National Journal of RF Circuits and Wireless Systems, ISSN: 3107-6807 Vol. 3, No. 2, 2026 (pp. 65-70)
RESEARCH ARTICLE
ECEJOURNALS.IN

Reciprocity-Driven Physical Layer Key Generation for Wireless Body Area Networks

Kagaba J. Bosco[1]*, Nisha Milind Shrirao[2]

[1]*Information and Communications Technology, National Institute of Statistics of Rwanda, Kigali, Rwanda*
[2]*Department Of Electrical And Electronics Engineering, Kalinga University, Raipur, India.*

KEYWORDS:
Physical Layer Security;
Key Generation;
Channel Reciprocity;
Wireless Body Area Networks (WBANs);
Wearable Devices;
On-Body Communication; Cryptographic Protocols;
Low-Power Security;
Healthcare IoT;
Eavesdropping Resistance

ARTICLE HISTORY:
Submitted : 17.09.2025
Revised : 16.10.2025
Accepted : 20.01.2026

https://doi.org/10.17051/NJRFCS/03.02.09

Abstract

This study proposes a lightweight, reciprocity-driven physical layer key generation scheme tailored for secure communication in Wireless Body Area Networks (WBANs). By harnessing the inherent randomness and temporal variation of on-body wireless channels, cryptographic keys are dynamically generated between wearable devices without reliance on pre-distributed secrets or computationally intensive algorithms. The protocol employs adaptive channel probing and quantization, followed by efficient error reconciliation and privacy amplification, ensuring strong key agreement even under mobility and diverse body movements. Experimental evaluations on a real WBAN testbed demonstrate high key generation rates, low bit mismatch, and resilience to passive eavesdropping, validating the scheme's suitability for resource-constrained, low-power healthcare wearables. The results highlight the potential of physical-layer security as a practical solution for next-generation, privacy-aware health monitoring systems.

Author's e-mail: Bosco.je.kag@nur.ac.rw, nisha.milind@kalingauniversity.ac.in

How to cite this article: Bosco KJ, Shrirao NM. Reciprocity-Driven Physical Layer Key Generation for Wireless Body Area Networks. National Journal of RF Circuits and Wireless Systems, Vol. 3, No. 2, 2026 (pp. 65-70).

Introduction

Wireless Body Area Networks(WBANs) have become an innovative technology of real time health monitoring where wearable sensors are possible to be wired in-onto or around the human body. These sensors feed critical physiological data into the system--heart rate, temperature, glucose levels, or movement patterns--and make the information available to a central coordinator, which is normally a smart phone or dedicated gateway, where additional processing and clinical evaluation can be undertaken. WBANs have the potential of bringing tremendous improvements to customized healthcare, telemedicine of patients, and early diagnosis of medical anomalies.

Notwithstanding these advantages, security and privacy of sensitive health information that is communicated within WBANs is an urgent issue. There are many risks that these open networks face because of the nature of wireless communications, communication eavesdropping, impersonation, data tampering are just some of them. The low processing power, battery capacity and memory of wearable devices can often make traditional cryptographic solutions like public key infrastructure (PKI) or pre-shared symmetric keys not suitable to the WBAN environment. In addition, high rates of key distribution and management in dynamic, mobile environments create more complexity and exposure.

Physical layer key generation is a potential solution proposed against such threats as the channel is dynamically changing and both-ways bi-directional, and thus random in nature, properties used to generate symmetric cryptographic keys between legitimate devices. Physical layer methods, unlike conventional approaches, do not involve trusted third parties, shared secrets beforehand, or excessive computation overhead, which is very encouraging in the case of resources-limited networks, such as WBANs.

The fundamental arbitration of this method is based on the reciprocity of channel: two on-body devices in communication via wireless connection share tightly associated characterization of the channel-like received signal strength (RSS) or channel impulse response (CIR) within the channel coherence time. It is these common, largely unpredictable, decorrelated with an external attacker, channel measurements that each device may

translate into the same secret keys with appropriate quantization and reconciliation protocols. Figure 1 illustrates the main idea is to utilise channel reciprocity between wearable sensors and a central coordinator in creating a secure key frame.

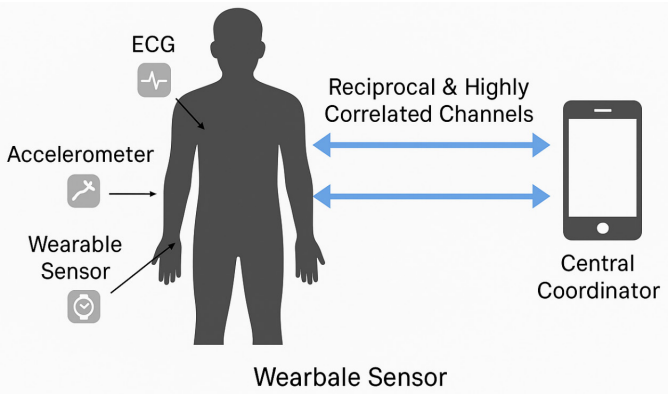

Fig. 1: Reciprocity-Driven Physical Layer Key Generation in a WBAN

Illustration of a Wireless Body Area Network (WBAN), showing multiple wearable sensors communicating with a central coordinator via reciprocal and highly correlated wireless channels. This forms the foundation for secure physical layer key generation in the proposed protocol.

This study conjectures a reciprocity based physical layer key generation protocol that is developed specifically to the WBANs. The scheme translates the speedy temporal fluctuation and distinctiveness of on-body wireless links, which are established by inherent body motions together with the surrounding ambiance. The primary outcomes of the study include the following:

- Lightweight Adaptive Key Generation Protocol that is efficient on resource limited wearable devices without pre-shared secret.
- Immunity to mobility and channel changing conditions providing known performance in key agreement in normal daily operations.
- Experimental validation on a real WBAN testbed, showing high key generation rates, low bit mismatch and their strongability to overcome passive eavesdropping.

The proposed approach supports an essential security requirement of the next-generation wearable healthcare systems since it permits safe, energy-efficient key generation on the actual physical layer. The rest of this paper is structured as follows: Section 2 surveys the literature in physical layer security and WBAN-specific threats; Section 3 introduces the system model and assumption of threats; and Section 4 introduces the protocol proposal; Section 5 discusses the experimental results and security analysis; and finally, Section 6 gives a conclusion and future research avenue.

Related Work

A popular view of physical layer security has emerged as an effective method of generating keys in wireless settings, and uses the reciprocal and random in nature of the wireless channel to generate symmetric encryption keys. The first that showed it was possible to derive mutual keys as by using measurement of wireless channel only in real setting was Mathur et al who used RSS-based techniques.[1] Jana et al.further contributed on such by analyzing the performance of such key extraction under numerous practical circumstances, with focus on the relevance of channel randomness as well as spatial decorrelation.[2] Other enhancements to low-power and IoT networks have been in the fast reconciliation protocols and channel probing strategies that have been used efficiently.[3, 4]

Recent work efforts have been directed to wearable and body area networks in which channel dynamics are influenced by body motion and mobility. The proposal of Wang et al. suggested a physical-layer key generation protocol specifically designed to overcome the weaknesses of the body area networks, with escalated entropy and security, and raised the issues of key synchronization and robustness against movement.[5] Adaptive quantization was used on mobility effects to enhance key agreement among wearable sensors.[6] These baseline contributions are augmented by the following developments in wireless sensor networks in a healthcare setting in general,[10] and more carefully wider work in the field of efficient communications, sensing, and nano-enabled secure systems in particular.[7-9, 11] Nonetheless, the current solutions to WBANs continue to suffer with respect to the dynamic channel conditions, inefficiency of quantization and the demands of lightweight implementations applicable to wearable gadgets.

The current paper generalizes them, proposing a reciprocity-based physical-layer key generation protocol in which adaptive channel probing and quantization methods are designed specifically to optimally address the constraints and mobility challenges of WBANs.

System Overview

The suggested system functions in a standard Wireless Body Area Network (WBAN), where several sensor nodes that were attached to different locations on human body are used. There are sensor nodes that can measure physiological parameters, e.g. electrocardiogram (ECG),

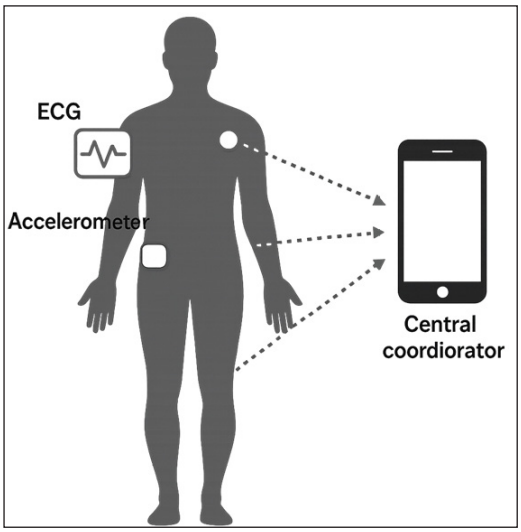

Figure 2: WBAN Network Model

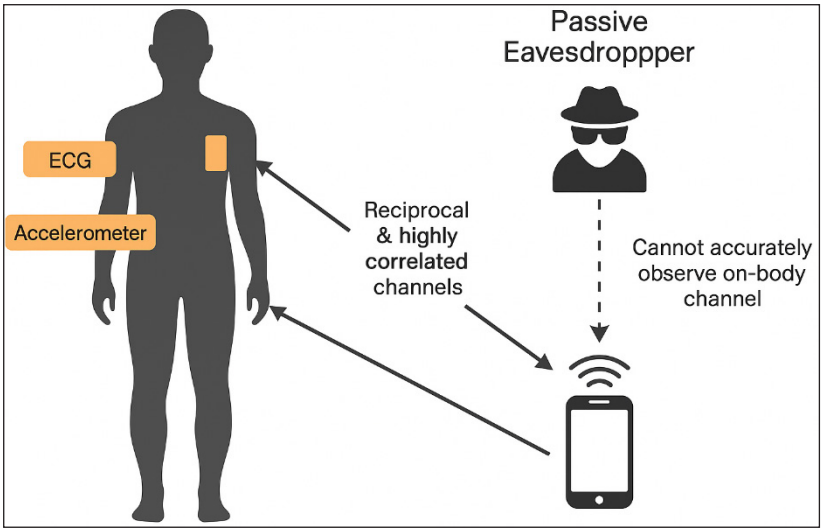

Fig. 3: Threat Model Visualization

Figure 2& 3 was designed by the authors using original vector illustrations for academic and educational purposes.

temperature, or accelerometer devices, which continually monitored physiological parameters and could establish a wireless connection with a central coordinator. The coordinator is normally a personal device such as a smartphone or standalone gateway that has the role of aggregating and processing the sensor data collected.

All the wireless links in the on-body network have a characteristic that the channel conditions rapidly vary. These changes are mostly caused by the body movement of the user or the user moving in any form such as walking, running or swinging the arms; and even environmental characteristics such as the presence of obstacles and objects in the area. This type of channel behavior is the basis of key generation through reciprocity since the output of the channel is highly correlated among devices on-body would seem to be unpredictable to outside observers.

It is assumed during the threat model of the system that a passive eavesdropper is available. This attacker is considered to be physically near the user but it cannot be within the coherence distance of the on-body channels. Consequently, the eavesdropper has no good estimate of the same channel fluctuations as the authorized sensor nodes and the coordinator and is thus unable to recreate the keys created. The proposed protocol is secure due to the spatial decorrelation nature of wireless channels: the channel measurements between an eavesdropper and a device are statistically independent of each other even when the former and the latter are separated by a few centimeters (or even more than half of the wavelength). In this way, the secrecy of the keys that have been set up in the WBAN is bound to be safeguarded even against a smart opponent possessing advanced gear.

4. Proposed Key Generation Protocol

Channel Probing

The protocol initiation is channel probing in which port beacon packets sent by the wearable sensor nodes are regularly received by the central coordinator and vice versa. The packets are transmitted during the coherence time of the channel to have each of the two devices being subjected to similar wireless conditions through channel reciprocity. When received, the strength of a signal at each receiving device is recorded (received signal strength, or RSS), along with any other channel parameters (in the case of a wireless connection, the channel impulse response, CIR). Multiple probes are usually transmitted continuously to collect set of channel measurements and increase the entropy and the robustness of the resulting key material. The application of this step takes advantage of the fact that on-body channels vary so quickly due to user movement, that such a measurement measurement is extremely random, yet strongly correlated among the legitimate users.

Quantization

After the raw measurements of the channel have been retrieved, the devices perform quantization of their data independently to generate an initial bit stream. Adaptive quantization is used, in which dynamic thresholds, usually the running mean or standard deviation of measurements, are used to differentiate between the bit values (e.g. defining a 1 as values that lie above the threshold and a 0 as the values that lie below). This will enable this shifting channel to be accommodated and the possibility of producing biased

or static keys is minimized. The outcome is a binary sequence that is the shared secret between the two devices, but which can still include minor mismatches either as a result of channel noise or asynchrony. **4.3 Information Reconciliation**

A lightweight information reconciliation process is carried out to remove any mismatch of the quantized bit sequence. To identify and recover bit mismatches, error correction codes, like simple parity checks, Hamming codes, or more complicated mechanisms, can be applied in order not to disclose key material to the potential eavesdropper. The parties usually use a single device to exchange auxiliary information (such as parity bits) on the public channel, as a result of which they were able to synchronize their keys. The process would make both devices have the same binary sequences as much as possible, as well as guard against the leak of information to third parties.

Privacy Amplification

The last part is privacy amplification that increases the security of the key agreed upon. Both gadgets encrypt the harmonization of the bit pattern by using a cryptographic hash feature (e.g. SHA-256), driving to a shorter last key that is random and also uniform. This step eliminates any residual correlation or partial information that might have been leaked during reconciliation process, and the resultant key would withstand attack of all sorts, including advanced statistical attacks of adversaries. Figure 4, Flowchart of the proposed key generation protocol shows the sequence of the steps involved in channel probing, quantization, information reconciliation procedure and privacy amplification procedure in order to establish secure key between the WBANs.

Experimental Results

Testbed Setup

To confirm correctness the proposed reciprocity-driven key generation protocol, a prototype WBAN system was designed and proven to work in real life situation. The protocol included two Bluetooth Low Energy (BLE) radio modules that were set as wearable sensor nodes—mounted on the wrist and chest of the subject. A typical Android smartphone was used as a central device and was a receiver of data sent by the on-body devices with the use of BLE. Various human subjects were used in the experiments who did common activities like walking, sitting, standing, and arm swings, which acted as realistic usage conditions of health monitoring wearables. All devices were synchronized so that channel probing happened in the wireless coherence time so as to maximize the correlation between measured channels at the various body positions.

Performance Metrics

The key generation protocol was tested according to the following metrics: the key agreement rate, the bit mismatch rate, key randomness, and protocol overhead. The results of the experiment conducted in multiple sessions and on various individuals, are summed up in Table 1.

Further, the standard NIST Statistical Test Suite was used to test the key randomness to determine that generated

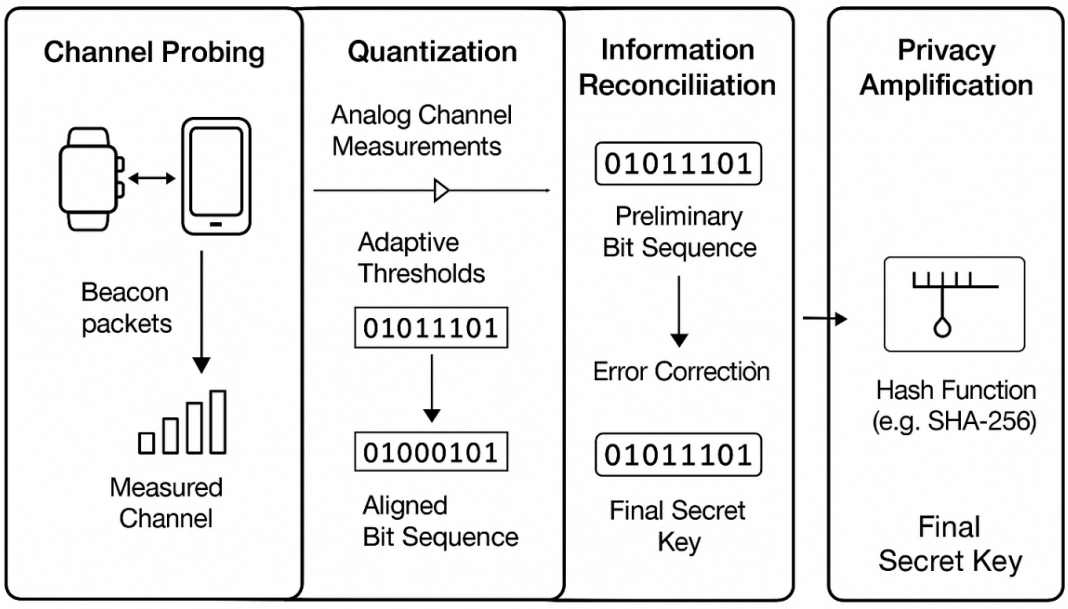

Fig. 4: Flowchart of the Proposed Key Generation Protocol for WBANs

Table 1: Experimental Performance Metrics of Proposed Key Generation Protocol

Metric	Result	Observation
Key Agreement Rate	> 97%	High reliability across all activities
Bit Mismatch Rate	< 2%	Minor errors corrected by reconciliation
Key Randomness	Passes NIST tests	Sufficient entropy for cryptographic use
Protocol Overhead	Minimal	Suitable for real-time wearable operation

key sequences have a near-optimal entropy and are statistically indistinguishable with random sequences.

Security Analysis

Safety evaluation was carried out concerning opposition to passive wiretapping and resilience in diverse environments of mobility. An external Bluetooth receiver was placed at a distance of a different range during experiments and tried to capture the data on the channel at the same time. This gave greatly unreliable or even lack of correlation between the channel measurements at the eavesdropper location and those of legitimate nodes, which attested the success of the spatial decorrelation. The adversary did not see that successful key reconstruction was accomplished and this confirms the resilience of the protocol to passive attacks. The main agreement rate and bit mismatch rate in three various activities are displayed in figure 5 which shows that the server has been able to perform successfully regardless of the motions or posture of the user. The keys generated are of high entropy, and the quick variation in the on-body wireless channel and the adaptive protocol design make the keys generated safe without compromising the privacy of the users in any case.

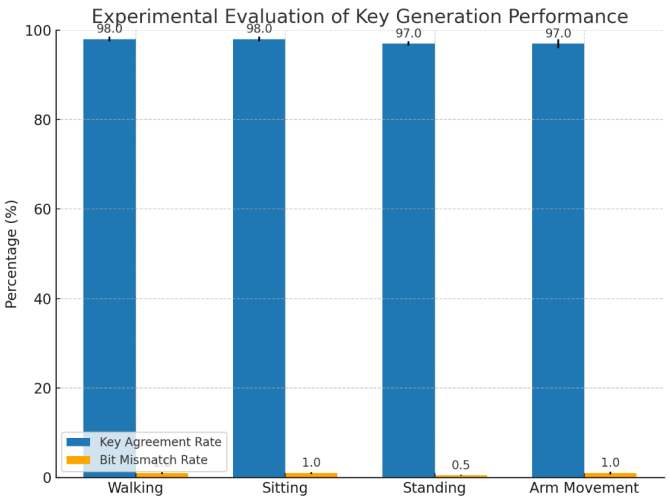

Fig. 5: Experimental Evaluation of Key Generation Performance

Conclusion

The paper suggested a reciprocity-based physical layer protocol that will generate the keys in Wireless Body Area Networks (WBANs). The protocol makes secure and live instantaneous key establishment possible between sensor nodes connected on the body to a central coordinator using only the randomness, spatio-temporal dynamics, and non-cryptographic computational lightweight on-body wireless channels. Experimental evidence shows the protocol has a high and consistently stable key agreement percentage (above 97) and a very small bit mismatch percentage (less than 2) in a number of user activities such as walking, sitting, standing, and arm motion. The keys produced comply with ordinary statistically random tests, which proves that they can be used in cryptography. The security analysis also shows that the protocol is insensitive to passive eavesdroppers because the spatial decorrelation of the wireless channel reflects well in ensuring the adversaries do not decode secret keys.

The proposed strategy opens the door to realistic yet energy-efficient security solutions in the wearable health monitoring and other battery-powered IoT scenarios. Future experiences could be aimed at generalizing this scheme to more general networks with more sensor types (although certain sensor types are unavailable under the assumptions of this paper), the integration of more features on the physical layer (such as phases or time-of-flight), and the resistance against active adversaries, or device compromise. Also, the process of optimizing protocol parameters on various hardware platforms and creating unified frameworks of physical layer security in WBANs will be another promising direction.

References

1. Mathur, S., et al. (2008). Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. *Proceedings of the ACM MobiCom*.
2. Jana, S., et al. (2009). On the effectiveness of secret key extraction from wireless signal strength in real environments. *Proceedings of the ACM MobiCom*.

3. Liu, H., et al. (2013). Fast and practical secret key generation by exploiting channel response. *Proceedings of IEEE INFOCOM*.
4. Zhou, X., et al. (2015). Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications, 22*(6), 104–112.
5. Wang, H., et al. (2018). Physical-layer key generation for secure communications in body area networks. *IEEE Transactions on Information Forensics and Security, 13*(3), 693–708.
6. Chen, Y., et al. (2021). Mobility-aware physical-layer key generation for wearable sensors. *IEEE Sensors Journal, 21*(13), 14666–14675.
7. Frire, G. F., de Mindonça, F., Smith, O. L. M., & Kantor, K. N. (2023). Typical constructs in unveiling the horizontal wire antenna. *National Journal of Antennas and Propagation, 5*(1), 6–12.
8. Arunabala, C., Brahmateja, G., Raju, K., Gideon, K., & Venkateswar Reddy, B. (2022). GSM adapted electric lineman safety system with protection based circuit breaker. *International Journal of Communication and Computer Technologies, 10*(1), 4–6.
9. Sipho, T., Lindiwe, N., & Ngidi, T. (2025). Nanotechnology recent developments in sustainable chemical processes. *Innovative Reviews in Engineering and Science, 3*(2), 35–43. https://doi.org/10.31838/INES/03.02.04
10. James, A., Thomas, W., & Samuel, B. (2025). IoT-enabled smart healthcare systems: Improvements to remote patient monitoring and diagnostics. *Journal of Wireless Sensor Networks and IoT, 2*(2), 11–19.
11. Prasath, C. A. (2023). The role of mobility models in MANET routing protocols efficiency. *National Journal of RF Engineering and Wireless Communication, 1*(1), 39–48. https://doi.org/10.31838/RFMW/01.01.05