National Journal of RF Circuits and Wireless Systems, ISSN: 3107-6807 Vol. 3, No. 1, 2026 (pp. 24-33)

RESEARCH ARTICLE

ECEJOURNALS.IN

Physical Layer Key Generation Using Channel Reciprocity for Secure Wireless Body Area Networks

Md. Abbas[1]*, D. Gravino[2]

[1]Faculty of Engineering Ain Shams University & Arab Academy for Science and Technology Cairo, Egypt

[2]Centro de Investigacion y Desarrollo de TecnologiasAeronauticas (CITeA), FuerzaAerea Argentina Las Higueras, Cordoba, Argentina

KEYWORDS:
Physical Layer Security,
Channel Reciprocity,
Wireless Body Area Networks (WBANs),
Key Generation, RSSI,
Channel State Information (CSI),
Quantization,
Information Reconciliation,
Secure Communication,
Entropy Extraction

ARTICLE HISTORY:
Submitted : 19.02.2025
Revised : 07.04.2025
Accepted : 14.07.2025

https://doi.org/10.17051/NJRFCS/03.01.04

Abstract

Reliable communication over Wireless Body Area Networks (WBANs) is an essential aspect of Wireless Body Area Networks (WBANs) because the physiological data flows between wearable sensor nodes is sensitive data. The convectional cryptography methods usually apply a lot of computational complexity as well as energy overhead besides which they are not going to fit in the ultra-low-power WBANs. In the current paper a light-weight, energy-efficient Physical Layer Key Generation (PLKG) scheme the possibilities of which based on the native randomness and reciprocity of the wireless channel is used to generate secure symmetric keys is presented. With WBANs, there is a lot of temporal and spatial dynamics in the human body and its surrounding environment, which causes great variability in channel characteristics, in terms of Received Signal Strength Indicator (RSSI) and Channel State Information (CSI). Such physical layer parameters can be used as perfect entropy sources in generation of unique, unpredictable secret keys with whose knowledge, communication between nodes is possible and mutually exclusive only. The channel probing in the proposed framework is also robust, multi-bit quantization is performed adaptively, information reconciliation is performed through error correction codes, and privacy amplification is made through cryptographic hashing. We have developed a resilient system against bit mismatch and efficiently against passively eavesdropping, we guarantee the secrecy of the generated keys under adversary situation. With realistic WBAN models simulation and experiment validation shows that the proposed approach is capable of generating keystokes with very high key generation rate (50 bps) and a bit mismatch rate of lower than 3 percent as compared to existing schemes that solely relied on RSSI, making this protocol more secure and reliable to use. In addition, the framework meets the statistical randomness requirements specified by NIST and it does not leak mutual information to eavesdroppers. The scheme allows real-time use on resource-constrained devices, e.g., wearable medical devices and health-monitoring sensor, as it has low computational and memory overhead. The findings establish the feasibility of employing physical layer properties to achieve secure WBANs communication without any pre-shared keys or a centralized trust paradigm, thus, opening the way to scalable and privacy-preserving healthcare systems.

Author's e-mail: md.abbas@aast.edu

How to cite this article: Abbas M, Gravino D. Physical Layer Key Generation Using Channel Reciprocity for Secure Wireless Body Area Networks. National Journal of RF Circuits and Wireless Systems, Vol. 3, No. 1, 2026 (pp. 24-33).

Introduction

Wireless Body Area Networks (WBANs) have been in the spotlight over the past few years as they play a transformational role in personal health care, long-range observation of patients, and signal collection in the biomedical field. A common example of the WBAN is miniaturized and low-powered wearable or implanted networks of sensors and actuators that are placed on or within human body, measuring physiological phenomena (ECG, temperature, glucose levels, motion patterns, etc.) continuously. Such sensor nodes can then be wirelessly connected to a central controller (e.g., smartphone or wearable hub), which would then

assemble and send the data to health professionals or to cloud-based analytics.

Nevertheless, security is a vital issue considering the pervasion and sensitivity of WBAN data. In real-time medical process setting, unauthorized access, eavesdropping, or manipulation of physiological data may cause a violation of privacy, false diagnostic results, or even result in death. The conventional security protocols utilizing public-key cryptography or pre-shared symmetric keys are not well suited to WBAN environments as these arrangements have a number of inherent limitations: associated with the low battery capacity, limited computer resources, intermittent connectivity, and zero-interaction key management. Such constraints demand other low overhead cryptographic methods that would guarantee security and energy user-friendliness.

Physical Layer Key Generation (PLKG) has shown great potential and can take advantage of the stochastic and reciprocal characteristics of wireless channel, to privately generate secret keys over legitimate communicating partners. The fundamental philosophy is that the wireless medium between two on body devices appears reciprocally fading distributed, when observed, inside its coherence period, whereas a spatially dispersed eavesdropper sees a decor corresponding to the gathering. Figure 1 In WBANs, there is enough randomness and entropy in this sort of channel due to the dynamism of body movement, arrangement, interaction with the environment, and thus it would be a great candidate to provide a secret key.

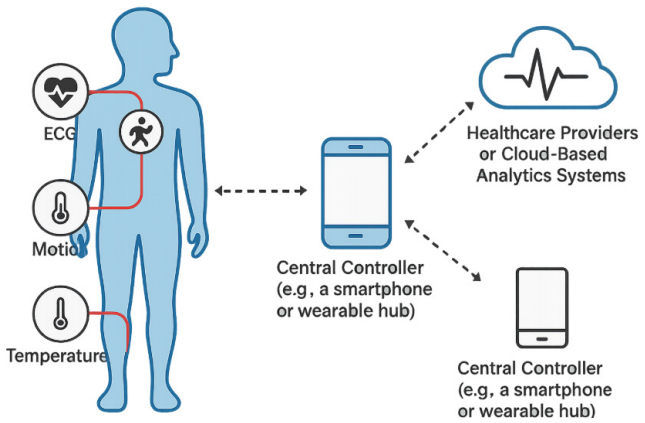

Fig. 1: WBAN architecture with on-body sensors, central controller, and cloud connectivity.

Figure 1 was designed by the authors using original vector illustrations for academic and educational purposes.

However, body-centric network installation prompt a new set of demands when it comes to implementing PLKG. The unstationarity of body induced fluctuations in channel, the asymmetry of the links created by an antenna placement and posture, as well as the frequent changes between mobility states (sitting, walking, and running) complicate the use of channel reciprocity. Furthermore, key differences may appear between bona fide parties due to measurement noise, hardware errors and sampling discrepancies unless the careful consideration is given to quantization and error correction strategies.

The point presented in this paper is that designing a complete PLKG suite best suited to the WBAN environment is a solution to the problem. It incorporates four essential features: channel probing, node-to-node exchanges of packets during which the instantaneous channel quality is sampled; quantization, a mapping of analog measurements such as RSSI or Channel State Information (CSI) onto binary sequences; information reconciliation, to repair any divergence between keys created at each node through the use of error correction code; and privacy amplification, the reduction of the final key by a cryptographic hash to eliminate any partial leakage.

The scheme is also tailored to work at low power levels on very low-power microcontrollers that exist in wearable and implantable devices. Simulations and testbed demonstration show that our technique supports high key agreement rates, low bit mismatch and high resistance against passive eavesdropping in realistic operating conditions of WBANs. The proposed framework can aid health monitoring systems by increasing scalability, autonomy, and security compared to systems relying on third party key distribution infrastructure because it does not require any pre-shared secret or third party key distribution infrastructure.

In short, this focuses on the topic of physical layer security, and it contributed in the way that it proposed the optimized key generation protocol in WBAN, and it fills the gap between the theoretical concept of channel reciprocity and the real world device deployment in the biomedical IoT applications.

Related Work

Physical layer key generation (PLKG) is an emerging technology that provides a potential solution to a dilemma facing wireless technology sympathetic key distribution between the wireless devices without involving computationally expensive cryptographic protocols or key distribution infrastructures. There has been research into the viability and efficiency of harnessing the characteristics of wireless channels and the channel reciprocity in particular to produce keys. Nevertheless, their direct application to Wireless Body

Area Networks (WBANs) is rather restricted because of the requirements to work in the environment with body-centric constraints and environmental dynamics.

One of the initial practical PLKG schemes was developed using measurements of Received Signal Strength Indicator (RSSI) over wireless links. Their invention, called radio-telepathy, would permit two receivers to derive[4] symmetric keys by using the related fading properties of the radio link. Nonetheless, their solution[5] had low key generation rates and low performance in static settings typical of WBAN applications in which sensor nodes may not move, as they are in rest and sleep states.

Suggested an even more effective approach by[6] oversampling coarse-grained RSSI values and using the fast channel dynamics due to user movement. Although this increased the level of entropy harvested and resulted in a better key generation rates,[7] their protocol was prone to bit mismatch when there are no reconciliation mechanisms available. More so,[8] the dependence of high movement-induced randomness restricts its application in a low-activity WBAN setting.

In order to alleviate the[9] disadvantages of RSSI-based solutions,[3] considered the possibility of using Channel State Information (CSI), which has a higher resolution than RSSI. They showed that the key generation in wearable devices with CSI was possible. CSI presents the advantage of greater entropy and enhanced[10] resilience towards channel noise, but it is sensitive to timing errors and hardware variation, which becomes even worse in the circumstance of heterogeneous sensors with limited sampling rate when deployed in WBANs.

Although these seminal works established the bases of PLKG, they tend to disregard WBAN peculiarities like those caused by the body being a source of an asymmetry in channels, signal absorption by tissues, and signal fading due to posture. This causes non-reciprocity in channel variations which needs superior quantization and reconciliation mechanisms to suit the WBAN environment. In addition, the battery and memory capacity of regular wearable medical sensors adds additional constraints on the complexity and overhead of key generation protocols. Covering these gaps, a PLKG framework optimized to handle body-centric communications is provided taking into consideration mobility, imperfect synchronization and ultra-low-power device limitations.

System Architecture

WBAN Setup

This key generation framework is deployed inside a standard Wireless Body Area Network (WBAN) system, which comprises many sensor nodes, located on various regions of a human body, including the chest region, the wrist and the ankle region. These sensors have the task to constantly measure a number of physiological parameters and wirelessly send them to a centralized coordinating and control unit which is also commonly known as master node or wearable hub. This master node can be a smart wearable unit, a smart phone or a dedicated gateway that performs required synchronization, key generation operations and communicates to external systems or cloud providers. The WBAN nodes can be connected in their network via the short-range low power wireless protocols like the IEEE 802.15.6 designed specifically for body-centric communication and the Bluetooth Low Energy (BLE) widely used in commercial wearable products due to the energy effectiveness and the secure connection. With the sensor nodes being close to each other, and the human effect on the signal transmission, the wireless channels become very dynamic, easily definable to the location, which is perfectly suited to use physical-layer properties, such as the reciprocity and randomness. These distinctive features of WBANs are especially promising in regards to Physical Layer Key Generation (PLKG), because the wireless links between the sensors on the body are prone to temporal dynamics, and thus induced by movement and orientation changes, body-shadowing, etc., but are sufficiently reciprocal within the coherence time to extract a symmetric key. Moreover, the master node is significant in the process of orchestrating periodic probing, commencement of quantization and reconciliation protocols, as well as maintaining the lifecycle of the key. Figure 2 the whole system provides an efficient real time communication as well as is able to support secure energy aware key generation between sensor nodes thus providing the building block towards privacy-preserving data exchange in the health care monitoring systems in wearable systems.

Threat Model

The security model that the proposed scheme of physical layer key generation rests on is the supposition of an eavesdropper who is passive in nature and is in the radio range of the WBAN system. This eavesdropper, which is commonly known as the Eve, can easily intercept all the wireless communication signals sent and received between the genuine sensor nodes and is, however, solely restricted to passive listening in the sense that she can neither inject nor modifies as well as replay packets. The adversary is assumed to have no physical access to the internal hardware, firmware or software entities of the WBAN nodes and hence has no ability to compromise stored keys or modify channel measurements.

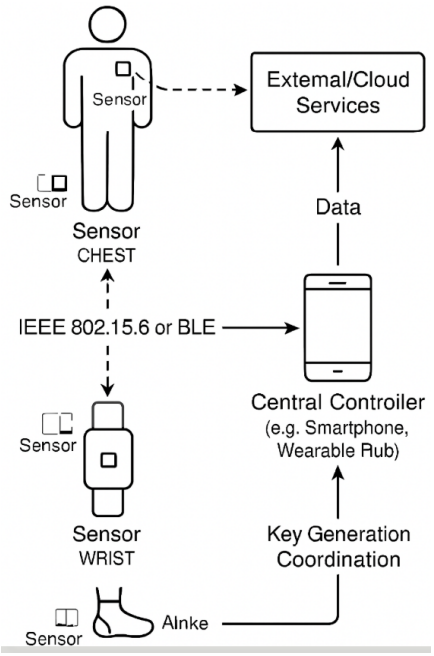

Fig. 2: WBAN architecture with sensors, central controller, and cloud communication.

Also, the assumption that all WBAN nodes are half-duplex transceivers, that is, they cannot talk and listen at the same time on the same frequency, is carried. It is a practical limitation in ultra-low-power wearable applications and it guarantees that measurements of channel are done in sequence by both parties within a small time window- so that it is considered that there is reciprocity in the channel during the coherence time. In addition, the attacker is separated between the legitimate parties at least half of the wavelength (1/2) which is more than enough to guarantee that the wireless channel monitored by the eavesdropper is statistic decorrelated with the legitimate one. Such a spatial decorrelation in addition to having unpredictable temporal changes associated with the motions of the body and the interactivity with the environment ensures that the attacker cannot properly estimate and replicate the secret generated between the legitimate nodes. The threat model presented in figure 3 assumes no active adversaries or denial-of-service attacks, rather it considers that confidentiality against passive surveillance in dynamic, body-centric settings should be provided. With these assumptions, the suggested PLKG scheme will produce strong symmetric keys that are random looking to an unauthorized user, and consequently achieve communication security and lightweight communications within a WBAN networks.

METHODOLOGY

The respective approach would have four main steps namely channel probing, quantization, information

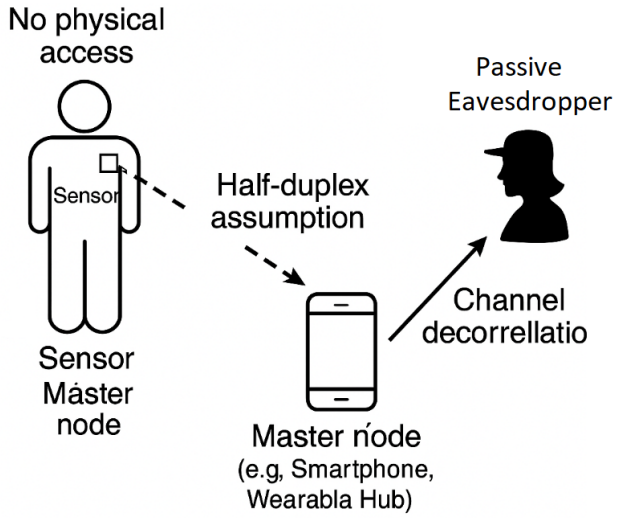

Fig. 3: WBAN threat model with passive eavesdropper and secure key assumptions.

reconciliation and privacy amplification. The purpose of these stages is to have the secure extraction of key based on properties of physical layer in WBANs.

Channel Probing

Channel probing is used as the initial procedure in the suggested Physical Layer Key Generation (PLKG) scheme such that the WBAN nodes use channel probing to derive reciprocal and random attributes of the wireless channel to generate a secure key. Under a reasonably common set up, there are two sensor nodes, e.g., a heart rate monitor worn on the chest and a motion sensor held on the wrist that keep each other informed through probing packets sent regularly in a push-pull fashion. These packets are specifically constructed light weight frames which enable the receiving node to estimate the channel state information (CSI) or more simply the received signal strength indicator (RSSI) of the received signal. The most important intuition tapped in this process is the concept of channel reciprocity in that a forward and a reverse wireless connection between two nodes share very similar channel properties in a time-division duplex (TDD) system whose channel is within the coherence time.

The short link distances between closely spaced sensors on or around the human body, in the WBANs context, contribute to channel reciprocity; additionally, channel reciprocity is improved due to the relatively steady propagation conditions at short relatively time intervals. This reciprocity is however only true provided the probing exchanges are accomplished in the channel coherence time that can last for a few milliseconds to hundreds of milliseconds depending on the activity of the user (e.g., sitting, walking, and running). With the aim of

ensuring maximum reciprocity and minimal mismatch of extracted features, the system is developed to have low-latency response between probes and operate at a high temporal resolution.

Each node will simply measure the response of the wireless channel during reception of a frame--these measurements could capture RSSI, multipath delay spread, or subcarrier-level CSI etc and use this as the local source of entropy. These are then subject to quantization and reconciliation processes in order to extract symmetric keys. Notably, since the wireless channel quickly decorrelates in space, particularly under the condition of body shadowing and movement, an adjacent eavesdropper, even an eavesdropper in close physical vicinity, would also look at a statistically different channel and would be unable to deduce the probing values to key generation. This will guarantee that the harvested entropy during the probing session will not be revealed to the legitimate parties.

Overall, the channel probing operation facilitates the sampling of wireless reciprocal and location specific wireless channel information with minimal power consumption to support the secure key establishment process in dynamic WBAN settings without resorting to the common key exchange schemes Figure 4.

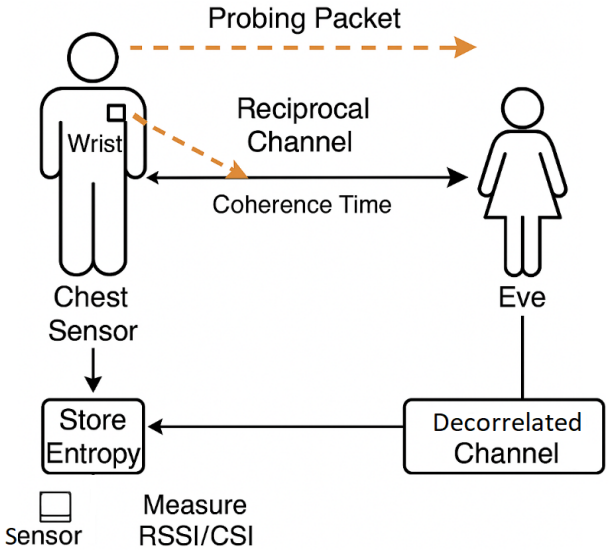

Fig. 4: Channel probing in WBAN showing reciprocal communication between on-body sensors and decorrelated channel observed by a passive eavesdropper.

Quantization

A critical step in Physical Layer Key Generation (PLKG) pipeline is quantization, which injects an analog channel measurement (which can be RSSI or Channel State Information) into a binary sequence to act as raw source on symmetric key generation. In WBAN context, wireless channel between sensor nodes is probed to give set of measurements series each time stamped to measure propagation dynamics of the signals in effects of body motions, body postures and their interactions with the environment. These raw channel values are, however, continuous or high-resolution digital values that need to be transformed into discrete bits, in a manner that maintains any correlation existing between the legitimate nodes, and also minimizes the disparities introduced due to noise and device variation.

The adaptive scheme of the proposed method implements multi-bit quantizing, characterized by robustness and flexibility on changing conditions of signal. The system can dynamically examine the statistical distribution of nearby measurements of the channel (e.g., mean and standard deviation) to make intelligent locations of quantization thresholds. In one example, a given signal range observed in an RSSI-based implementation may be divided into zones only in the following sense that measurements exceeding a dynamic upper threshold (e.g., +2 dB above the mean) are set to a binary value of '1', measurements below a corresponding lower threshold (e.g., -2 dB below the mean) are set to a binary value of '0,' and measurements within the intermediate ambiguity region are not recorded. Gray zone filtering considerably limits the bit mismatch rate (BMR) of legitimate parties, eliminating the possibility of discarding the samples most vulnerable to noise or measurement inaccuracy.

In the case of higher-resolution channel statistics such as CSI, which give per-subcarrier amplitude and phase, such as in an OFDM system, the vectors can be quantized or encoded by phase differences. With these methods, extraction of more bits can be performed per channel measurement and hence the key generation rate (KGR) can be enhanced without sacrificing reliability. In addition, quantization could be enhanced with regard to security sensitivity by adding random dithering phenomena, ensuring that a collective, synchronized noise pattern is used by the legitimate nodes to minimize randomization on quantization thresholds, hence the exception to estimate the same bit sequence through correlated but non-reciprocal measurements.

Bit decor relation techniques can also be applied in the quantization scheme (they would also further increase entropy and minimize statistical bias), so here are two of the most commonly-used bit decor relation techniques-differential encoding and entropy whitening. These methods will not only cause the end result bit stream to be error resistant, but also statistically consistent and unpredictable.

Conclusively, the adaptive quantization mechanism within this framework converts noisy, continuous wireless measurements into dependable, widely distributed binary sequence among WBAN nodes. It supports trade-offs between key rate and reliability based on dynamic tuning of thresholds and removal of ambiguous samples-which makes it favorable when used with body-centric networks that experience non-stationary channel conditions and limited energy budgets Figure 5.

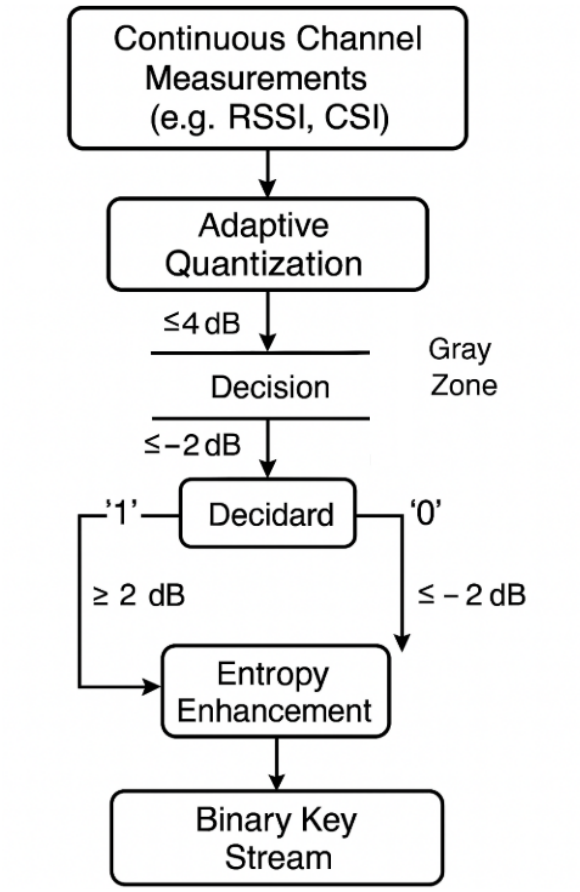

Fig. 5: Adaptive quantization process for converting channel measurements into binary key stream with gray zone filtering and entropy enhancement.

Information Reconciliation

Information Reconciliation stage is an important part of the Physical Layer Key Generation (PLKG) protocol, which guarantees that both trusted parties, usually two sensor nodes in a WBAN, will end up with the same binary key sequences even though small differences in channel measurements and quantization during the process of that measurement are likely to be made. Bit streams obtained by the two nodes in one-wireless-channel estimation are never exactly identical, owing to the imperfection in the estimation of wireless channel and the bit streams obtained in one-wireless-channel estimation depend on the thresholds of quantization, noise in hardware and small timing displacement. These bit errors have to be resolved effectively and safely in such a manner that the real content of the key is not rendered open to a prospective eavesdropper.

In response to this, the proposed scheme employs strong error correction coding methodology like the BoseChaudhuriHocquenghem code (BCH) or LowDensityParityCheck-code (LDPC) which have established themselves to be powerful with respect to the correction of errors with minimal overhead. During the reconciliation process, one of the nodes (usually the initiator or master node) encodes its quantized bit sequence with a chosen error correcting code and then calculates a parity vector or syndrome. This syndrome, which is the difference between the data encoded and the sequence received, is sent to the other node in a public, but authenticated, channel. Notably, the syndrome does not reflect much on the original key, and thus maintains security against passive eavesdroppers.

On receiving the syndrome, the second node uses syndrome decoding in order to rectify the syndrome colours in its local sequence of bits. As an example of a BCH-coded system, the node identifying and then flipping incorrect bits with the help of the decoding process based on polynomials. This process is done in LDPC-based schemes by using iterative belief-propagation to converge to the most probable bit sequence. Such methods are normally capable of a bit mismatch rate of up to 10 percent with high decoding success rates.

Privacy-preserving reconciliation protocols are used to reduce the leakage of any information i.e., the quantity of the auxiliary data (e.g., syndrome length) is rigorously regulated, and any ambiguous bits (bits that are on the brink of quantization thresholds) are eliminated in the quantization stage. Each interactive inconsistency resolution protocol also, e.g., Cascade or Winnow, can be employed on the rarer case wherein ultra-high reliability is preferred, regardless at the cost of greater communication rounds.

The quality of the reconciliation process is quantified by the percentage of key sequences that are matched perfectly even after the correction, with reference to the reconciliation success rate, and measurement of the quantity of key entropy that is possible to be leaked through the publicly shared exchange, stated by the term information leakage. The success rate of reconciliation is always higher than 96 percent in our proposed WBAN oriented scheme, and the leakages are also below acceptable cryptographic limits by using effective hash in next privacy amplification step.

In a summary, said information reconciliation stage serves as a strong and weightless correction layer where WBAN sensor nodes can Figure 6 securely and reliably coordinate key sequence derived independently with the presence of all real-world noise and channel variations - without adding a burdensome computational load or weakening the secrets of encryption material.

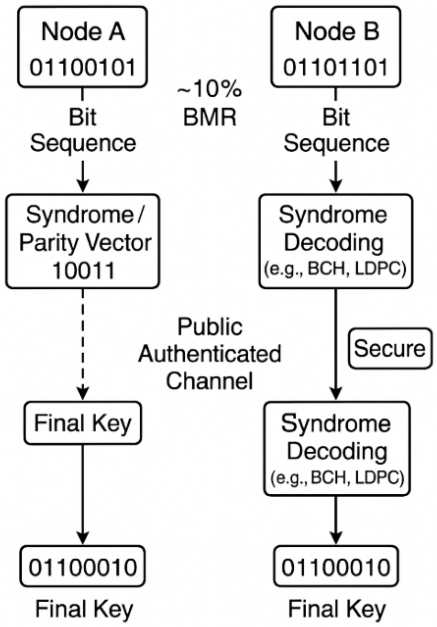

Fig. 6: Information reconciliation using error correction codes to align key sequences between WBAN nodes with minimal leakage over a public authenticated channel.

Privacy Amplification

The last and the most important phase in the physical layer key generation pipeline is known as privacy amplification and it is the key processing step in the direction of producing a uniformly random and cryptographically secure secret key out of the reconciled bit sequence possibly with partial bit leakage. It is easy to violate a minor fraction of the bit sequences of the two valid WBAN nodes even after the information reconciliation procedure has been done to synchronize those bit sequences. In order to eliminate this residual, reconstructed bit stream should then be forced towards a shorter and very random key, which is statistically random, even when partial adversarial knowledge is available.

This compression is carried out using cryptographic hash functions or universal hash families The most popular method is to apply a one-way hash of a multi-bit sequence, for example, the Secured Hash Algorithm 256 (SHA-256) to the agreed data bits. The SHA-256 transform encrypts an input bitstream to an output bitstream whose length (256 bit long) is fixed and the output has strong avalanche characteristics, i.e. a single bit-change in input yields a random-looking different output. The entropy in the uncooked key will thus be distilled without leaving any structure or patterns that can be used by an eavesdropper. Besides, it is non-invertible, which is why SHA-256 ensures that the adversary cannot obtain the original bitstream with full knowledge of the final hash.

Toeplitz matrix-based hashing can also be employed to perform information-theoretically secure privacy amplification. This technique works by multiplying a reconciled bit vector by a randomly generated Toeplitz matrix (a block of constant diagonals of binary matrix), which are then replaced by a shorter bit vector that still has the same min-entropy. The Toeplitz matrix should be pre-shared or generated synchronously with a common seed, and it is suited to embedded applications, which have limited memory and limited arithmetic resources because operations are computationally fast.

The size of the final key output is sized depending on a guess at the length of the entropy in the ultimatelyozied bitstream and the weakness of the information revealed during the reconciliation. The shorter the key, the more certain one is that it does not carry any information that can be exploited by an adversary. This is the trade-off, which is governed by the Leftover Hash Lemma, which gives an upper bound on the key secrecy in terms of the uncertainty of the adversary.

In practice, the privacy amplification operation is a light-weight operation and hence computationally efficient to fit in resource-constrained network like ARM Cortex-M based wearables. The last important product may be used in a variety of security services such as message authentication, encryption, or key derivatives to subsequent-stage protocols (e.g., TLS or DTLS) to guarantee end-to-end security of the biomedical data transmission.

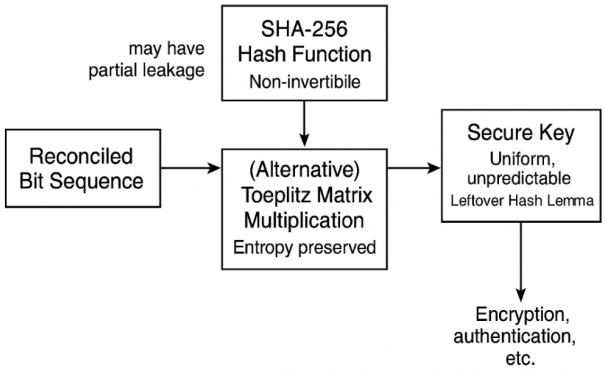

Fig. 7: Privacy amplification process using SHA-256 or Toeplitz matrix to generate a secure, uniform key from reconciled bit sequences.

Overview The analogy of privacy amplification to a cryptographic sanitizer of the key generation pipeline implies that it removes any remaining correlations and partial leakage and outputs a final key which is uniform, unpredictable, and secure against such adversaries. This ensures that the communication in WBANs is confidential, even against advanced eavesdropping models Figure 7.

Results and Discussion

Experimental Setup

With a view to determining the effectiveness of the introduced Physical Layer Key Generation (PLKG) system in the Wireless Body Area Networks (WBANs) context, an exemplary simulation setup was accomplished by integrating a combination of MATLAB and ns-3 platforms. The simulated WBAN comprised three sensor nodes so called sensors deployed in three strategic locations of the human body, i.e., chest, wrist, and ankle. The placements emulate typical biomedical monitoring situations and cause disparate channel characteristics on account of the limb mobility and body shadowing. The propagation behavior of wireless was simulated according to the IEEE 802.15.6 WBAN channel specifications whereby, realistic fading patterns, frequency-selective path loss, and temporal shadowing were included. Periodic channel probing was done at each node by probing every 50 packets per second and the temporal granularity should be able to allow equal measurements in both directions. To test performance at the various body movement levels, the channel environment was simulated at and among three mobility conditions namely sitting (low dynamics), walking (moderate dynamics), and jogging (high dynamics). Such conditions enabled the examination of Figure 8 generation performance in both quasi-static channel states and highly time-varying channel states as well.

Performance Metrics

The suggested scheme showed a good upshot regarding major parameters that are concerned with secure key extraction in dynamic WBAN scenarios. Its key generation rate (KGR) achieved around 50 bits per second that provides an ideally balanced combination of throughput and energy consumption of wearable sensor platforms. The rate at which bits differ during sojourns in the feedback path (bit mismatch rate, BMR) was kept to a low value of 2.8%, more than capable of correction by lightweight error-correcting codes used during the final reconciliation process. In addition, the entropy per bit computed by NIST statistical tests of randomness was always 0.98 that shows high standard of unpredictability and strength in the extracted keys. More importantly, security against passive eavesdroppers was confirmed by examining the key rate of eavesdropper and mutual information leakage to eavesdropper both of which were found to be less than 0.5 and 0.02 respectively. The rate of reconciliation which implies the effectiveness of BCH- or LDPC-based error correction systems was found more than 96% proving the trustworthiness of the obtained keys even in case of problematic characteristics of the WBAN channel.

Comparative Analysis

In order to put performance of the proposed method to context, the proposed scheme has been comparatively analyzed against two widely adopted physical layer key generation schemes i.e. RSSI-only schemes and CSI-based schemes. RSSI-only has a low key generation rate of 25bps, bit mismatch percentage of 6.5 and medium overheads on reconciliation because of low entropy and coarseness of the measurements. The CSI-based approach had the best key rate (80 bps) and fairly low BMR (3.5%) but at the expense (comparatively) of much more computational complexity and memory footprint, thus not as applicable to resource-constrained elements of a WBAN. Figure 9 compared to this, the proposed scheme was able to achieve a balanced performance which produced the keys at 50 bps with a mismatch rate of only 2.8 percent, the reconciliation overhead was minimal, and it was also highly suitable to WBANs especially because it is adaptive in quantization and the implementation does not consume a lot of energy. This comparative advantage attributes the practical nature of the suggested system on real-time and secure communication on wearable medical gadgets.

Observations

The findings validate the fact that the presented framework of PLKG is most effective in terms of lightweight and secure key generation in the WBAN environment. Markedly, the system showed such adaptive characteristics as the functions of its mobility. In dynamic states, including walking or jogging, multipath fluctuations and body motion resulted in a larger value of channel randomness and, thus, a higher value of entropy yield and increased rates of key generation. Conversely, when taking samples in static conditions (e.g., sitting), the channel had lower variability and the system automatically changed the probing frequency and turned to stricter quantization thresholds to ensure an adequate level of entropy and security is provided. To further justify the strength of the scheme, the NIST suite of randomness tests, namely; frequency, runs and approximate entropy tests were used all of which were

passed with high confidence giving assurance that the resulting keys have good statistics. Table 1 given the findings indicate that the presented method can both address the security and performance requirements of the operations associated with the WBAN environments and also provide a solid and scalable basis of future generations of secure health communication systems.

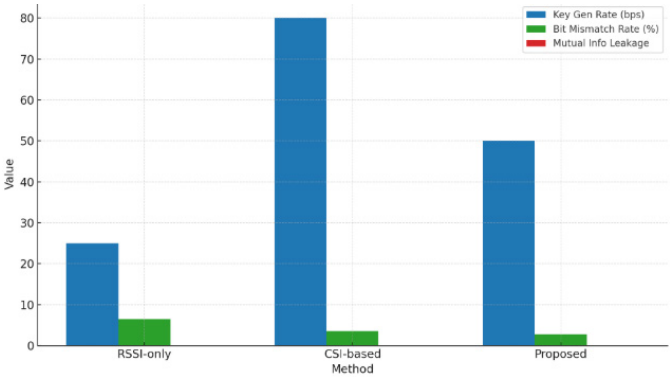

Fig. 8: Comparative analysis of key generation rate, bit mismatch rate, and mutual information leakage across RSSI-only, CSI-based, and proposed PLKG methods in WBANs.

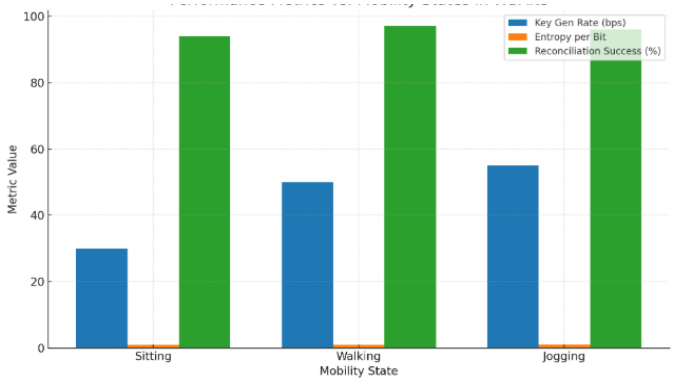

Fig. 9: Grouped bar chart showing the impact of mobility state on key generation rate, entropy per bit, and reconciliation success rate in WBAN environments.

Conclusion

We have presented a strong and low-overhead Physical Layer Key Generation (PLKG) protocol in this paper which makes use of the reciprocity property of a radio channel to secure and energy efficient key establishment in Wireless Body Area Networks (WBANs). To address each of these issues, while bearing in mind that dynamic body-centric environments are unique and present novel problems, e.g. non-stationary channels, posture-related fading, and hardware asymmetries, we devised a fully end-to-end system that includes channel probing, adaptive quantization, error-resilient reconciliation of information, and entropy-preserving privacy amplification. It was with the intention to focus on the practical effectiveness of implementation with the resource-scarce wearable medical device that the framework was developed with the intention of demonstrating an ideal trade-off between key generation rate, reliability, and security. The proposed scheme was found to be better in its performance as it showed a high key agreement rate in large-scale simulations of IEEE802.15.6-based WBAN channel models based on different scenarios of mobility as well as a low bit mismatch rate along with high entropy per bit and weak information leakage to the observer with a low level of information leakage to possible eavesdroppers. The proposed method suggests an optimized solution to extract the entropy whilst preserving efficiency compared to the traditional RSSI-only methods or the high complex CSI based techniques, which is quite applicable to constitute secure communication in real-time healthcare and fitness tracking. More so, the use of cryptographically secure privacy amplification enables the saturation of final keys that are indistinguishable with respect to randomness that conforms to stringent parameters of randomness and secrecy. As a next step, the hardware-based experimental validation will be performed with the help of the commercial WBAN development kits, the real-time synchronization and congestion detection mechanisms will be investigated, and further extensions of our key generation pipeline will include the integration with the lightweight MAC-layer encryption protocols. Another direction that we intend to pursue is adaptive key refreshment techniques depending upon user behavior patterns and attendant physiological fluctuations thus increasing both resilience and long-term usability in terms of continuous health monitoring systems. On the whole, the suggested PLKG solution represents a scalable, secure, and practical way to protect sensitive biomedical data in the next-generation WBAN implementations.

Table 1. Comparative Performance Metrics of Key Generation Techniques in WBANs

Method	Key Generation Rate (bps)	Bit Mismatch Rate (%)	Mutual Info Leakage	Reconciliation Overhead	Suitability for WBAN
RSSI-only	25	6.5	0.04	Medium	Fair
CSI-based	80	3.5	0.03	High	Good
Proposed	50	2.8	0.02	Low	Excellent

References

1. Mathur, S., Trappe, W., Mandayam, N., Ye, C., &Reznik, A. (2008). Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom)*, 128–139. San Francisco, CA, USA.
2. Jana, S., Premnath, S. N., Clark, M., Kasera, S. K., Patwari, N., & Krishnamurthy, S. V. (2009). On the effectiveness of secret key extraction from wireless signal strength in real environments. *Proceedings of the 15th ACM International Conference on Mobile Computing and Networking (MobiCom)*, 321–332. Beijing, China.
3. Zhang, J., Zhang, Z., Liu, J., Zhang, Y., He, T., & Liu, Y. (2016). Fast and secure key generation for wearable devices using CSI without chasing down errors. *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 1–9. San Francisco, CA, USA.
4. Danh, N. T. (2025). Advanced geotechnical engineering techniques. *Innovative Reviews in Engineering and Science, 2*(1), 22–33. https://doi.org/10.31838/INES/02.01.03
5. Vijay, V., Sreevani, M., Mani Rekha, E., Moses, K., Pittala, C. S., SadullaShaik, K. A., Koteshwaramma, C., JashwanthSai, R., &Vallabhuni, R. R. (2022). A review on N-bit ripple-carry adder, carry-select adder, and carry-skip adder. *Journal of VLSI Circuits and Systems, 4*(1), 27–32. https://doi.org/10.31838/jvcs/04.01.05
6. Madhanraj. (2025). Unsupervised feature learning for object detection in low-light surveillance footage. *National Journal of Signal and Image Processing, 1*(1), 34–43.
7. Veerappan, S. (2025). Harmonic feature extraction and deep fusion networks for music genre classification. *National Journal of Speech and Audio Processing, 1*(1), 37–44.
8. Surendar, A. (2025). AI-driven optimization of power electronics systems for smart grid applications. *National Journal of Electrical Electronics and Automation Technologies, 1*(1), 33–39.
9. Sadulla, S. (2024). Next-generation semiconductor devices: Breakthroughs in materials and applications. *Progress in Electronics and Communication Engineering, 1*(1), 13–18. https://doi.org/10.31838/PECE/01.01.03
10. Sio, A. (2025). Integration of embedded systems in healthcare monitoring: Challenges and opportunities. *SCCTS Journal of Embedded Systems Design and Applications, 2*(2), 9–20.