Biometric Authentication in Galvanic Coupling Communications: A Physical Layer Approach for Secure Wearable Medical Systems

Stefano Caputo[1 [0000−0002−4516−8910]], Anna Vizziello[2 [0000−0002−6378−141X]], Antonio Coviello[3 [0000−0001−9080−3584]], Maurizio Magarini[3 [0000−0001−9288−0452]], Giacomo Borghini[1 [0009−0006−8964−6490]], Pietro Savazzi[2 [0000−0003−0692−8566]], Sara Jayousi[4] and Lorenzo Mucchi[1 [0000−0001−6389−0221]]

[1] Department of Information Engineering, University of Florence, Florence, Italy
name.surname@unifi.it
[2] Dept. of Electronics, Computer and Biomedical Eng., University of Pavia, Italy
name.surname@unipv.it
[3] Dept. of Electronics, Information and Bioengineering, Politecnico di Milano, Italy
name.surname@polimi.it
[4] Polo Universitario Città di Prato, Prato, Italy
name.surname@pin.unifi.it
Corresponding author: lorenzo.mucchi@unifi.it

Abstract. This paper presents a biometric authentication framework based on Galvanic Coupling (GC) signals for secure communication in Wireless Body Area Networks (WBANs). Unlike traditional biometric systems that rely on handcrafted features, our approach leverages a Long Short-Term Memory (LSTM) neural network to classify raw GC signals directly, exploiting the subject-specific characteristics of the propagation channel. The system is designed for on-body configurations and integrates a lightweight authentication protocol that operates at the physical layer. Experimental results demonstrate the effectiveness of the proposed method in mitigating both over-the-air and direct contact attacks, achieving high classification accuracy and robustness through confidence-based rejection mechanisms. The solution is optimized for low-resource environments, making it suitable for real-time medical applications.

Keywords: Physical Layer Authentication · Wireless Body Area Network · Galvanic Coupling (GC) · On-Body Communications · Long Short Term Memory Neural Network (LTSM) · Deep Learning signal classification

1 Introduction

Wearable technologies are increasingly shaping the future of healthcare by enabling real-time tracking of physiological parameters, personalized therapeutic interventions, and enhanced recovery. These compact and intelligent devices are particularly beneficial in managing chronic illnesses such as cardiovascular and

neuromuscular disorders. Their integration into clinical workflows allows continuous data acquisition and remote patient supervision. Despite these advantages, the reliability and security of wireless communication among devices remain a major concern, especially in scenarios involving sensitive medical data [1,2]. According to recent market analyses, the global wearable medical devices market was valued at USD 42.74 billion in 2024 and is projected to reach USD 168.29 billion by 2030, growing at a compound annual growth rate (CAGR) of 25.53% from 2025 to 2030 [3].

In parallel, the widespread use of mobile electronics, such as smartphones, tablets, and smartwatches, has significantly changed how users interact with digital services. These devices now serve as multifunctional platforms, supporting activities from financial transactions to health monitoring. As a result, the need for secure and user-friendly authentication systems has become increasingly important [4]. Traditional approaches relying on passwords or physical tokens often suffer from usability and security limitations. Biometric authentication, which leverages unique physiological traits such as fingerprints or facial features, offers a more robust alternative [5]. To enhance the reliability of these systems, artificial intelligence (AI) techniques are commonly employed. Machine learning (ML) models can define biometric features, while deep learning (DL) approaches allow automatic feature extraction and classification. Furthermore, recent research has explored privacy-preserving methods for continuous authentication using sensor-based data, aiming to balance usability with data protection [6].

Galvanic Coupling (GC) has recently emerged as a promising technique for Body Area Networks (BANs), enabling on-body and intra-body communication through electrodes placed on or implanted within the skin [7]. Unlike traditional wireless methods, GC uses low-power electrical signals that propagate primarily through biological tissues, with most of the signal confined within the body and a small portion extending into the near-body region [8]. This results in a transmission path that is largely internal but not strictly limited to the body. The predominant confinement of the GC signal within the body reduces vulnerability to external interference and eavesdropping. Additionally, the use of low-power electrical signals and the short-range nature of GC transmission contribute to lower energy consumption compared to traditional wireless methods.

Inspired by Electroencephalogram (EEG)-based authentication systems, this work investigates the potential of GC signals for biometric verification in wearable medical applications. The unique and stable nature of the GC propagation channel, influenced by individual physiological traits, suggests its suitability for subject-specific identification. The proposed approach aims to integrate biometric authentication directly into the physical communication layer, enhancing the security of intra-body data exchange.

1.1 Related Work

GC has been extensively studied as a secure and energy-efficient communication method for BANs. Its ability to propagate signals primarily through biological tissues has led to various applications in medical and biometric systems. Prior

research has addressed physical layer design for authentication [9], transmission optimization for implantable devices [8], and experimental channel characterization [7], highlighting the subject-specific and stable nature of GC channels.

Building on these foundations, further studies have investigated the use of GC for cryptographic key extraction. Methods have been proposed to generate secret keys by exploiting the reciprocity of GC channels, enabling secure communication between on-body devices without the need for key exchange [10]. Earlier approaches have also leveraged channel randomness and movement-induced variations to enhance key entropy and authentication robustness [11, 12]. The integration of authentication into the key extraction process has been shown to be effective in preventing impersonation attacks [13].

In parallel, biometric authentication using physiological signals, particularly EEG, has been extensively studied. Multi-class classifiers such as neural networks [14], multilayer perceptrons [15], and convolutional architectures [16–18] have demonstrated high accuracy in user identification. Other machine learning models, including decision trees, support vector machines, and probabilistic classifiers, have also yielded promising results [19]. One-class classifiers have been employed to detect intrusions and authenticate users based on specific EEG patterns [20–22], while anomaly detection techniques like Isolation Forest and Local Outlier Factor have been applied to physiological data, although not always in the context of authentication [23–27].

1.2 Our Contribution

This work introduces a biometric authentication framework based on GC for BANs. The approach leverages subject-specific characteristics of the GC propagation channel to enable secure user identification. A Long Short-Term Memory (LSTM) network classifies raw GC signals directly, without relying on handcrafted feature extraction. The system operates in on-body configurations, such as communication between an implantable or wearable sensor and a GC-enabled smartwatch receiver, aiming to verify the identity of the transmitting device from the intrinsic properties of the propagation channel.

In addition, a lightweight authentication protocol is integrated into the communication process between wearable devices. This protocol incorporates biometric verification at the physical layer and is validated through experiments involving human subjects. The proposed solution is optimized for low-resource environments, making it suitable for real-time applications in medical contexts.

The remainder of this paper is structured as follows. Section 2 introduces the overall methodology, presenting the considered threat models and the design of the authentication framework. The experimental campaign, together with the setup adopted for GC signal acquisition, is then described in Section 3. Numerical results and performance analysis are discussed in Section 4, while Section 5 concludes the paper and outlines possible directions for future research.

2 Methodology

In wearable medical systems, secure communication between on-body devices is essential to protect sensitive biometric data. Traditional wireless methods are vulnerable to interception, particularly in scenarios where adversaries attempt to compromise the system through physical proximity or direct interaction with the body. Two primary threat models are considered:

- Over-the-Air (OTA) attacks: the adversary places external antennas in the vicinity of the subject and attempts to intercept, inject, or modify wireless signals.
- Direct contact attacks: the adversary physically connects a pair of electrodes to the subject's body and transmits falsified data to the receiver.

To counter these threats, the proposed system integrates biometric authentication directly into the physical communication layer. The approach leverages the subject-specific nature of the GC propagation channel, which is influenced by physiological factors such as tissue composition, body geometry, and electrode placement. This results in a transmission path that is unique and stable over time, making it difficult to replicate or spoof.

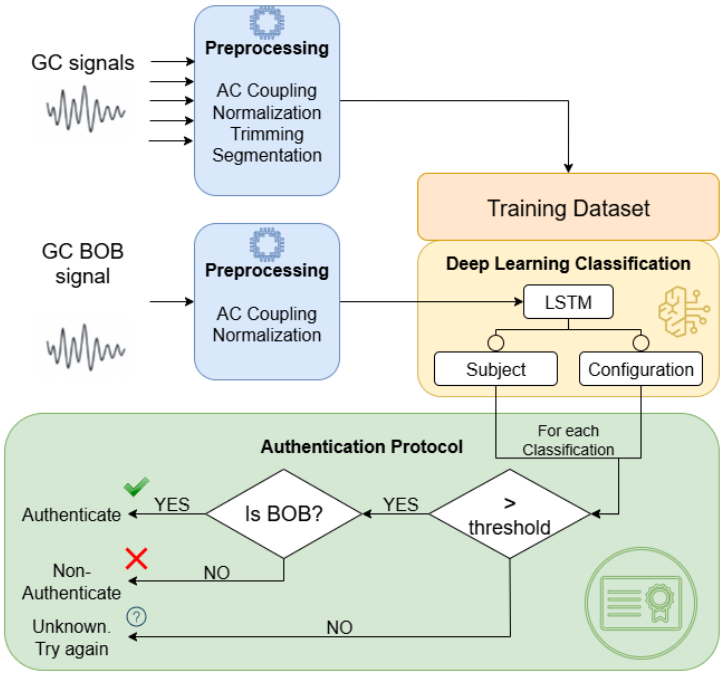


Fig. 1: Architecture of proposed authentication system

The authentication framework is designed to operate in on-body configurations, such as communication between a wearable or implantable sensor and a GC-enabled smartwatch receiver. It consists of two neural network classifiers:

- A subject classifier, which identifies the individual transmitting the signal, ensuring protection against OTA attacks by verifying the identity regardless of electrode placement.
- A configuration classifier, which determines the distance between electrodes, enabling detection of anomalies in electrode setup and mitigating direct contact attacks.

The following subsections describe the signal processing pipeline, the architecture of the deep learning models for classification, and the authentication protocol, which is designed to operate efficiently in low-resource medical environments, as shown in Fig. 1.

2.1 GC Signal Dataset for Neural Network

To enable biometric authentication based on GC signals, the raw data acquired during the experimental campaign is preprocessed and structured into a dataset suitable for training and evaluating a neural network classifier. The preprocessing pipeline is designed to preserve subject-specific signal characteristics while removing irrelevant or misleading components.

The first step involves removing the DC component from the acquired signal. This is achieved by applying AC coupling to the entire signal packet, effectively centering the signal around zero and eliminating any baseline offset introduced by the acquisition system. This ensures that only the dynamic variations of the signal are retained, which are more informative for classification.

Next, the signal is normalized with respect to its maximum absolute value. This operation scales the signal to the range $[-1, 1]$, removing amplitude variations caused by path loss and electrode placement. While path loss is a prominent and easily distinguishable feature, it is also the most vulnerable to estimation by an eavesdropper. By eliminating this dependency, the classifier is forced to rely on more subtle and robust features embedded in the signal structure.

The third step consists of trimming the signal to exclude portions where no transmission occurred. These segments contain only noise and do not contribute meaningful information for authentication. Removing them improves the signal-to-noise ratio and ensures the dataset contains only relevant samples.

The cleaned signal is then segmented into fixed-length portions of 100 samples, without overlap between segments. This segmentation allows the neural network to process consistent input sizes and facilitates batch training. Each segment is treated as an independent sample, capturing a snapshot of the GC signal under specific conditions.

Finally, each signal segment is annotated with two labels: one indicating the electrode configuration used during acquisition, and the other identifying

the subject. This dual-labeling enables the network to learn both configuration-specific and subject-specific patterns, supporting evaluation of classification performance across different experimental setups.

2.2 Deep Learning Classifier

Recurrent Neural Networks (RNNs) are a class of artificial neural networks designed to process sequential data. Unlike feedforward networks, RNNs include internal memory states that allow them to retain information across time steps. This temporal structure enables RNNs to model dynamic behaviours and dependencies in time-series data, making them particularly suitable for tasks such as speech recognition, handwriting analysis, and physiological signal processing.

LSTM networks are a specialized type of RNN designed to overcome the limitations of standard RNNs, such as vanishing or exploding gradients. LSTMs introduce memory cells and gating mechanisms that regulate the flow of information, enabling the network to learn long-term dependencies more effectively. This makes LSTMs particularly well-suited for analysing biomedical signals like GC, where subtle temporal patterns may carry subject-specific information useful for authentication.

The LSTM network used in this work is designed to classify segments of GC signals into subject identities. The input to the network consists of signal segments of 100 samples, preprocessed as described in the previous section. The architecture includes a single LSTM layer with 120 hidden units, followed by fully connected layers and a final softmax output layer. The softmax layer outputs a probability distribution over the possible classes, corresponding to the subjects in the dataset.

The dataset used for training and evaluation consists of 72,840 signal segments. A random 90% of the dataset (70,416 segments) is used for training, while the remaining 10% (7,824 segments) is reserved for testing. This split ensures that the model is evaluated on unseen data, providing a reliable estimate of its generalization performance.

The network is trained using the Adam optimizer, which combines the advantages of adaptive learning rates and momentum. The learning rate is set to 0.002, and the model is trained for 200 epochs. The primary evaluation metric is classification accuracy, which measures the proportion of correctly identified signal segments. The training process is performed in batches, and early stopping is applied to prevent overfitting.

This architecture provides a balance between model complexity and computational efficiency, making it suitable for deployment on resource-constrained wearable devices. By learning directly from raw GC signals, the network avoids the need for handcrafted features and leverages the temporal dynamics of the signal for robust user authentication.

2.3 Authentication Protocol and Performance Evaluation

The authentication protocol is based on the output of two independent neural network classifiers. One classifier identifies the subject transmitting the signal, while the other determines the electrode configuration used during signal acquisition. Both networks operate on 100-sample GC signal segments and produce a probability distribution over their respective classes using a softmax activation function. The class associated with the highest probability is considered the most likely prediction.

However, in biometric authentication systems, a classification result alone may not be sufficient. A misclassification could be interpreted as a successful impersonation attempt. To mitigate this risk, the protocol introduces a confidence score threshold: if the highest predicted probability (i.e., the confidence score) does not exceed a predefined value θ, the system rejects the authentication attempt. This mechanism allows the system to respond with "uncertain" rather than forcing a potentially incorrect classification.

This threshold-based decision introduces a trade-off between responsiveness and security. Increasing θ improves the reliability of accepted predictions but leads to a higher rejection rate. Conversely, lowering θ increases the number of accepted segments but may reduce robustness against adversarial attacks. Given that each 100-sample segment corresponds to approximately 2 milliseconds of transmission time, the protocol can afford to discard uncertain segments and request retransmission without significantly impacting system performance.

To evaluate the effectiveness of the protocol, two key performance indicators are defined:

- Reliability: the proportion of signal segments that are accepted by the system, i.e., those for which the confidence score exceeds the threshold θ. It is defined as:
$$Reliability = \frac{N_{\text{accepted}}}{N_{\text{total}}},$$
where N_{accepted} is the number of segments with confidence score above θ, and N_{total} is the total number of transmitted segments.
- Security: the proportion of correctly classified segments among those that are accepted. It reflects the system's robustness against impersonation and is defined as:
$$Security = \frac{N_{\text{correct}}}{N_{\text{accepted}}},$$
where N_{correct} is the number of accepted segments that are correctly classified.

In the results section, the threshold θ is varied from 0 (inclusive) to 1 (exclusive) to analyse the trade-off between reliability and security, and to identify optimal operating points for different application scenarios.

3 Experimental Campaign

GC enables on-body communication by transmitting low-power alternating currents (below 1 mA) through biological tissues using surface electrodes. The signal is applied differentially between a pair of transmitting electrodes, while a pair of receiving electrodes detects the attenuated signal after propagation through the body. The human body acts as a conductive medium, allowing signal transmission in the frequency range of 1 kHz to 100 MHz.

In previous work [10], the GC channel was characterized through estimation of the Channel Impulse Response (CIR) for cryptographic key extraction. In contrast, the present study focuses on biometric authentication and directly uses the received signal segment as input to a classification model. This approach eliminates the need for channel estimation, reducing computational complexity and enabling faster processing suitable for real-time applications.

3.1 Measurement Setup and Experimental Protocol

The experimental platform (see Fig. 2) consists of two battery-powered laptops acting as transmitter (TX) and receiver (RX), connected via LINE OUT and LINE IN ports, respectively. Signal generation and acquisition are performed using MATLAB. The analog signal is transmitted through the TX sound card and injected into the body via two Ag/AgCl surface electrodes (PG10C, FIAB, CE-certified). The received signal is captured by two electrodes and digitized at 48 kHz with 16-bit resolution.

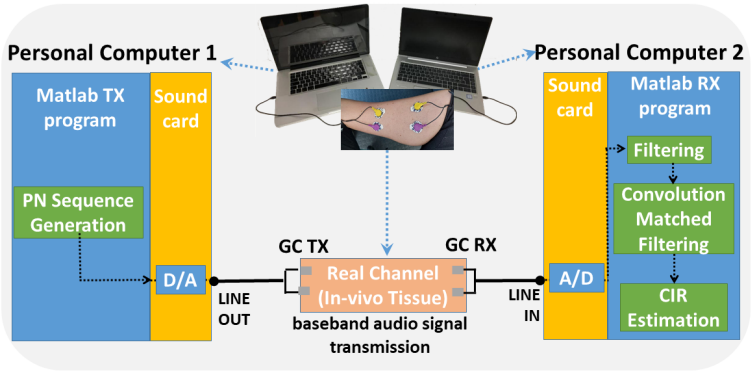


Fig. 2: Experimental setup for GC signal acquisition, showing the connection between transmitter and receiver, and the placement of electrodes on the forearm.

To ensure galvanic isolation and avoid shared ground paths, both laptops operate on battery power. A 50 Hz notch filter is applied to suppress power line interference. The transmitted signal is a pseudorandom noise (PN) sequence generated using a linear-feedback shift register, representative of arbitrary data exchanged between wearable devices.

Experiments were conducted on eight healthy volunteers (ages 24–30). Electrodes were placed on the inner forearm, with multiple configurations tested to evaluate signal variability. As illustrated in Fig. 3, the longitudinal distance (d_l) between TX and RX pairs was set to 3, 5, 10, and 15 cm, while the transverse distance (d_t) within each pair was 3 or 5 cm. Each configuration was repeated five times to ensure statistical consistency.

Before each test, the system was configured to ensure optimal signal transmission and acquisition. The following steps were followed:

- Cable connection: TX connected to LINE OUT, RX to LINE IN.
- Audio settings: LINE IN and LINE OUT volumes set to 80% of maximum; all other channels disabled.
- Format configuration: Both laptops set to "16-bit, 48000 Hz"; audio enhancements disabled.
- Power isolation: Laptops disconnected from power supply to avoid ground loops.
- Electrode placement: Electrodes applied to the skin with distances as specified.
- Transmission: RX software started approximately 2 seconds before TX to ensure synchronization.

If the signal was not properly acquired, the test was repeated. This procedure ensures consistent and reliable acquisition of GC signals for biometric analysis under controlled conditions.

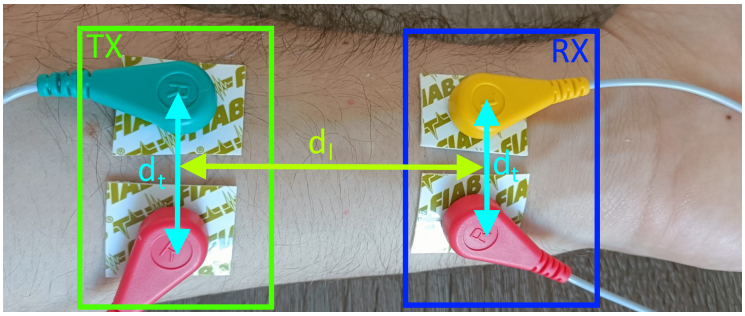


Fig. 3: Electrode placement scheme illustrating longitudinal distance (d_l) between TX and RX pairs, and transverse distance (d_t) within each pair.

4 Numerical Results and Discussion

This section presents the performance evaluation of the proposed biometric authentication system based on GC signals. The analysis focuses on the system's ability to withstand two distinct threat models previously introduced: direct contact attacks, which are addressed through classification of the electrode configuration, and OTA attacks, mitigated by identifying the subject transmitting the signal.

For each scenario, the system's behaviour is studied by varying the confidence score threshold θ in the range $[0, 1)$, and observing how this affects the two key performance indicators: reliability and security. As defined earlier, reliability measures the proportion of signal segments accepted by the system, while security quantifies the accuracy of classification among those accepted segments.

To complement the analysis of these metrics, we also present confusion matrices for two representative operating conditions. The first corresponds to $\theta = 0$, where the confidence-based rejection mechanism is disabled and all segments are accepted. The second refers to the case where θ is set such that the system achieves a reliability of 0.8, meaning that 2 out of 10 segments are rejected.

4.1 Reliability and Security Performance for Contact Direct Attack

The evaluation of the system under the direct contact attack scenario focuses on its ability to correctly classify the electrode configuration used during signal acquisition. This classification is crucial to detect unauthorized physical connections to the body, where an adversary attempts to transmit falsified data by mimicking the legitimate electrode setup.

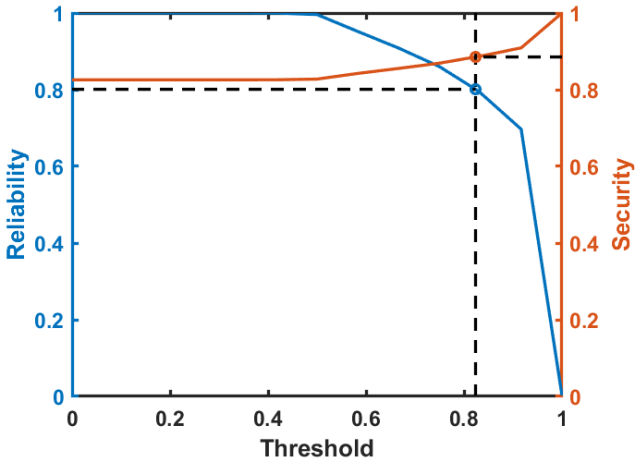
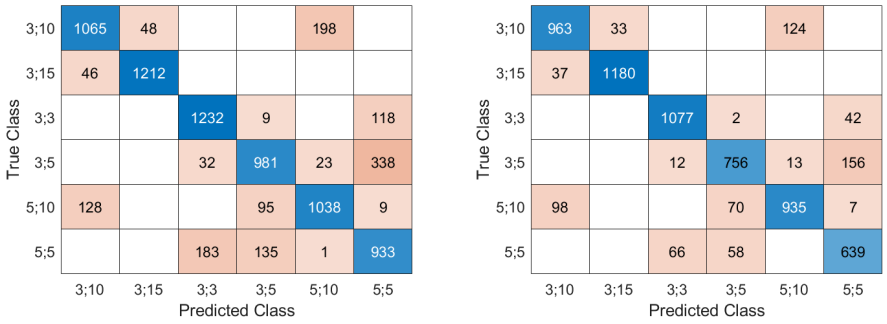


Fig. 4: Reliability and Security Performance

Figure 4 illustrates the behaviour of reliability and security as the confidence score threshold θ is varied. When the threshold is set to zero, meaning that all segments are accepted regardless of confidence, the system achieves a security of 82%. This indicates that even without any filtering, the classifier is able to correctly identify the configuration in the majority of cases. By increasing θ to a value that yields a reliability of 0.8, the security improves to 88%, showing that discarding low-confidence segments enhances the robustness of the classification. However, achieving perfect security (100%) requires setting θ so high that only 0.02% of the segments are accepted. Given that each segment corresponds to approximately 2 milliseconds of transmission time, this implies that authenticating with absolute certainty would require around 10 seconds of continuous transmission, which is impractical for real-time applications.



(a) Reliability = 100% (b) Reliability = 80%

Fig. 5: Confusion Matrix

Figure 5 provides further insight into the classification performance by comparing the confusion matrices for two operating points: $\theta = 0$ and the threshold corresponding to 80% reliability. In both cases, the system demonstrates high overall accuracy, but struggles to distinguish between configurations with similar electrode placements. Misclassification events are more frequent when the longitudinal and transverse distances between electrodes are close, suggesting that the signal features become less discriminative in these conditions.

Despite these limitations, the authentication system remains effective in detecting adversarial configurations, provided that the attacker is not positioned too close to the legitimate transmitter. The results confirm that the GC signal retains sufficient spatial sensitivity to support configuration-based authentication, especially when low-confidence segments are filtered out.

4.2 Reliability and Security Performance for OTA Attack

In the context of OTA attacks, the authentication system is evaluated based on its ability to correctly identify the subject transmitting the GC signal. This

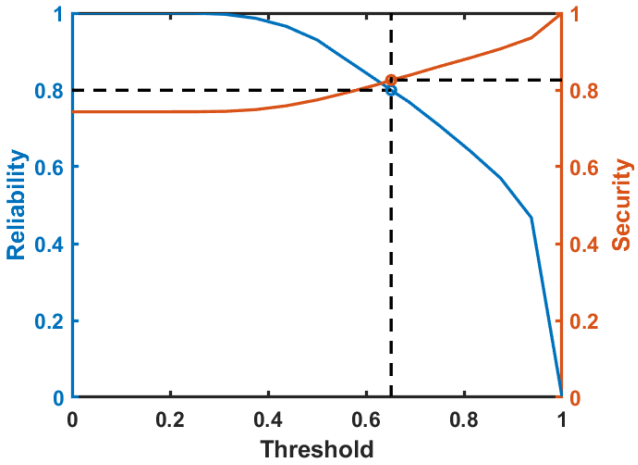


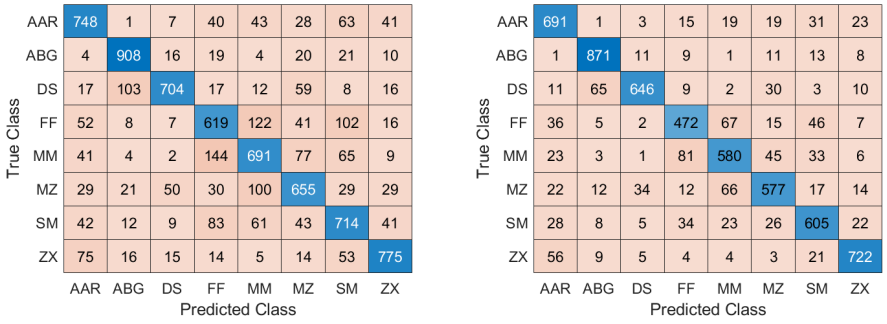
Fig. 6: Reliability and Security Performance

classification is essential to prevent adversaries from impersonating legitimate users by injecting signals wirelessly through their own GC transmission channel.

Figure 6 shows the variation of reliability and security as the confidence score threshold θ increases. When the threshold is set to zero, meaning that all segments are accepted, the system achieves a security of 74%. This baseline performance indicates that the classifier is able to distinguish users with reasonable accuracy even without filtering. By increasing θ to a value that yields a reliability of 0.8, the security improves to 82%, confirming that discarding low-confidence segments enhances the system's resistance to impersonation. As in the previous scenario, achieving perfect security (100%) requires a threshold so strict that only 0.02% of the segments are accepted, resulting in an impractical authentication time of approximately 10 seconds.

The confusion matrices in Figure 7 provide additional insight into the classification behavior. Unlike the direct contact attack scenario, where errors are concentrated among similar configurations, the misclassifications in the OTA case are more evenly distributed across the matrix. As the threshold increases from 0 to the value corresponding to 80% reliability, the number of errors gradually decreases across all classes. This suggests that the classifier is able to refine its predictions uniformly, without being disproportionately affected by specific subject pairs.

Although some subjects exhibit signal characteristics that are more similar to others—leading to occasional misclassifications—the differences are less pronounced than in the configuration classification task. Overall, the system demonstrates strong discriminative capability in identifying users, and the use of a confidence-based rejection mechanism significantly improves its robustness against OTA attacks.



(a) Reliability = 100% (b) Reliability = 80%

Fig. 7: Confusion Matrix

5 Conclusion and Future Directions

This work presents a physical-layer biometric authentication framework for BANs based on GC signals. By leveraging a deep LSTM network trained on raw GC data, the system successfully exploits the subject-specific features of the propagation channel, providing robust protection against both direct contact and over-the-air attacks. Experimental results confirm that the confidence-based rejection mechanism significantly improves security while maintaining acceptable reliability, making the approach suitable for real-time applications in medical environments.

Future work will focus on expanding the experimental dataset to include a larger and more diverse subject population, improving generalization and reducing bias. Additional research will explore the integration of multimodal biometric features and adaptive thresholding techniques to dynamically balance security and usability.

Acknowledgments

This work was supported in part by the Italian Ministry of Foreign Affairs and International Cooperation, grant number US23GR04 (CUP: D43C23000350001). This work was also partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART"), by the European Telecommunication Standard Institute (ETSI), Smart Body Area Networks (SmartBAN) Technical Committee, by the European Union's Horizon 2020 programme under grants No. 872752 and No. 101017331, and by Fondazione Cassa di Risparmio di Firenze (project: SmartHUB on Medical & Social ICT for Territorial Assistance).

References

1. A. Coviello, C. Cavigliano, V. Tasso, E. T. Tavassi, Y. Giacalone, and M. Magarini, "Emerging peripheral nerve injuries recovery: advanced nerve-cuff electrode model interface for implantable devices," in *2024 Global Conference on Wireless and Optical Technologies (GCWOT)*, pp. 1–7, IEEE, 2024.
2. L. Mucchi, S. Jayousi, A. Martinelli, S. Caputo, and P. Marcocci, "An overview of security threats, solutions and challenges in wbans for healthcare," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp. 1–6, IEEE, 2019.
3. Grand View Research, "Wearable medical devices market size, share & trends analysis report by product (diagnostic, therapeutic devices), by site (handheld, headband, strap, shoe sensors), by application, by region, and segment forecasts, 2025 - 2030." https://www.grandviewresearch.com/industry-analysis/wearable-medical-devices-market. Accessed: 2025-09-10.
4. T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*. Berlin/Heidelberg, Germany: Springer, 2009.
5. M. Obaidat, I. Trore, and I. Wougang, *Biometric-Based Physical and Cybersecurity Systems*. Berlin/Heidelberg, Germany: Springer, 2019.
6. L. Hernández-Álvarez, J. De Fuentes, L. González-Manzano, and L. Hernández Encinas, "Privacy-preserving sensor-based continuous authentication and user profiling: A review," *Sensors*, vol. 21, p. 92, 2021.
7. A. Vizziello, P. Savazzi, R. R. Guerra, and F. Dell'Acqua, "Experimental channel characterization of human body communication based on measured impulse response," *IEEE Transactions on Communications*, vol. 72, no. 7, pp. 3970–3984, 2024.
8. M. Swaminathan, A. Vizziello, D. Duong, P. Savazzi, and K. R. Chowdhury, "Beamforming in the body: Energy-efficient and collision-free communication for implants," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, IEEE, 2017.
9. W. J. Tomlinson, *Physical layer design and implementation of a biometric authentication system using galvanic coupling intra-body communication*. Ph.d. thesis, Northeastern University, 2018.
10. S. Caputo, A. Vizziello, A. Coviello, M. Magarini, S. Jayousi, P. Savazzi, and L. Mucchi, "Secret key extraction using galvanic coupling in wireless body area networks," in *2025 19th International Symposium on Medical Information and Communication Technology (ISMICT)*, 2025.
11. L. Shi, J. Yuan, S. Yu, and M. Li, "Ask-ban: authenticated secret key extraction utilizing channel characteristics for body area networks," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pp. 155–166, ACM, 2013.
12. L. Shi, J. Yuan, S. Yu, and M. Li, "Mask-ban: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 52–62, 2015.
13. J. Yuan, L. Shi, S. Yu, and M. Li, "Authenticated secret key extraction using channel characteristics for body area networks," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 1030–1032, ACM, 2012.
14. Q. Gui, Z. Jin, and W. Xu, "Exploring eeg-based biometrics for user identification and authentication," in *2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB)*, pp. 1–6, IEEE, 2014.

15. B. Kaur, D. Singh, and P. Roy, "A novel framework of eeg-based user identification by analyzing music-listening behavior," *Multimedia Tools and Applications*, vol. 76, pp. 25581–25602, 2017.
16. Q. Wu, Y. Zeng, C. Zhang, L. Tong, and B. Yan, "An eeg-based person authentication system with open-set capability combining eye blinking signals," *Sensors*, vol. 18, no. 11, p. 335, 2018.
17. T. Schons, G. Moreira, P. Silva, V. Coelho, and E. Luz, "Convolutional network for eeg-based biometric," in *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, pp. 601–608, Springer, 2018.
18. A. Bidgoly, H. Bidgoly, and Z. Arezoumand, "Towards a universal and privacy preserving eeg-based authentication system," *Scientific Reports*, vol. 21, pp. 1–12, 2022.
19. A. Valsaraj, I. Madala, N. Garg, M. Patil, and V. Baths, "Motor imagery based multimodal biometric user authentication system using eeg," in *2020 International Conference on Cyberworlds (CW)*, pp. 272–279, IEEE, 2020.
20. A. Zuquete, B. Quintela, and J. Cunha, "Biometric authentication using brain responses to visual stimuli," in *Third International Conference on Bio-inspired Systems and Signal Processing (BIOSIGNALS)*, pp. 103–112, 2010.
21. E. Gupta, M. Agarwal, and R. Sivakumar, "Blink to get in: Biometric authentication for mobile devices using eeg signals," in *2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2020.
22. L. Moctezuma and M. Molinas, "Multi-objective optimization for eeg channel selection and accurate intruder detection in an eeg-based subject identification system," *Scientific Reports*, vol. 10, p. 5850, 2020.
23. Y. e. a. Guo, "Epileptic seizure detection by cascading isolation forest-based anomaly screening and easyensemble," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 30, pp. 915–924, 2022.
24. S. Ketu and P. Mishra, "Hybrid classification model for eye state detection using electroencephalogram signals," *Cognitive Neurodynamics*, vol. 16, pp. 73–90, 2022.
25. V. Kumaravel, E. Farella, E. Parise, and M. Buiatti, "Near: An artifact removal pipeline for human newborn eeg data," *Developmental Cognitive Neuroscience*, vol. 54, pp. 1–14, 2022.
26. S. e. a. Saba-Sadiya, "Unsupervised eeg artifact detection and correction," *Frontiers in Digital Health*, vol. 2, p. 608920, 2021.
27. S. Chakravarthy and H. Rajaguru, "Effective breast tumor classification using k–strongest strength with local outlier factor algorithm," *International Journal of Aquatic Science*, vol. 12, pp. 1596–1603, 2021.