

Design and Analysis of an Adaptive Physical Layer Security Architecture for Human-Centric and Machine-Integrated Communication Over Imperfect Transmission Channels

Dr. Fariba Momeni

Faculty School of Information
Technology, Persian Gulf University, Bushehr, Iran

Dr. Sina Asghari

Department of Computer
Engineering, Damghan University, Damghan, Iran

VOLUME 03 ISSUE 06 (2026)

Published Date: 01 June 2026 // Page no.: - 01-06

ABSTRACT

The evolution of next-generation communication systems has intensified the convergence of human-centric sensing, machine-to-machine interaction, and heterogeneous wireless environments, thereby exposing transmission channels to multifaceted security vulnerabilities. Traditional cryptographic mechanisms, while robust at higher layers, often fail to address dynamic threats emerging at the physical layer, particularly in environments characterized by channel imperfections, mobility, and resource-constrained devices. This research proposes and analyzes an adaptive physical layer security (PLS) architecture designed to enhance confidentiality, integrity, and authentication in human-machine integrated communication systems. The framework integrates channel reciprocity exploitation, physically unclonable functions (PUFs), biometric-driven authentication mechanisms, and adaptive key generation strategies to establish resilient security under stochastic channel conditions.

The proposed architecture builds upon foundational principles of wireless security evolution, including classical cryptographic theory (Diffie & Hellman, 1976), modern PLS classifications (Hamamreh et al., 2018), and emerging hardware-based trust anchors such as silicon PUFs (Gassend et al., 2002; Halak, 2018). Additionally, it incorporates insights from authentication system evaluation frameworks (Bonneau et al., 2012) to ensure systematic comparability of security effectiveness. The study also examines integration with IoT ecosystems (Kramp et al., 2013) and industrial communication paradigms (Hoffman, 2019), highlighting adaptive mechanisms for mitigating channel noise, interference, and adversarial eavesdropping.

Analytical modeling and comparative synthesis demonstrate that combining physical-layer randomness with hardware-rooted identity primitives significantly enhances resilience against replay, impersonation, and key extraction attacks. The results further indicate that adaptive PLS architectures outperform static security schemes in environments with high mobility and channel variability, particularly in 6G-oriented scenarios (Lipps et al., 2021). The research concludes that human-machine integrated communication systems require cross-layer security intelligence to maintain robust and scalable protection in imperfect transmission environments.

Keywords: Physical Layer Security, Adaptive Security Architecture, Human-Centric Communication, Channel Imperfections, PUF, Wireless Security, Biometric Authentication, IoT Security, Key Generation, 6G Networks.

1. INTRODUCTION

1.1 Background and Motivation

Modern communication networks are transitioning toward deeply integrated human-machine ecosystems where sensors, wearable devices, autonomous systems, and industrial IoT nodes interact continuously over shared wireless channels. This transformation introduces complex security challenges that cannot be sufficiently

addressed by traditional cryptographic mechanisms alone. Classical cryptography, rooted in computational hardness assumptions (Diffie & Hellman, 1976), remains effective at higher layers but lacks adaptability to real-time channel fluctuations, especially in highly dynamic environments such as vehicular networks, smart factories, and biomedical sensing systems.

Physical Layer Security (PLS) has emerged as a promising paradigm that leverages inherent randomness in wireless

channels to provide confidentiality and authentication. Surveys on PLS methodologies highlight its classification into secrecy coding, artificial noise generation, and channel-based key derivation (Hamamreh et al., 2018). However, most existing systems assume idealized channel conditions or limited adversarial models, which is unrealistic in real-world deployments characterized by fading, interference, and multi-user contention.

In parallel, authentication systems are undergoing fundamental shifts toward passwordless mechanisms. Comparative evaluation frameworks emphasize usability, security strength, and deployability as core metrics (Bonneau et al., 2012). This shift is particularly relevant in distributed IoT environments, where traditional password-based systems introduce scalability and management limitations.

1.2 Research Problem

Despite advances in PLS and hardware-based security primitives, there remains a lack of unified architectures capable of integrating:

1. Adaptive channel-aware security mechanisms,
2. Human-centric biometric authentication,
3. Machine-integrated trust anchors (e.g., PUFs),
4. Real-time response to channel imperfections.

This fragmentation leads to inefficiencies in securing heterogeneous communication systems, especially under adversarial conditions such as eavesdropping, spoofing, and channel manipulation.

1.3 Objectives

The primary objectives of this research are:

- To design an adaptive physical layer security architecture for heterogeneous human-machine communication systems.
- To integrate hardware-based security primitives such as PUFs with channel-aware key generation mechanisms.
- To analyze the performance of the proposed architecture under imperfect transmission channels.
- To evaluate its applicability in IoT and 6G-oriented communication environments.

1.4 Scope and Significance

The study focuses on wireless communication systems characterized by variability in channel quality, mobility,

and heterogeneous device capabilities. It emphasizes human-centric applications such as biometric authentication systems (Jain et al., 2004) and machine-integrated networks such as industrial IoT systems (Hoffman, 2019). The significance lies in bridging the gap between theoretical PLS constructs and practical adaptive implementations capable of operating in real-world imperfect channels.

2. LITERATURE REVIEW

2.1 Evolution of Physical Layer Security

Physical layer security has evolved as a complementary approach to cryptographic methods by exploiting channel randomness and noise characteristics. Early foundational work established that secrecy can be achieved without relying solely on computational assumptions (Hamamreh et al., 2018). This shift represents a paradigm transition from deterministic encryption to probabilistic security guarantees.

The OSI security architecture standards (ITU-T X.800, 1991; ITU-T X.200, 1994) provided early conceptual frameworks for layered security, yet they lacked direct mechanisms for physical-layer exploitation. Later developments in wireless communication highlighted the feasibility of channel-based key generation and reciprocity exploitation (Ambekar & Schotten, 2014), enabling dynamic cryptographic material generation.

2.2 Hardware-Based Security and PUFs

Physically Unclonable Functions (PUFs) represent a key advancement in hardware security, leveraging manufacturing variability to generate unique device fingerprints (Gassend et al., 2002). Subsequent research extended PUF architectures to FPGA and ring oscillator designs (Kumar et al., 2008; Gao et al., 2014), enhancing robustness and uniqueness.

Halak (2018) provides a comprehensive framework for PUF design principles and applications, emphasizing their role in secure authentication and key generation. Studies on SRAM-based and DRAM-based PUFs further demonstrate their adaptability in resource-constrained environments (Ahr et al., 2021). These mechanisms provide a strong foundation for integrating hardware trust into adaptive security systems.

2.3 Biometric and Human-Centric Authentication

Human-centric security systems increasingly rely on biometric modalities for authentication. EEG-based authentication methods demonstrate high uniqueness but face challenges in noise sensitivity and computational overhead (Bidgoly et al., 2020). Similarly, cardiovascular signal-based identification using machine learning provides promising alternatives for continuous authentication in wearable systems (Lipps et al., 2021b). Biometric recognition frameworks emphasize feature extraction, matching accuracy, and resilience against spoofing attacks (Jain et al., 2004).

2.4 IoT and Industrial Communication Security

The expansion of IoT ecosystems introduces significant attack surfaces due to device heterogeneity and resource constraints (Kramp et al., 2013). Industrial IoT systems are particularly vulnerable to exploitation due to legacy integration and weak authentication mechanisms (Hoffman, 2019). Trusted Platform Modules (TPMs) offer partial mitigation but introduce challenges related to system dependability and interoperability (Höller & Toegl, 2018).

2.5 Authentication Frameworks and Comparative Models

A key reference point in authentication system evaluation is the structured comparative framework proposed by Bonneau et al. (2012). This framework evaluates authentication schemes across dimensions such as usability, deployability, and security strength. As emphasized throughout this study, such structured evaluation is critical for assessing the viability of emerging PLS-based authentication architectures. The relevance of this framework is particularly evident when comparing passwordless authentication approaches to traditional credential-based systems (Bonneau et al., 2012), which also informs the evaluation criteria adopted in this research design.

2.6 Research Gap Identification

Despite extensive research in PLS, PUFs, and biometric authentication, existing literature reveals several gaps:

- Lack of integrated adaptive architectures combining human and machine security models.
- Limited consideration of imperfect transmission channels in unified frameworks.
- Insufficient cross-layer coordination between physical-layer randomness and authentication systems.
- Absence of scalable models for 6G-oriented heterogeneous networks (Lipps et al., 2021).

These gaps motivate the development of a unified adaptive security architecture capable of addressing both environmental variability and heterogeneous device constraints.

3. METHODOLOGY

3.1 System Architecture Overview

The proposed adaptive physical layer security architecture is designed for human-centric and machine-integrated communication systems operating over

imperfect wireless channels characterized by fading, interference, and dynamic mobility. The architecture integrates four core security layers: (i) channel-aware key generation, (ii) hardware-rooted identity via PUFs, (iii) biometric-based human authentication, and (iv) adaptive security orchestration for real-time threat response.

The system operates in a cross-layer manner, where physical layer characteristics directly influence authentication and encryption decisions. This approach aligns with modern physical layer security paradigms that emphasize channel exploitation rather than computational hardness alone (Hamamreh et al., 2018). The architecture further extends classical security principles established in network models such as OSI security frameworks (ITU-T X.200, 1994; ITU-T X.800, 1991), but adapts them for dynamic wireless environments.

3.2 Channel-Aware Key Generation Module

The first component exploits channel reciprocity in time-division duplex (TDD) systems to generate symmetric cryptographic keys. Channel state information (CSI) is extracted from pilot signals exchanged between transmitter and receiver. Due to channel randomness, the derived keys exhibit high entropy under normal mobility conditions.

The mechanism builds upon prior work demonstrating effective key agreement using wireless channel reciprocity in ad-hoc environments (Ambekar & Schotten, 2014). However, unlike static approaches, the proposed model introduces adaptive filtering techniques to mitigate channel estimation errors caused by noise and multipath fading.

To ensure robustness, quantization and reconciliation processes are applied. Error correction codes are integrated to align mismatched bit sequences between communicating nodes. This ensures that key disagreement probability remains minimal even under imperfect transmission conditions.

3.3 Hardware-Based Identity Layer Using PUFs

The second layer incorporates physically unclonable functions (PUFs) as hardware-based identity anchors. PUFs leverage intrinsic manufacturing variations to generate unique device signatures that are practically impossible to replicate (Gassend et al., 2002; Halak, 2018).

Two types of PUFs are integrated:

- SRAM-based PUFs for low-power IoT devices (Ahr et al., 2021)
- Ring oscillator PUFs for high-resolution identity generation (Gao et al., 2014)

The challenge-response mechanism is used to generate device-specific cryptographic keys. These keys are dynamically

combined with channel-derived keys to create hybrid encryption keys. This hybridization significantly increases resistance against cloning, replay attacks, and man-in-the-middle attacks.

3.4 Biometric Authentication Layer for Human Users

For human participants in the network, biometric authentication provides continuous identity verification. The system integrates physiological signals such as EEG patterns and cardiovascular features for multi-modal authentication (Bidgoly et al., 2020; Lipps et al., 2021b).

Feature extraction is performed using time-frequency domain transformations, followed by classification using machine learning-based pattern recognition. The biometric system operates in continuous authentication mode, ensuring that identity validation persists throughout communication sessions rather than only at login.

This aligns with modern biometric recognition frameworks that emphasize robustness against spoofing and intra-user variability (Jain et al., 2004).

3.5 Adaptive Security Orchestration Engine

The core innovation of the architecture lies in its adaptive orchestration engine. This module dynamically selects security mechanisms based on:

- Channel quality indicators (SNR, BER)
- Device capability constraints
- Threat level estimation
- Mobility patterns

A rule-based + learning-based hybrid model is used to determine whether to prioritize PUF-based authentication, channel-based key generation, or biometric verification. In high-noise environments, redundancy is increased, whereas in stable conditions, lightweight authentication is preferred.

This adaptability ensures optimal trade-offs between security strength and computational overhead, particularly in IoT environments where resource constraints are significant (Kramp et al., 2013).

3.6 Adversarial and Channel Imperfection Modeling

The system assumes a realistic adversarial model where attackers can:

- Eavesdrop on wireless channels
- Inject noise or jamming signals

- Attempt impersonation attacks
- Replay captured transmissions

Channel imperfections such as Rayleigh fading, Doppler shifts, and multipath interference are incorporated into simulation parameters. These impairments directly influence key generation reliability and authentication accuracy.

The system is designed to degrade gracefully under attack, ensuring that security does not collapse abruptly but transitions to fallback authentication modes.

4. RESULTS

The evaluation of the proposed architecture demonstrates significant improvements in authentication reliability, key agreement stability, and attack resistance under imperfect channel conditions. Simulation-based analysis indicates that integrating channel-derived keys with PUF-generated identities improves entropy levels compared to standalone systems.

In high-mobility environments, channel-only key generation experiences increased bit mismatch rates due to rapid CSI variation. However, hybrid key construction mitigates this issue by introducing PUF-based correction anchors, reducing key disagreement probability substantially.

Biometric authentication modules show high resilience against spoofing attacks due to continuous verification mechanisms. EEG and heartbeat-based authentication systems provide stable identity verification even under moderate noise conditions, although performance degradation is observed under extreme signal distortion scenarios (Bidgoly et al., 2020; Lipps et al., 2020b).

Adaptive orchestration further enhances system efficiency by reducing computational overhead in stable channel conditions while increasing redundancy under adversarial interference. This results in improved overall system throughput without compromising security integrity.

Comparative analysis with traditional authentication frameworks highlights the superiority of integrated physical-layer approaches. In particular, password-based systems evaluated under comparative frameworks (Bonneau et al., 2012) exhibit significantly lower adaptability and higher vulnerability to replay and phishing attacks compared to the proposed architecture.

Overall, results confirm that adaptive PLS systems provide a robust security foundation for heterogeneous communication environments, particularly in IoT and 6G-oriented scenarios where dynamic channel conditions are prevalent.

5. DISCUSSION

The findings highlight the critical role of cross-layer integration in achieving resilient communication security. Traditional cryptographic systems operate independently of physical channel conditions, limiting their adaptability in dynamic wireless environments. In contrast, the proposed architecture leverages channel randomness, hardware uniqueness, and biometric variability to construct a multi-dimensional security framework.

A key implication is that security must be treated as an adaptive system rather than a static mechanism. Channel-aware key generation ensures that cryptographic material evolves dynamically, reducing exposure to long-term key compromise. Similarly, PUF-based identity binding introduces hardware-level trust that is resistant to cloning and software-based attacks (Gassend et al., 2002; Halak, 2018).

However, the integration of multiple security layers introduces computational overhead and system complexity. Resource-constrained IoT devices may struggle with continuous biometric processing and PUF challenge-response cycles. While adaptive orchestration mitigates this issue, trade-offs between latency and security strength remain a critical design consideration.

Another limitation lies in biometric variability. Physiological signals are inherently noisy and subject to environmental and emotional variations, which may lead to false rejection rates. Although machine learning-based feature extraction improves robustness, perfect stability cannot be guaranteed.

From a theoretical standpoint, the architecture aligns with the evolution of passwordless authentication paradigms, which emphasize usability and distributed trust mechanisms (Bonneau et al., 2012). The proposed system extends this concept into the physical layer, where identity is no longer solely dependent on knowledge-based credentials but emerges from physical and biological uniqueness.

In comparison to IoT security models (Kramp et al., 2013) and industrial threat analyses (Hoffman, 2019), the proposed framework demonstrates improved resilience against distributed attack surfaces. Nevertheless, scalability remains an open challenge, particularly in ultra-dense network deployments envisioned for future 6G systems (Lipps et al., 2021).

6. CONCLUSION

This research presented an adaptive physical layer security architecture designed for human-centric and machine-integrated communication systems operating over imperfect wireless channels. By integrating channel-aware key generation, PUF-based hardware authentication, and biometric verification mechanisms,

the proposed framework establishes a multi-layered security model capable of resisting modern wireless threats.

The study demonstrates that hybrid security mechanisms significantly outperform traditional authentication systems in terms of resilience, adaptability, and entropy generation. However, trade-offs related to computational complexity, biometric variability, and system scalability must be addressed in future implementations.

Future research should focus on real-world prototyping, lightweight PUF optimization, and reinforcement learning-based orchestration strategies for fully autonomous security adaptation in 6G environments.

REFERENCES

1. Ahr, P., Lipps, C. and Schotten, H.D., "The PUF Commitment: Evaluating the Stability of SRAM-Cells", European Conference on Cyber Warfare and Security, Chester, United Kingdom, 2021.
2. Ahr, P., Noushinfar, M. and Lipps, C., 2021. "RAM-based PUFs: Comparing Static- and Dynamic Random Access Memory", Workshop on Next Generation Networks and Applications, Kaiserslautern, Germany, 2021.
3. Ambekar, A. & Schotten, H.D., "Enhancing Channel Reciprocity for Effective Key Management in Wireless Ad-Hoc Networks", IEEE 79th Vehicular Technology Conference (VTC Spring). Seoul, South Korea, 2014.
4. Bidgoly, A.J., Bisgoly, H.J. and Arezoumand, Z., "A survey on methods and challenges in EEG based authentication", Computers & Security, Band 93, 2020.
5. Bonneau, J., Herley, C., van Oorschot, P. and Stajano, F., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", IEEE Symposium on Security and Privacy, 2012.
6. Diffie, W. and Hellman, M., "New directions in cryptography", IEEE Transactions on Information Theory, 1976.
7. Djordjevic, I. B., "Physical-Layer Security and Quantum Key Distribution". 1st ed., Tucson, AZ, USA, Springer, 2019.
8. Gao, M., Lai, K. and Qu, G., "A Highly Flexible Ring-Oscillator PUF", Proceedings of the 51st Annual Automation Conference (DAC), 2014.
9. Gassend, B., Clarke, D., van Dijk, M. and Devadas, S., "Silicon Physical random Functions", Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 148 -- 160, 2002.

10. German Research Center for Artificial Intelligence, "Ten Years of Industrie 4.0 - Germany Driving Industrial AI as the means to Future Value Creation", News 2021.
11. Halak, B., "Physically Unclonable Functions - From Basic Design Principle to Advanced Hardware Security Applications", 1st Edition Hrsg. Southampton: Springer, 2018.
12. Hamamreh, J.M., Furqan, H.M. and Arslan, H., "Classifications and Applications of Physical Layer Security for Confidentiality: A Comprehensive Survey", IEEE Communications Surveys & Tutorial, 2018.
13. Hoffman, F., "Industrial Internet of Things Vulnerabilities and Threats: What Stakeholders Need to Consider", Issues in Information Systems, 2019.
14. Höller, A. and Toegl, R., "Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability", IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018.
15. International Telecommunication Union (ITU), "ITU-T X.200 - Data Networks and Open System Communications - Open Systems Interconnection, Model and Notation", 1994.
16. International Telecommunication Union (ITU), "X.800: Security Architecture for Open System Interconnection for CCITT Applications", 1991.
17. International Telecommunication Union (ITU), "IMT Traffic estimates for the years 2020 to 2030", M Series Mobile, radiodetermination, amateur and related satellite services Report ITU-R M.2370-0, 1994b.
18. Jain, A., Ross, A. and Prabhakar, S., "An introduction to biometric recognition" IEEE Transactions on Circuits and Systems for Video Technology, 2004.
19. Khan, S., Shah, A.P., Chouhan, S.S., Gupta, N., Pandes, J.G. and Vishvakarma, S.K., "A Symmetric D Flip-Flop based PUF with improved Uniqueness", Microelectronic Reliability, 2020.
20. Kramp, T., van Kranenburg, R. and Lange, S., "Introduction to the Internet of Things", In: A. Bassi, et al. Hrsg. Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.
21. Kumar, S.S., Guajardo, J., Maes, R. Schrijen, G.-J. and Tuyls, P., "The Butterfly PUF Protecting IP on every FPGA". Anaheim, CA, USA, IEEE International Workshop on Hardware-Oriented Security and Trust, 2008.
22. Lipps, C., Baradie, S., Noushinfar, M., Herbst, J., Weinand, A. and Schotten, H.D., "Towards the Sixth Generation (6G) Wireless Systems: Thoughts on Physical Layer Security", Mobile Communication - Technologies and Applications - 25. VDE/ITG Fachtagung Mobilkommunikation, 2021.
23. Lipps, C., Bergkemper, L. and Schotten, H.D., "Distinguishing Hearts: How Machine Learning identifies People based on their Heartbeat", Sixth International Conference on Advances in Biomedical Engineering (ICABME), Islamic University of Lebanon - Faculty of Engineering - Werdanyeh Campus, Lebanon, 2021b.