# Securing Hybrid Wireless Body Area Networks (HyWBAN): Advancements in Semantic Communications and Jamming Techniques

Simone Soderi[1](✉), Mariella Särestöniemi[2,3], Syifaul Fuada[3], Matti Hämäläinen[3], Marcos Katz[3], and Jari Iinatti[3]

[1] IMT School for Advanced Studies Lucca, Lucca, Italy
simone.soderi@imtlucca.it

[2] Health Sciences and Technology, Faculty of Medicine, University of Oulu, Oulu, Finland
mariella.sarestoniemi@oulu.fi

[3] Centre for Wireless Communications, Faculty of Information Technology and Electrical Engineering, University of Oulu, Oulu, Finland
{syifaul.fuada,matti.hamalainen,marcos.katz,jari.iinatti}@oulu.fi

**Abstract.** This paper explores novel strategies to strengthen the security of Hybrid Wireless Body Area Networks (HyWBANs), which are essential in smart healthcare and Internet of Things (IoT) applications. Recognizing the vulnerability of HyWBAN to sophisticated cyberattacks, we propose an innovative combination of semantic communications and jamming receivers. This dual-layered security mechanism protects against unauthorized access and data breaches, particularly in scenarios involving in-body to on-body communication channels. We conduct comprehensive laboratory measurements to understand hybrid (radio and optical) communication propagation through biological tissues. We utilize these insights to refine a dataset for training a Deep Learning (DL) model. These models, in turn, generate semantic concepts linked to cryptographic keys for enhanced data confidentiality and integrity using a jamming receiver. The proposed model significantly reduces energy consumption compared to traditional cryptographic methods, like Elliptic Curve Diffie-Hellman (ECDH), especially when supplemented with jamming. Our approach addresses the primary security concerns and sets the baseline for future secure biomedical communication systems advancements.

**Keywords:** Heterogeneous · WBAN · energy · security · optical · RF · near-infrared communications

## 1 Introduction

The advent of wireless and mobile communications technologies has been essential in enhancing healthcare, marking a paradigm shift towards more proactive

M. Särestöniemi et al. (Eds.): NCDHWS 2024, CCIS 2084, pp. 369–387, 2024.
https://doi.org/10.1007/978-3-031-59091-7_24

and personalized medical interventions. The concept of smart healthcare is at the forefront of this transformation, offering many opportunities to address the growing needs of an ageing population and the increasing prevalence of chronic diseases [1]. Remote health monitoring, a cornerstone of modern healthcare, has emerged as a cost-effective and efficient approach to disease prevention and healthcare provision, especially with the integration of 5G and 6G technologies. These advancements are pivotal in supporting in-body communications with implanted medical devices, enabling real-time health provisioning, virtual consultations, better diagnostics, and telesurgeries, among other benefits [1]. Historically, information transmission through biological tissues has predominantly relied on radio and acoustic waves [2]. However, these conventional methods are fraught with challenges, including security, safety, privacy, and interference, necessitating the exploration of alternative communications media. The vulnerabilities of implantable or in-body devices to hacks and unauthorized access have underscored the urgent need for enhanced security measures [3,4].

Optical Wireless Communications (OWC) has emerged as a promising alternative, utilizing light, especially in the near-infrared range, to transmit information through biological tissues. This method offers many advantages, including high security, privacy, safety and low complexity, as well as low power consumption. It has been used to successfully establish connectivity to electronic devices embedded under the skin [5]. Going further, a hybrid solution which is merging both radio-based and optical-based technologies in Wireless Body Area Network(WBAN) context can open a new, more secure way to implement personalized healthcare services and transfer personal health data. This is also a way to reduce radio signal emission towards the human body.

Hybrid Wireless Body Area Networks (HyWBANs) stand at the forefront of innovation in healthcare and Internet of Things (IoT) applications, merging radio and OWC. These networks offer remarkable advantages such as data throughput enhancement, enhanced security, and improved reliability, making them ideal for critical healthcare applications and various services, from patient monitoring to advanced diagnostics. Reconfigurable HyWBANs takes adaptability to the next level with a dynamic architecture, ensuring consistent performance in diverse environments. Preliminary studies on HyWBANs underscore their potential, showcasing notable performance and energy efficiency improvements [6]. Energy harvesting is crucial to HyWBANs [7], focusing on developing energy-autonomous nodes that enhance sustainability and reduce maintenance. The networks' advanced sensing capabilities support single and dual-mode sensing, enabling comprehensive data collection for diverse applications. Moreover, HyWBANs' design promotes sustainable operations, which is essential in today's environmentally conscious landscape. Optimized data transmission functionality in HyWBANs caters to the high demands of medical and IoT applications. A significant feature is the ability to transfer energy to in-body devices, ensuring continuous operation. Additionally, HyWBANs' advanced sensing capabilities are essential in medical diagnostics, allowing for detailed tissue analysis and health monitoring, thus revolutionizing healthcare and IoT applications [1].

Over the years, academia has shown interest in Physical Layer Security (PLS) solutions that aim to protect communications by exploiting the properties of the communication media [8–11]. These techniques consist of processing the signal sent over a channel in such a way as to obtain certain security properties without resorting to specific primitives, typically cryptography, offered by layers above the physical level. In this paper, we show how to combine PLS techniques with Deep Learning (DL) algorithms to improve the security of HyWBANs.

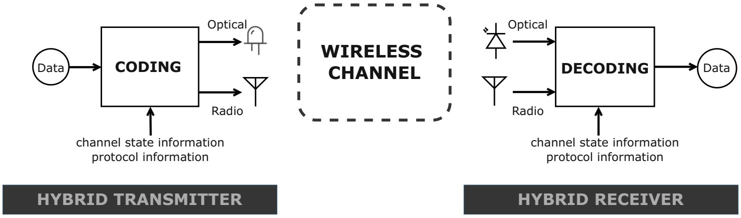


**Fig. 1.** Coding strategy for hybrid networks.

**Motivation.** In this article, we have decided to use a model already used in the literature that involves defining operating modes based on the combinations of the two communications channels [6,12]. Figure 1 depicts how hybrid radio-optical wireless networks utilize Shannon's theory, which defines the maximum channel capacity for communications. It shows the dynamic selection of the device's operating modes based on factors like channel state information (radio/optical) and user context. In our view, HyWBANs can improve *security* by integrating in the radio transmissions the OWC, which is known for the localised and secure transmission of signals. Encoding signals across radio and optical channels maximises secrecy, in line with recent theoretical work on conventional networks. This approach exploits the inherent security features of optical communications, addressing the vulnerabilities of WBANs. This paper uses data measured in the laboratory to implement an *innovative hybrid network security scheme* using semantic communications and intentional interference.

**Contribution.** In particular, hybrid communications have been of great interest for sensor networks. In a digital healthcare scenario, protecting these communications and doing so effectively while consuming as little energy as possible makes significance. The contributions of this article can be summarised as follows. *(i)* We present a novel concept that exploits the combination of Communications (SC) with a jamming receiver to improve the confidentiality and integrity of these wireless communications. *(ii)* We performed measurements in the laboratory to study the propagation of hybrid (radio and optical) communications in biological tissue. These measurements allowed us to define part of the dataset used for the DL model. Finally, *(iii)* we evaluated and performed a security analysis of the HyWBANs.

The remainder of the paper is organized as follows. Section 2 briefly recalls the concepts useful for understanding the paper. Section 3 discusses the major security threats in this scenario. Then, Sect. 4 presents the proposed scheme to enhance the security of hybrid networks. Section 5 presents the results achieved in terms of performance and energy cost. Finally, Sect. 6 concludes the paper by discussing our findings.

## 2 Background

This section introduces the radio and optical technologies used for wireless sensor communication. The aim is to provide some notions before discussing how hybrid networks combine these two technologies.

### 2.1 Radio-Based WBAN Technologies

WBAN is a way to link various wearable sensor nodes wirelessly into one individual and personalized network used to monitor a person's psycho-physiological vital signs. Depending on the need, the vital sensors can be distributed all around the human body. Low-power consumption, small size, and lightweight are the requirements set for the nodes to enable user acceptance. In principle, the amount of connected sensors within one WBAN can be high, but a realistic number is less than five for the sake of usability. The basic idea behind a WBAN is that dedicated sensors are collecting vital information and transmitting it wirelessly to the central node (called a hub), which then pre-process the data or conveys it further. Figure 2 shows the variability of the vital sensor nodes, which can be used in the WBAN context (the list of sensors is not exhaustive) [13]. In addition to sensors which are attached to the skin, so called on-body sensors, WBAN can utilize smart implants, such as pacemakers, or other in-body sensors/devices, such as Wireless Capsule Endoscope (WCE). In WBAN, all the nodes are connected to the on-body hub to enable real-time information transmission towards backbone infrastructure. Typically, WBAN is using a one-hop star network topology.

Currently, *de facto* wireless standard in WBAN is Bluetooth Low Energy (BLE) but there are also other dedicated WBAN standards available, such as ETSI SmartBAN [14], IEEE 802.15.6 [15], or IEEE 802.15.4 [16]. The latter one is better known via its higher layer protocols ZigBee and 6LoWPAN.

From a radio technology point-of-view, WBAN connectivity can be based on narrowband (NB) signals, which are used, e.g., in BLE and SmartBAN, or ultra wideband (UWB), which is adopted by [15]. The most common frequency band at the moment for NB signal is Industrial, Scientific and Medical (ISM) band at about 2.4 GHz. On the other hand, e.g., [15] defines several NB frequency bands for WBAN use also occupying sub-GHz frequencies. As operating in a highly populated frequency range, ISM band is typically subject to high interference originated from other radio equipment nearby. The selected frequency band, as well as signal bandwidth, also have an impact on the observed signal propagation properties through/along tissues, positioning accuracy, throughput, etc., depending on the application and use-case. If high resolution, real-time data is needed, then UWB can be the best option from radio-based technologies. Lower performance requirements and deeper in-body penetration, however, are favouring NB technology. Reference [15] also defines Human Body Communications(HBC) technology operating around 21 MHz, but this is omitted in this review due to its deviation from the conventional Radio Frequency (RF)-based communications as being a coupling-based solution.

The original network topology in WBAN is based on a star topology, where all the data flows are going through the central node, the hub. In this case, the hub is also a bridge from the body domain to the backbone network. The recent development, e.g., in ETSI SmartBAN has introduced and defined a hub-to-hub communications to transfer information between adjacent WBAN networks [17]. In addition, a two-hop relay functionality is included in the SmartBAN technical specification [18]. From the security viewpoint, all the hops between WBAN nodes, although being short, should be reliable but also secure as the communications chain is as reliable as its weakest link. This highlights the importance of light security protocols to be used also in the WBAN context.

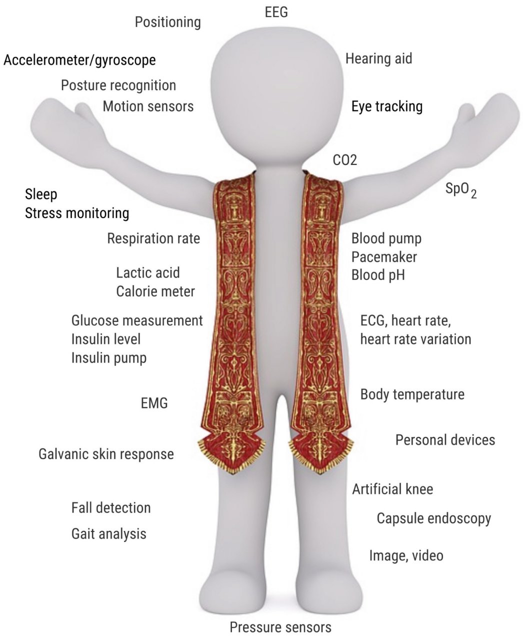


**Fig. 2.** Variability of the possible sensors that can be used in the WBAN context.

### 2.2 Optical Communications in Wireless Sensor Networks

The utilization of optical communications, including Visible Light Communication (VLC) and Infrared (IR) technologies, in wireless sensor networks is gaining interest for various IoT and body network applications. Optical communication offers security, bandwidth, and energy efficiency advantages, which are crucial for IoT deployments.

VLC utilizes Light Emitting Diodes (LED) to transmit data using the visible spectrum. This approach is inherently secure due to the limited light propagation and offers high data rates, making it suitable for indoor IoT applications [19]. VLC's potential in hybrid optical-wireless networks for next-generation communications, especially in 5G and beyond, is highlighted in [20]. IR communication leverages the non-visible spectrum for data transmission, offering benefits in terms of device miniaturization and reduced interference with existing RF systems. Its suitability for low-data-rate IoT applications, especially in hybrid networks combining IR and VLC, is explored in [7]. IR in hybrid radio-optical wireless networks offers innovative solutions for versatile IoT applications, as discussed in [21]. Integrating optical and wireless technologies in a hybrid framework opens new avenues for enhancing IoT network performance. The synergy of RF and optical communication technologies in hybrid networks is investigated in [22], which outlines the implementation and advantages of such an approach.

## 3 Security Analysis of HyWBANs

Developing next-generation networks to support better biomedical applications presents an opportunity. However, cyber-security risks arise mainly from this technology's highly interconnected and ubiquitous nature [1]. Therefore, the cybersecurity analysis of these hybrid communications begins with choosing a system model that best represents the problem.

WBANs are components of cyberspace that assist people in their daily activities and collect data from persons. WBANs and, more broadly, wearable wireless networks (WWNs) have three communication layers, according to the *tier model* [23]. As shown in Fig. 3, wearable sensors capture data in Tier 1 and transmit it to Tier 2 for aggregation and data processing. Finally, data is sent to Tier 3 and made available for remote access. The HyWBANs follow the same system model, where radio link, optical link, or both can be used for each type of communication in Tier 1 and Tier 2. As illustrated in Fig. 3, we have different types of communications in HyWBAN: on-body to in-body devices (labelled as *On-In*) and on-body to on-body (labelled as *On-On*) devices that operate in Tier 1. Instead, at Tier 2, all communications are off-body, including on-body to off-body devices (labelled *On-Off*). We assume that HyWBANs operate up to Tier 2, as depicted in Fig. 3.

One of the main security problems of this communication chain is that Eve, the adversary (attacker) shown in Fig. 3, can carry out several attacks. We can assume that she has complete control to intercept and modify all messages

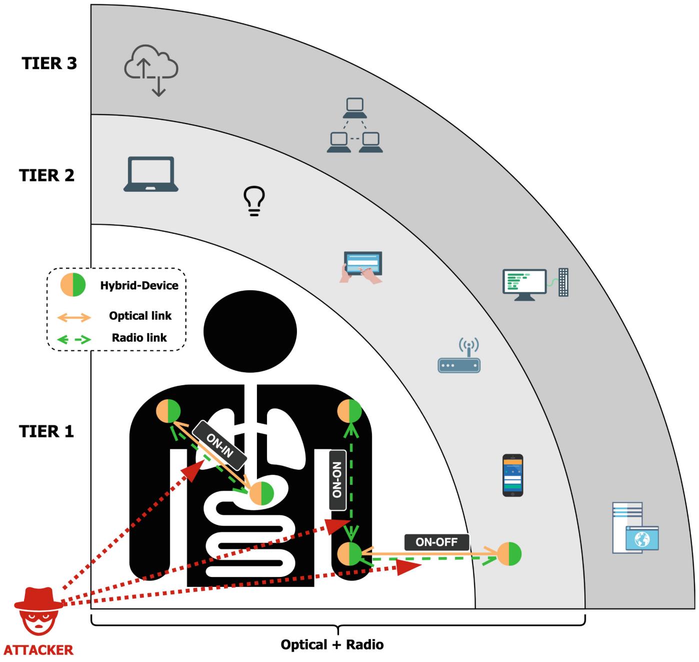


**Fig. 3.** Communications tiers system model, in which hybrid communications operate in the first two tiers.

exchanged between HyWBAN nodes [24]. In the rest of the paper, we analyse the possible attacks and their mitigation.

### 3.1 Security Threats Overview

The complexity of HyWBANs, which combines RF and OWC, far exceeds traditional communications systems due to their dual-channel nature. This sophistication poses significant challenges for attackers attempting to compromise the network, as they must navigate radio and optical channels.

In the HyWBANs domain, the security of communication channels is essential, especially when considering transmitting sensitive health data. This section delves into the nuanced vulnerabilities inherent to RF and OWC, laying the groundwork for understanding the superior security posture of optical communications in specific scenarios. RF communications, by their very nature, are susceptible to eavesdropping due to their omnidirectional signal propagation. This characteristic allows malicious entities to intercept signals without necessitating a direct line of sight, thereby posing a significant risk to the confidentiality of transmitted data. Conversely, optical communications demand a line-of-sight for effective transmission, inherently restricting the potential for unauthorized interception. Despite this advantage, optical channels are not impervious to secu-

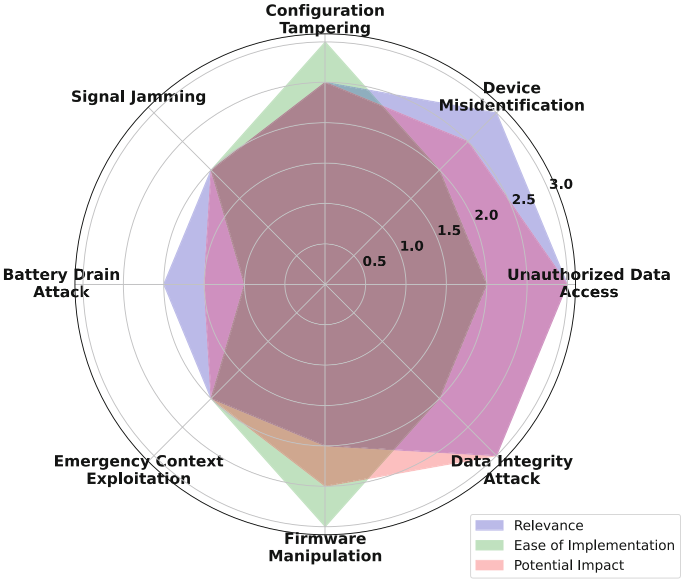


**Fig. 4.** Security threats to HyWBAN.

rity threats. A breach in the line-of-sight or sophisticated techniques to capture reflected optical signals can compromise data integrity and confidentiality.

In the context of HyWBANs, an attacker would primarily focus on tactics that enable eavesdropping on biomedical device communications. These tactics could include exploiting network security protocol vulnerabilities, conducting Man-in-the-Middle (MitM) attacks to intercept data, or using sophisticated techniques to bypass encryption. Reconnaissance plays a crucial role, as the attacker must gather detailed information about the network's configuration and security mechanisms to successfully deploy malware or other attack vectors.

Figure 4 presents a multifaceted evaluation of security threats in HyWBANs. Each threat is analyzed based on three critical dimensions: *relevance* to the network's security, *ease of implementation* by potential attackers, and the *potential impact* on network integrity and functionality. This brief assessment enables a slight understanding of each threat's effectiveness and helps prioritize security measures.

To fortify the security framework of HyWBANs against these vulnerabilities, we introduce a semantic communication method that significantly enhances the security of transmitted data.

## 4 Enhancing the Security of HyWBAN Through Semantic Communications

Understanding the implications for security in the dynamic landscape of HyWBANs is essential. Adversaries exploiting vulnerabilities in these networks could potentially gain unauthorized access to the human body, leading to critical threats like hijacking pacemakers, reconfiguring smart pill dispensers, or even creating novel types of diseases. The dual nature of these networks, encompassing radio and optical wireless channels, adds a layer of complexity to potential attacks. This study proposes a novel security mechanism combining the principles of semantic communications with the strategic deployment of a jamming receiver (see Fig. 5), enhancing the confidentiality and integrity of HyWBANs.

Semantic communications [25], an emerging paradigm in network security [26], involves generating semantic concepts related to biomedical applications or patient health status. This approach utilizes a DL model trained on a dataset comprising measured, augmented, and synthetic biological signals [1,27]. During an enrollment phase, assumed free from adversarial presence, each semantic concept is associated with a secret, such as a cryptographic key, stored in the nodes' memory.

The transmission of semantic concepts over the wireless channel, although susceptible to interception by malicious adversaries, is protected through a jamming receiver. As shown in Fig. 5, this receiver introduces intentional interference on either the light or radio channel, or both, effectively interfering with the transmitted data from the in-body device. Consequently, an adversary attempting to decode the data encounters altered signal characteristics, such as decreased Signal-to-Noise Ratio (SNR) for radio and input power for Near-Infrared (NIR) signals; this leads to an *erroneous classification of semantic concepts.*

However, the legitimate receiver, Bob, *knows the jamming pattern* and can reverse the artificially induced bias to correctly decode the transmitted semantic

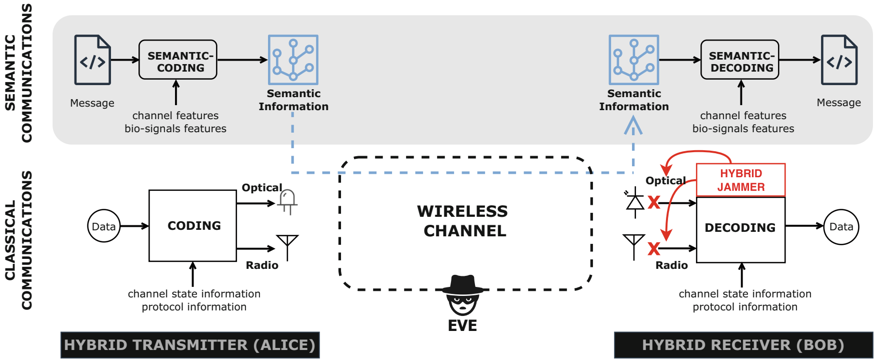


**Fig. 5.** AI-based data stream encoding in HyWBANs using semantic communications and a jamming receiver to harden the security of wireless communications.

concept. In contrast, an adversary, referred to as Eve, who lacks this knowledge, faces significant challenges in decoding the data accurately [9,11]. This approach, leveraging semantic communication and controlled jamming, offers a dual-layered defence mechanism, enhancing the resilience of HyWBANs against sophisticated cyber threats. The rest of the section describes how the data were prepared and how we propose to use a DL algorithm on devices with constrained resources.

### 4.1 Radio and Optical Channels Data Measurement

In this study, we investigate the efficacy of hybrid communications that utilize optical and radio channels, explicitly investigating their capacity to penetrate biological tissues. Two distinct experimental setups were designed to assess the performance characteristics necessary for effective and secure communications through such mediums. For optical communications, NIR frequencies were employed, selected for their proven proficiency in penetrating biological tissues. On the other hand, UWB technology, recognized for its superior transmission capabilities, particularly noise-like signals, was chosen for radio communications. This dual-faceted approach allows for a comprehensive evaluation of the potential of hybrid communication systems in medical applications.

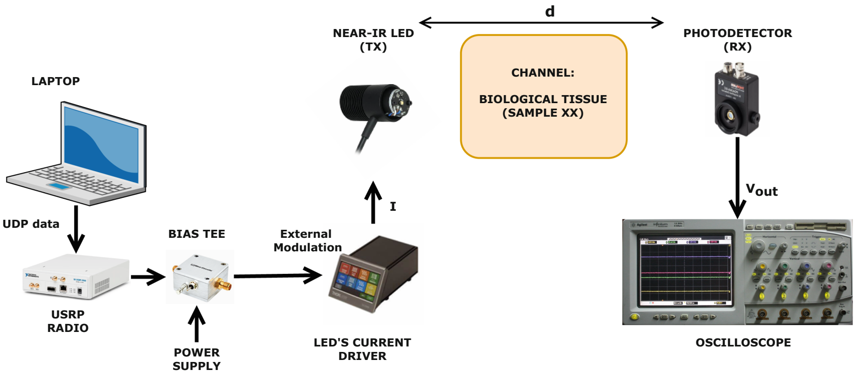


**Fig. 6.** Measurement set-up with NIR communications (as OWC) through the biological tissue.

The experimental setup, depicted in Fig. 6, is an optical communication part; it comprises various components that can be divided into two subsystems: transmitter and receiver front end. The transmitter unit includes a NIR LED (M810L3, THORLABS) with 810 nm wavelength, a bias-tee, and a LED driver. The receiver unit utilizes a Photo-Detector (PD) (PDA 36A-EC switchable gain detector, THORLABS). A sample of biological tissue was used, acting as the communications channel. The LED is driven by a current driver module (DC2200, THORLABS), which is controlled by an external modulation source.

The modulation of the NIR LED is essential for transmitting data through the biological tissue. The PD, positioned at a specific distance ($d$ is the thickness of the meat sample used in the measurements) from the NIR LED, captures the transmitted light after it has passed through the tissue. The output from the PD ($V_{out}$) is then analyzed using an oscilloscope (with 50 $\Omega$ impedance) to assess the effectiveness of data transmission through the tissue sample. Using a laptop, we sent the same ASCII character with the User Datagram Protocol (UDP) protocol to a software-defined radio USRP that modulated the signal before sending it to the LED driver. Two NI USRPs (2920 model) were employed in this study. We also used a bias-tee (ZFBT-4R2GW-FT+, Mini-Circuits) to combine the modulation signal and the bias current to feed the driver. We measured the peak of the received burst signal for each character sent from the laptop. The $V_{out}$ is then converted into an input power unit by using the equation provided in the datasheet of PDA36A-EC. This setup is crucial for evaluating the feasibility of NIR communications in scenarios where signals need to penetrate biological tissues, such as in implantable medical device applications.

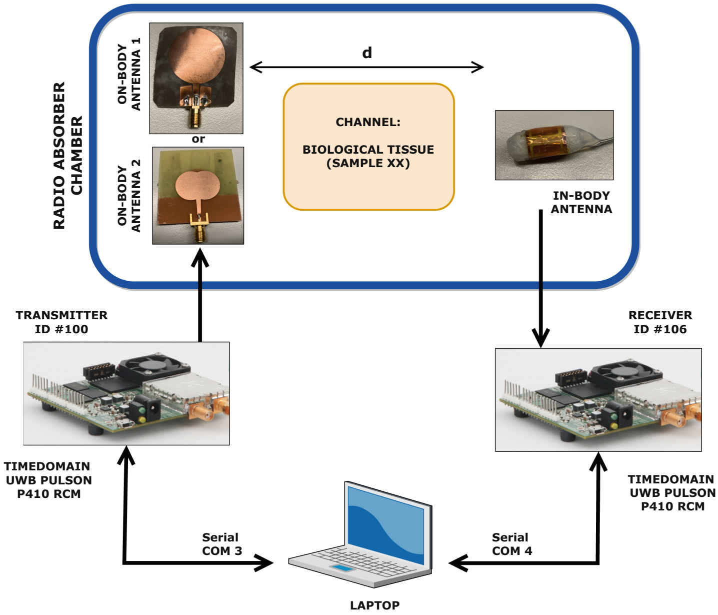


**Fig. 7.** Measurement set-up with UWB radio through the biological tissue.

As illustrated in Fig. 7, the radio measurement setup was meticulously designed to evaluate the performance of radio communications in HyWBANs. It consists of a UWB transmitter (P410 PulsON, Time Domain) inside the body (i.e., in-body device) that communicates with a UWB receiver (P410 PulsON, Time Domain) that has its antenna positioned on the porcine skin (i.e., on-body).

Using Time Domain's Channel Analysis Tool (CAT) software, we simulated the communications scenario inside the body by sending signals from the transmitter to the receiver. We enclosed the antennas inside a box of RF absorber material to avoid external interference. The received signals were saved on a laptop using CAT software and analyzed later using MATLAB. This system makes it possible to accurately measure the radio signal's capability to penetrate biological tissue and the effectiveness of UWB technology in an in-body communications scenario, essential for developing reliable hybrid WBANs.

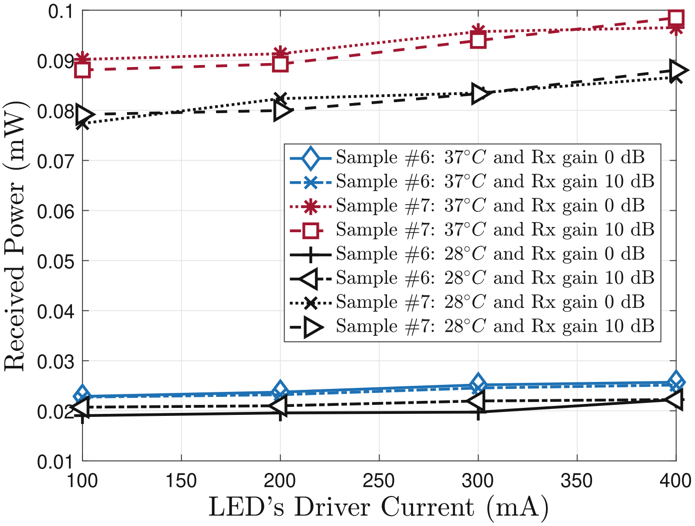
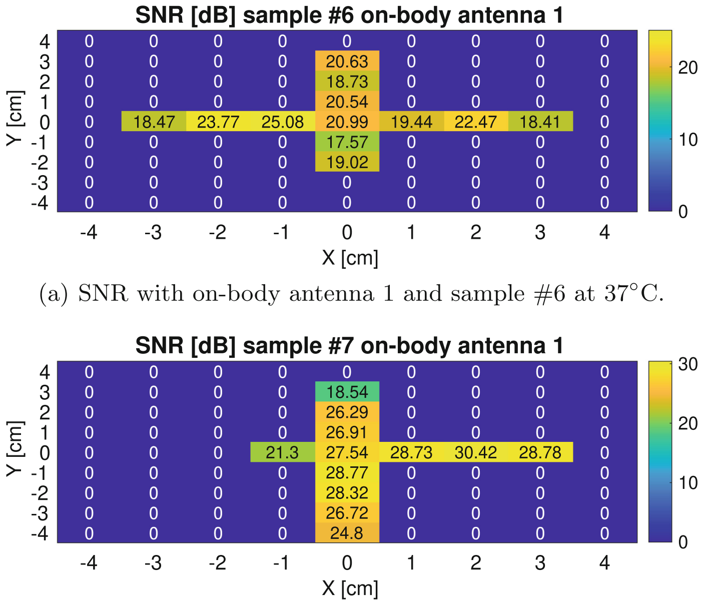


**Fig. 8.** NIR received power varying the temperature of two biological tissue samples (i.e., sample #6 and #7) and the gain of the PD .

Figure 8 shows the power (expressed in mW) of the NIR signal received after passing through the two biological tissue samples with a maximum thickness of 37 mm and 39 mm for samples #6 and #7, respectively. From Fig. 8, it is evident how the propagation capabilities improve when the temperature reaches 37°$C$, which is considered almost typical for a human body. Selecting a higher gain (i.e., from 0 dB to 10 dB) in the receiver (PDA 36A-EC offers this option using a rotary switch) does not lead to a significant advantage regarding receiver sensitivity.

Figure 9 shows the UWB SNR measured by the on-body antenna placed on the skin. Meanwhile, the transmitter and receiver were aligned for light. For the UWB measurements, we left the in-body antenna at the fixed position while we moved the on-body antenna in 1 cm steps to investigate the communication limit.



(a) SNR with on-body antenna 1 and sample #6 at 37°C.

(b) SNR with on-body antenna 1 and sample #7 at 37°C.

**Fig. 9.** SNR measurements of UWB transmissions through biological tissue.

### 4.2 Dataset: Measured and Synthetic Data for Medical Applications Using HyWBAN

Developing and optimizing semantic communications and strengthening security within hybrid networks necessitate a comprehensive dataset for training and testing DL models. This dataset encompasses both measured features, such as SNR and the power received by the PD in NIR communications, as well as synthetic features. These synthetic features are conceptualized on the premise that the constituent devices of HyWBAN can acquire and process biological signals from individuals. This dual approach in dataset formulation facilitates a realistic assessment of the HyWBAN's operational capabilities and aids in simulating a wide range of scenarios for advanced medical applications.

To refine the dataset for DL models in the context of HyWBANs for medical applications, we employed a dual-strategy approach involving both the *augmentation of measured data* and the *generation of synthetic data*. The augmentation process for the measured attributes, specifically SNR for UWB and received power for NIR, employs a statistical methodology in which new values are generated based on a Gaussian distribution. This distribution is centred on the measured mean and standard deviation. This statistical rigour ensures the augmented data are closely aligned with realistic measurement variations. We generated values for a few parameters: acceleration, heart rate and body temperature to generate synthetic data to emulate the ability of HyWBAN devices to measure biological signals. We assumed that a hybrid device could access these quantities (as a knowledge base for semantic communications) in a medical application or at least a part of it. These synthetic values are derived from a Gaussian distribution, adhering to predefined mean and standard deviations to ensure they fall within physiologically plausible ranges. The Table 1 summarises the specification of statistics for the data generation process. Our semantic communication model uses a binary classification approach, simplifying complex data into categories like 'HIGH_SNR' or 'LOW_SNR' using the thresholds defined in Table 1. This method efficiently filters out noise, focusing on key data aspects and significantly reducing computational load. This binary representation accelerates model training and enhances interpretability, facilitating fast and decisive communications analysis. We can then define the labels to be associated with each type of communication in a supervised manner (see Table 2). These labels are the *semantic concepts* that represent data the device measures in a compressed manner. This particular approach to dataset preparation supports the robustness of the developed models. It ensures the simulation of diverse scenarios, which is critical for applying HyWBAN in medical settings.

**Table 1.** Statistical summary of augmented and synthetic features.

| Feature | Mean | Stand. Deviation | [Min, Max] | Threshold |
|---|---|---|---|---|
| SNR (dB)[a] | 23.6 | 4.23 | [17.57, 33.32] | 19 dB |
| Input Power (mW)[b] | 0.07 | 0.03 | [0.02, 0.09] | 0.05 mW |
| Acceleration ($m/s^2$) | 0 | 0.1 | [-0.5, 0.5] | 0.1 $m/s^2$ |
| Heart Rate (bpm) | 60 | 25 | [50, 120] | <60 bpm, >110 bpm |
| Body Temperature (°C) | 36 | 2 | [34, 42] | 37°C |

[a] UWB measured data.

[b] NIR measured data.

**Table 2.** Classification labels for semantic communications

| Label | Condition |
|---|---|
| Full Communications | HIGH_SNR and HIGH_LPW |
| Wide Communications | HIGH_SNR and LOW_LPW |
| Communications in Motion | (HIGH_SNR or HIGH_LPW) and HIGH_ACC |
| Critical Communications | (HIGH_HR or HIGH_TMP) and LOW LPW |
| Unstable Communications | LOW_SNR or LOW_LPW |
| Reduced Communications | Other scenarios not covered by above conditions |

## 5 Proposed Model Evaluation

Our study developed a deep learning model for semantic communication in HyWBAN: an autoencoder with a $64 - 32 - 64$ neuron structure and a classification model with dense layers and dropout regularization. The purpose of the autoencoder model within our semantic analysis is to reduce the dimensionality of the input data, including SNR and heart rate, thereby enabling more efficient processing and transmission. The autoencoder helps identify the most significant features crucial for semantic analysis by transforming the data into a lower-dimensional space. This process not only aids in preserving essential information but also contributes to the system's security by minimizing the amount of data exposed to potential threats.

We have conducted a series of experiments to determine the optimal architecture for our model. Our choice was guided by a grid search approach, where we evaluated various configurations and selected the one that minimized the reconstruction error on a validation set: the 64-32-64 structure balanced model complexity and the ability to capture the underlying patterns in the data. We also experimented with different activation functions and learning rates, ultimately choosing a Rectified Linear Unit (ReLU) activation for its efficiency and a learning rate of 0.001 for stable convergence. The training process of our autoencoder was carried out over 50 epochs, with early stopping implemented to prevent overfitting. We used a batch size of 256, which was determined to be optimal through experimentation, balancing the trade-off between training speed and memory constraints. The dataset (after an augmentation of the data by a factor of 50) comprised 2040 samples, split into 80% for training and 20% for validation. This information aims to enhance the transparency and reproducibility of our model evaluation.

To visualize the effectiveness of the autoencoder in capturing semantic relationships, we apply the t-Distributed Stochastic Neighbor Embedding (t-SNE) technique (see Fig. 10). This method is noted for its ability to represent high-dimensional data in lower dimensions while preserving data structures, allowing us to visually inspect the clustering of data points based on their semantic similarities. We have expanded our discussion on the interpretability of clusters formed in the t-SNE visualization. The clusters represent distinct data patterns that the autoencoder has learned to encode. By examining the characteristics of samples within each cluster, we can infer the model's ability to discern different features in the data, which supports its effectiveness.

The model is optimized using *Adam* optimizer and trained to categorize the data into predefined semantic classes, as described in our data preprocessing phase. Performance evaluation using a confusion matrix and accuracy metrics confirmed the model's efficacy. Finally, the model was converted to *TensorFlow Lite* [28] (i.e., a Tiny Machine Learning framework that supports the conversion of ML models into a format that can be run on microcontrollers), aligning with low-power, edge-based IoT device requirements, ensuring privacy, energy efficiency, and real-time processing. This approach signifies a substantial advancement in semantic communication for smart healthcare applications.

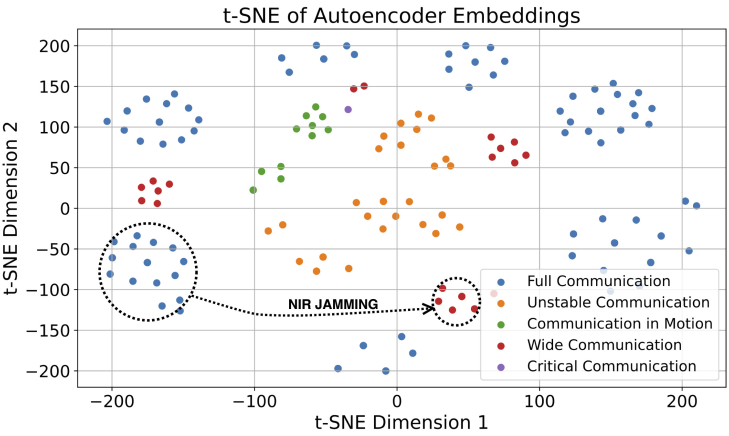


**Fig. 10.** Low-dimensional representation of data preserving semantic similarities. For example, the figure shows the effect of NIR jamming on the semantic concepts.

In our evaluation, we compared the energy efficiency of our semantic communication with a jamming solution to the Elliptic Curve Diffie-Hellman (ECDH) key exchange [29]. The comparison focused on various configurations, assessing the energy consumption for different key lengths in ECDH (160 and 256 bits) against our semantic communication model that can use 8 or 16 bits to represent the semantic concepts, and it is enhanced with jamming up to 8 and 16 bits (i.e., worst case for our proposal). We assumed 0.1 $\mu$J as the energy per bit and 0.2 $\mu$J as the energy cost to jam a bit. This analysis, crucial for understanding the practicality of deploying these methods in energy-constrained environments like HyWBANs, is visualized Fig. 11, illustrating the total energy consumption of each method. Such comparisons highlight the efficiency of semantic communi-

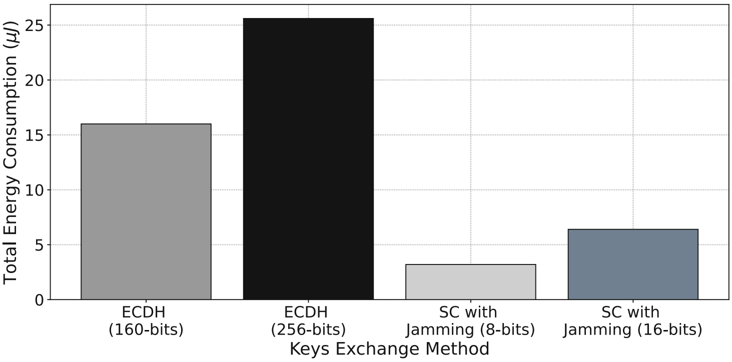


**Fig. 11.** Energy consumption comparison between SC with jamming and ECDH.

cations, especially when supplemented with jamming, in contrast to traditional cryptographic approaches like ECDH.

The classification performance of our TensorFlow model for semantic communication in HyWBANs demonstrated good precision and recall across most classes, with an overall accuracy of 94%. However, the corresponding TensorFlow Lite model, optimized for low-power devices, showed a variation in performance, particularly in precision and recall for specific communication classes like *Communication in Motion* and *Critical Communication*, resulting in an overall accuracy of 86%. This variation underscores the challenges in collecting more data with measurements and balancing model complexity with the constraints of edge computing devices.

## 6 Conclusions

The research presented in this paper marks a significant stride in enhancing the security of HyWBANs. By integrating semantic communications with jamming receivers, we demonstrate a robust method to protect sensitive health data and biomedical devices within the HyWBANs framework. Our experimental analysis provides valuable insights into the propagation characteristics of hybrid communications in biological tissues, forming the basis for an advanced DL model. This model's ability to generate and interpret semantic concepts, coupled with a strategic jamming mechanism, ensures the reliable transmission of encrypted data, thereby mitigating potential cybersecurity threats. Notably, our approach outperforms traditional cryptographic methods in energy efficiency, making it a viable solution for the energy-sensitive environment of HyWBANs.

The semantic strategy enhances security by transmitting only the necessary and relevant data, reducing the attack surface. The deep learning model contributes to this by learning to identify and filter out non-essential information, thus streamlining the communication process and making it more secure. The inherent security advantages of optical communications, such as the line-of-sight requirement for the interception, are exploited in our hybrid system to strengthen overall security further.

The findings and methodologies outlined in this study improve the security of current HyWBAN systems and pave the way for their broader adoption in smart healthcare services, aligning with the evolving landscape of 6G technology.

**Acknowledgments.** This research is partially funded by the Research Council of Finland Profi6 funded 6G Enabling Sustainable Society (University of Oulu) and Research Council of Finland 6G Flagship (grant 318927). and the European Union's Horizon 2020 programme under the Marie Sklodowska-Curie grant H2020-MSCA-RISE-2019 agreement No. 872752.

## References

1. Batista, E., Lopez-Aguilar, P., Solanas, A.: Smart health in the 6G Era: bringing security to future smart health services. IEEE Commun. Mag. 1–7 (2023)
2. Ahmed, I., Halder, S., Bykov, A., Popov, A., Meglinski, I.V., Katz, M.: In-body communications exploiting light: A proof-of-concept study using ex vivo tissue samples. IEEE Access **8**, 190378–190389 (2020)
3. Zafar, S., et al.: A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things. IEEE Access **9**, 93529–93566 (2021)
4. Ransford, B., et al.: Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. Pacing Clin. Electrophysiol. **40**(8), 913–917 (2017)
5. Halder, S., Särestöniemi, M., Ahmed, I., Katz, M.: Providing connectivity to implanted electronics devices: experimental results on optical communications over biological tissues with comparisons against UWB. In: Alam, M.M., Hämäläinen, M., Mucchi, L., Niazi, I.K., Le Moullec, Y. (eds.) BODYNETS 2020. LNICST, vol. 330, pp. 3–17. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64991-3_1
6. Saud, M.S., Ahmed, I., Kumpuniemi, T., Katz, M.: Reconfigurable optical-radio wireless networks: meeting the most stringent requirements of future communication systems. Trans. Emerg. Telecommun. Technol. **30**(2), e3562 (2019). https://doi.org/10.1002/ett.3562
7. Kamalakis, T., Ghassemlooy, Z., Zvanovec, S., Nero Alves, L.: Analysis and simulation of a hybrid visible-light/infrared optical wireless network for IoT applications. J. Opt. Commun. Netw. **14**(3), 69–78 (2022)
8. Bloch, M., Barros, J.: Physical-Layer Security: from Information Theory to Security Engineering. Cambridge University Press, Cambridge (2011)
9. Soderi, S., Mucchi, L., Hämäläinen, M., Piva, A., Iinatti, J.: Physical layer security based on spread-spectrum watermarking and jamming receiver. Trans. Emerg. Telecommun. Technol. **28**(7), e3142 (2017)
10. Soderi, S., Dainelli, G., Iinatti, J., Hämäläinen, M.: Signal fingerprinting in cognitive wireless networks. In: 2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), pp. 266–270 (2014)
11. Soderi, S., De Nicola, R.: 6G networks physical layer security using RGB visible light communications. IEEE Access **10**, 5482–5496 (2022)
12. Katz, M., Ahmed, I.: Opportunities and challenges for visible light communications in 6G. In: 2020 2nd 6G Wireless Summit (6G SUMMIT), pp. 1–5 (2020)
13. Hämäläinen, M., et al.: Recent Progress in ETSI TC SmartBAN Standardization. In: 2023 IEEE 17th International Symposium on Medical Information and Communication Technology (ISMICT), pp. 1–6 (2023)
14. Hämäläinen, M., et al.: ETSI SmartBAN architecture: the global vision for smart body area networks. IEEE Access **8**, 150611–150625 (2020)
15. IEEE Computer Society: IEEE standard for local and metropolitan area networks - part 15.6: Wireless body area networks. IEEE standard (2012)
16. IEEE Computer Society: IEEE standard for low-rate wireless networks. IEEE standard (2015)
17. ETSI Tc SmartBAN: Smart body area network (SmartBAN) Hub to Hub communication for SmartBAN medium access control (MAC). ETSI standard TS **103**, 806 (2023)

18. ETSI Tc SmartBAN: Smart body area network (SmartBAN) Relay functionality for SmartBAN medium access control (MAC). ETSI standard TS 103, 805 (2024)
19. Perera, A., Katz, M., Godaliyadda, R., Häkkinen, J., Strömmer, E.: Light-based internet of things: implementation of an optically connected energy-autonomous node. In: 2021 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–7 (2021)
20. Chowdhury, M.Z., Hasan, M.K., Shahjalal, M., Hossan, M.T., Min Jang, Y.: Optical wireless hybrid networks for 5g and beyond communications. In: 2018 International Conference on Information and Communication Technology Convergence (ICTC), pp. 709–712 (2018)
21. Teli, S.R., et al.: Hybrid optical wireless communication for versatile IoT applications: data rate improvement and analysis. IEEE Access **11**, 55107–55116 (2023)
22. Saud, M.S., Chowdhury, H., Katz, M.: Heterogeneous software-defined networks: implementation of a hybrid radio-optical wireless network. In: 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6 (2017)
23. Otto, C., Milenković, A., Sanders, C., Jovanov, E.: System architecture of a wireless body area sensor network for ubiquitous health monitoring. J. Mob. Multimed. **1**(4), 307–326 (2005)
24. Dolev, D., Yao, A.: On the security of public key protocols. IEEE Trans. Inf. Theory **29**(2), 198–208 (1983)
25. Calvanese Strinati, E., Barbarossa, S.: 6G networks: beyond Shannon towards semantic and goal-oriented communications. Comput. Netw. **190**, 107930 (2021). https://www.sciencedirect.com/science/article/pii/S1389128621000773
26. Du, H., Wang, J., Niyato, D., Kang, J., Xiong, Z., Guizani, M., Kim, D.I.: Rethinking wireless communication security in semantic internet of things. IEEE Wirel. Commun. **30**(3), 36–43 (2023)
27. Zafar, S., et al.: A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things. IEEE Access **9**, 93529–93566 (2021)
28. Dutta, D.L., Bharali, S.: TinyML meets IoT: a comprehensive survey. Internet Things. **16**, 100461 (2021). https://www.sciencedirect.com/science/article/pii/S2542660521001025
29. Stallings, W.: Cryptography and Network Security: Principles and Practice, 7th edn. Pearson Education Ltd., London (2017)