devices, cross-layer authentication can improve authentication performance by adding upper-level authentication and/or challenge-response-based mechanisms. This usually involves cryptographic authentication and key agreement (AKA) mechanisms. Due to the higher level of computational resources required for upper-level authentication and cryptographic schemes, these authentication schemes

TABLE II
CROSS-LAYER AUTHENTICATION TECHNIQUES IN IOT

Scheme	Year	PHY-AUTH?	Method	Strengths
[14]	2023	Yes	Upper-layer authentication followed by physical layer challenge-response for re-authentication.	Reduce overall complexity, computation, and communication overheads
[15]	2022	Yes	Situationally-aware switch module switches between physical layer authentication and cryptographic AKA to ensure communication performance	Improved reliability, switch method based on situational awareness & real-time performance evaluation.
[16]	2022	Yes	Cross-layer framework to authenticate preambles in initial access.	Reliable against attacks and eavesdropping.
[17]	2022	No	Use LDA to fuse authentication decisions by projecting high dimensional estimations to low dimension, thus keeping only necessary attributes for authentication	Reducing time required for attribute estimation and overhead of authentication. Lower latency and higher security.
[18]	2020	Yes	Use multiple physical layer attributes for authentication and involve upper-layer authentication only when attackers are detected.	Higher authentication accuracy. Suitable for dynamic communication scenarios.
[19]	2020	Yes	Physical layer authentication results are divided into rejected, authenticated, and ambiguous. Cryptographic checks are further performed on ambiguous results.	Defend against eavesdropping, impersonation, signal replay, brute force, and traceability attacks.
[20]	2020	Yes	Proposed Tagora, which combines physical layer authentication with a cryptographic system on the application layer	Tagora is lightweight and secure. Defend against eavesdropping attacks.
[21]	2019	Yes	Embedding authorisation code into packets for authentication. Authorization code changes over time.	Even if attackers eavesdrop on the current authorisation code, they can't deduce the next code.
[22]	2018	No	Radio trusted zone database concept is introduced to reduce the authentication recurrence.	Tested against redirection and black hole attacks, replay attacks, MITM, impersonation, DoS.
[23]	2018	Yes	Physical cross-verification tool that integrates conventional PKI-based authentication with available physical layer information.	Enhances the existing PKI-based authentication against location spoofing attacks.
[24]	2016	Yes	Integrate physical layer authentication and cryptographic schemes with physical and composite keys generation.	Defend against brute-search attacks
[25]	2013	No	Monitor and analyse packet error rate (PER) and the received signal strength indicator (RSSI) in IEEE 802.11 networks	Improved spoofing detecting capability over the single variable-based authentication.
[26]	2013	No	Generate anonymous signature generation and verification using parameters such as the current position of the signer and individual receiver.	Allows safety message authentication according to the relevance score of received messages in the individual access category.

TABLE III
ADVANTAGES AND DISADVANTAGES OF PHYSICAL LAYER AND CROSS-LAYER AUTHENTICATION SCHEMES

	Physical Layer	Cross-Layer
Advantages	Low complexity, power consumption, overhead, suitable for edge devices.	Higher authentication accuracy while reducing low latency and overhead. Foster defence against eavesdropping attacks
Disadvantages	Lack of reliability due to noises and feature variance	Involvement of upper-layer authentication and cryptographic elements may affect latency and device performance.

are only performed, typically on the server side, when physical layer authentication is insufficient. Additionally, certain studies have also utilised artificial intelligence as an authentication model for the proposed schemes.

On another hand, we have noticed that the authentication schemes proposed use both physical layer and cross-layer approach to only target a certain type of IoT network. We have yet to find research that evaluates such authentication schemes across different but similar IoT networks. Additionally, some authentication schemes were only evaluated analytically through hypothesis testing, which means that they were only confirmed to be effective in theories. However, it is still imperative that the schemes were deployed and evaluated on an actual testbed, as it would allow for observations of actual authentication performances and communication latency.

VI. CONCLUSION

We performed a systematic literature review of existing cross-layer and physical layer authentication schemes in IoT. We found that although physical layer authentication is able to provide better security with minimal computational power required, it is still unreliable due to feature variation. On another hand, cross-layer authentication techniques that integrate physical layer authentication techniques with upper-level or cryptographic authentication were found to be capable of remediating this issue. Despite the promising results shown in hypothesis testing of the authentication schemes, it is imperative that such authentication schemes are evaluated in a real testbed in order to observe the impacts that such authentication schemes have on communication network latency, delay, and overhead, which are all critical elements in IoT. Future work on this study could investigate the usage of proposed authentication schemes across different network types. Another research direction would be to analyse the impact of using artificial intelligence in cross-layer authentication schemes in

IoT, and whether it could be used to improve authentication performance and efficiency.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128610001568

[2] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (iot) authentication schemes," *Sensors*, vol. 19, no. 5, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/5/1141

[3] N. Xie, S. Zhang, and A. X. Liu, "Physical-layer authentication in non-orthogonal multiple access systems," *IEEE/ACM Transactions on Networking*, vol. 28, no. 3, pp. 1144–1157, 2020.

[4] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, H. Song, F. Xie, Y. Jiang, and M. Cao, "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, pp. 116 390–116 401, 2019.

[5] L. Alhoraibi, D. Alghazzawi, R. Alhebshi, and O. B. J. Rabie, "Physical layer authentication in wireless networks-based machine learning approaches," *Sensors*, vol. 23, no. 4, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/1814

[6] T. Ma, F. Hu, and M. Ma, "Securing 5g hetnets using mutual physical layer authentication," in *Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City*, ser. ICIT '19. New York, NY, USA: Association for Computing Machinery, 2020, p. 275–278. [Online]. Available: https://doi.org/10.1145/3377170.3377183

[7] Y. Leng, R. Zhang, W. Wen, P. Wu, and M. Xia, "Physical-layer authentication with watermarked preamble for internet of things," in *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2023, pp. 212–217.

[8] M. A. Shawky, Q. H. Abbasi, M. A. Imran, S. Ansari, and A. Taha, "Cross-layer authentication based on physical-layer signatures for secure vehicular communication," in *2022 IEEE Intelligent Vehicles Symposium (IV)*, 2022, pp. 1315–1320.

[9] K. Nagamani and R. Monisha, "Physical layer security using cross layer authentication for aes-ecdsa algorithm," *Procedia Computer Science*, vol. 215, pp. 380–392, 2022, 4th International Conference on Innovative Data Communication Technology and Application. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050922021111

[10] N. Xie, H. Tan, L. Huang, and A. X. Liu, "Physical-layer authentication in wirelessly powered communication networks," *IEEE/ACM Transactions on Networking*, vol. 29, no. 4, pp. 1827–1840, 2021.

[11] P. Zhang, G. Zhao, and L. Ma, "Phy-layer authentication for iot devices using frequency offset feature," in *Proceedings of the 1st International Workshop on Physical-Layer Augmented Security for Sensor Systems*, ser. PLAS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 22–25. [Online]. Available: https://doi.org/10.1145/3417311.3430707

[12] P. Hao, X. Wang, and W. Shen, "A collaborative phy-aided technique for end-to-end iot device authentication," *IEEE Access*, vol. 6, pp. 42 279–42 293, 2018.

[13] J. Yang, X. Ji, K. Huang, M. Yi, and Y. C. and, "Aka-pla: Enhanced aka based on physical layer authentication," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 7, pp. 3747–3765, July 2017.

[14] M. A. Shawky, M. Bottarelli, G. Epiphaniou, and P. Karadimas, "An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 7, pp. 8738–8754, 2023.

[15] H. Fang, X. Wang, and W. Zhu, "Intelligent integrated cross-layer authentication for efficient mutual verification in udn with guaranteed security-of-service," in *2022 IEEE Future Networks World Forum (FNWF)*, 2022, pp. 385–390.

[16] D. Xu, K. Yu, and J. A. Ritcey, "Cross-layer device authentication with quantum encryption for 5g enabled iiot in industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6368–6378, 2022.

[17] H. Wang, H. Fang, and X. Wang, "Safeguarding cluster heads in uav swarm using edge intelligence: Linear discriminant analysis-based cross-layer authentication," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1298–1309, 2021.

[18] Z. Zhang, N. Li, S. Xia, and X. Tao, "Fast cross layer authentication scheme for dynamic wireless network," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, 2020, pp. 1–6.

[19] Y. Lee, J. Yoon, J. Choi, and E. Hwang, "A novel cross-layer authentication protocol for the internet of things," *IEEE Access*, vol. 8, pp. 196 135–196 150, 2020.

[20] H. Park, H. Roh, and W. Lee, "Tagora: A collision-exploitative rfid authentication protocol based on cross-layer approach," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3571–3585, 2020.

[21] S. Yu, X. Zhang, P. Huang, and L. Guo, "Secure authentication in cross-technology communication for heterogeneous iot," in *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2019, pp. 1–2.

[22] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-layer authentication protocol design for ultra-dense 5g hetnets," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[23] A. Abdelaziz, C. Emre Koksal, R. Burton, F. Barickman, J. Martin, J. Weston, and K. Woodruff, "Beyond pki: Enhanced authentication in vehicular networks via mimo," in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2018, pp. 1–5.

[24] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152–158, 2016.

[25] P. Hao, X. Wang, and A. Refaey, "An enhanced cross-layer authentication mechanism for wireless communications based on per and rssi," in *2013 13th Canadian Workshop on Information Theory*, 2013, pp. 44–48.

[26] S. Biswas and J. Mišić, "A cross-layer approach to privacy-preserving authentication in wave-enabled vanets," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, 2013.

[27] J.-L. Tsai, "An improved cross-layer privacy-preserving authentication in wave-enabled vanets," *IEEE Communications Letters*, vol. 18, no. 11, pp. 1931–1934, 2014.

[28] K.-A. Shim, "Comments on "a cross-layer approach to privacy-preserving authentication in wave-enabled vanets" by biswas and mišić," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 588–10 589, 2017.