





Paper Type: Review Article

Security Analysis of Wireless Body Area Network Protocols: A Survey

Walid I. Khedr ^{1,2,*} , Aya Salama ¹ , Marwa M. Khashaba ¹  and Osama M. Elkomy ¹ 

¹ Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt.

Emails: wkhedr@fci.zu.edu.eg; ayasalama@fci.zu.edu.eg; mmkhashaba@fci.zu.edu.eg; omelkomy@fci.zu.edu.eg.

² College of Computer Science and Engineering, Taibah University, Saudi Arabia.

Received: 31 Aug 2023

Revised: 24 Nov 2023

Accepted: 25 Dec 2023

Published: 27 Dec 2023

Abstract

The Wireless Body Area Network (WBAN) has emerged as a transformative technology in the healthcare sector, particularly in the context of global health crises like pandemics, where the need for remote monitoring of patients is critical. WBANs consist of a network of sensors that are either worn on, implanted inside, or placed near the human body to continuously monitor a variety of physiological parameters, such as heart rate, blood pressure, and glucose levels. This continuous data collection enhances patient care by enabling healthcare providers to make more informed, timely decisions and interventions, even from remote locations. However, the transmission of such critical and sensitive data raises serious security concerns, as any compromise in the network could lead to dangerous consequences, including incorrect diagnoses or delayed treatment. To address these issues, this paper provides an extensive review of the recent advancements and research in WBANs, with a particular focus on the IEEE 802.15.6 standard, which governs communication protocols for these networks. The survey delves into the technical aspects of these protocols, identifying key vulnerabilities and proposing areas for improvement to ensure the security and reliability of data in WBANs. Additionally, the paper discusses the current challenges in safeguarding patient data and the potential risks posed by malicious attacks, offering insights into possible mitigation strategies that could enhance the robustness of WBAN security in real-world applications.

Keywords: WBAN; M2M; Security; IoT; IEEE 802.15.6; SDN; Blockchain; Big Data.

1 | Introduction

The Integrating the Big Data and Internet of Things (IoT) has significantly impacted the healthcare industry. One such technology is the Wireless Body Area Network (WBAN) is a type of a wireless sensor network (WSN) defined in IEEE 802.15.6. This network comprises sensors placed inside the body, on the body's surface, or at a distance ranging from several centimeters to five meters from the body. These sensors monitor vital signs and transmit data to caregivers, enabling patients to live independently and safely in their homes. WBANs have applications in both medical and non-medical fields [1-4]. Figure 1 below outlines the common applications that are associated with both of these domains.



Corresponding Author: wkhedr@fci.zu.edu.eg



Licensee International Journal of Computers and Informatics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

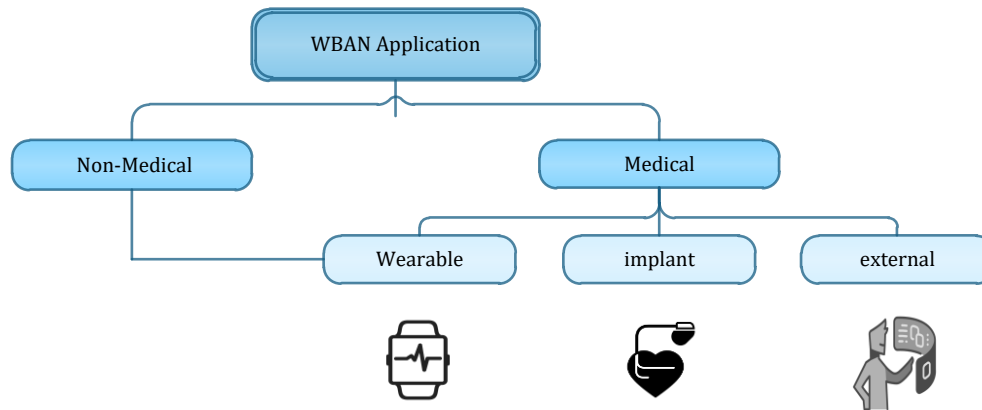


Figure 1. Classification sensors of WBAN.

WBANs have an important future for use in medical applications., proving beneficial to us in numerous routes. For example, Patients fitted with bio-sensors have complete freedom of movement, improving their mobility and reducing the number of patients requiring medical attention in a hospital setting. In addition, wireless body area networks can perform real-time health monitoring at any location and time, provide easy handling of queries and health care, and address issues related to aging and population growth by utilizing cutting-edge sensor components linked together topologically. Otherwise, protecting personal sensor data is a growing problem. Security and privacy are the two primary requirements to prevent illegal use in a WBAN system of information on the patient's related health. A WBAN system must fulfill both of these requirements. In the context of data collection, storage, transmission, processing, and usage, "security" refers to safeguarding sensitive information against unauthorized access at each stage. On the other hand, it refers to regulating the gathering and use of private information to prevent such information from entering the hands of unauthorized parties.

With the WBAN system, an attacker must be unable to get information on a patient that is both mission-critical and relevant to their health. If they leak, corrupt, or abuse the information, it might lead to embarrassing situations, job loss, mental disturbances, improper medication, bad treatment, or toxic relationships. Privacy is necessary to secure the information about the patient's health; moreover, to minimize the potential of the patient obtaining an inaccurate diagnosis as a consequence of data distortion (which, in the worst possible scenario, might kill the patient); it is essential to protect the data.

So, precautions need to be taken to protect sensitive and important patient information and to protect the patient's right to privacy and safety. For the system to work well, it is very important to stop these kinds of attacks from happening, and it employs numerous security techniques and processes to keep it safe from all the attacks a hacker has made. Moreover, authentication is necessary to ensure the confidentiality of the data since it limits the sensed data's arrival to the entities themselves that have been permitted to do so. Authenticating someone or something involves determining whether or not the claims made about that person or thing are accurate. The first stage in the WBAN process is authentication, which is unquestionably a crucial component of the system to protect the patient's information and maintain their privacy. Without authentication, unauthorized WBAN users of the system may be able to see private information about patients and make changes or additions that could lead to a missed diagnosis. Data authentication is essential for the coordinator and the WBAN nodes since both organizations need to verify that the data is delivered by a trusted organization [2].

The publication is formally organized as follows: Section 2 presents related work of recent research in WBN; Section 3 provides a brief background on WBAN architecture; Section 4 presents needs for the security system of WBAN, addition to threats; Section 5 discusses the security of the WBAN IEEE 802.15.6 Standard and protocols along with some security issues; Section 6 indicates the future direction of research integration of machine learning, SDN, Block Chain, and other trends; and Section 7 provides a conclusion.

2 | Related Work

Several surveys have been conducted in recent years, which are listed in Table 1. The authentication and security features of WBAN are the main topics of this research. For example, [5] conducted an assessment of the security concerns of WBAN; the authors focused on elaborating on the many uses, security and privacy basics, security risks, and practical solutions now in use. [6] Conducted a comprehensive analysis of the major security services and proposed several architectural suggestions for WBAN. Overall, the study aimed to offer a holistic perspective on the level of security present throughout the entire WBAN system.

Table 1. Comparison of the existing surveys discussed security in WBAN.

Subject of Surveys	Year	IEEE 802.15.6 protocols	Project	Architecture	Security	Attack	Attacker	Analysis	Open issues	Future work
[14]	2009			√	√	√				
[15]	2011				√	√				
[16]	2013			√				√		
[17]	2013			√	√	√			√	
[18]	2013			√	√					
[19]	2015				√	√				√
[20]	2016			√		√		√		
[21]	2016			√	√					
[22]	2017				√					
[23]	2017			√	√				√	√
[18]	2017			√	√	√			√	
[24]	2017			√						
[25]	2018			√	√	√		√		
[26]	2018			√	√	√				√
[27]	2018			√	√	√				
[5]	2018			√	√	√				
[6]	2018			√	√	√			√	
[7]	2018			√	√	√				
[8]	2019			√	√	√	√			
[9]	2019			√	√	√				
[10]	2019			√		√				
[11]	2019			√	√					
[12]	2019				√	√		√		
[13]	2020		√	√		√				
[2]	2021		√	√	√	√	√	√	√	√
This paper	—	√	√	√	√	√	√	√	√	√

[7] Centered on ensuring the safety of intra-BAN communication and reaching a strong consensus. It provided a complete examination of the existing keys to landscape agreement systems. It categorized them as either the traditional, based value of the physiological key, based key of the secret, or the based key of hybrid schemes. In addition, a characterization of any class is provided, and an investigation is carried out on the impedance of BAN to a variety of different sorts of assaults. The article [8] provided an overview of WBAN as well as its applicability in a variety of different disciplines. They described the many distinct security issues, requirements, assaults, and existing solutions to counteract the attacks that are taking place at the various tiers of WBAN. [9] Studies on privacy and security in WBAN qualified attacks on security and models of security for collecting the data, transition, and levels of storage. In addition, the need for maintaining patients' privacy and the dependability of healthcare systems are evaluated. [10] Conducted an in-depth study of existing authentication methods to dissect their structure, features, and operation. They looked at communication standards and design difficulties in WBAN and outlined the authentication scheme design process. Additionally, the article proposes measures to ensure the key is secure throughout the key management

process. [11] The authors suggest a taxonomy that makes it easy to divide authentication techniques into four categories: the based value of the physiological, the based channel, the based proximity, and the based cryptographic. [12] Present a universal survey to evaluate systems of authentication and add more intelligence to each plan. Their security features, assaults, strengths, weaknesses, and performances have all been thoroughly discussed. This discussion has also been published. [13] Investigated the most pressing issues with privacy and safety in WSNs and WBANs. This study compares and contrasts the two networks concerning their capabilities, design, applications, and security risks. [2] A comprehensive analysis of several facets of WBAN and safety.

3 | WBAN Architecture

Every year, more and more people fall victim to chronic illnesses. These individuals have considerable medical needs due to frequent hospital and clinic readmissions. State-of-the-art in patient care is the smart healthcare system, which is always being refined to better serve patients. WBAN, in which various health-related apps are deployed, is one such field. While designing a WBAN-based smart health application, the autonomy and self-organization of the connected devices are a top priority. In the next part, a more in-depth introduction to WBAN is provided.

3.1 | Wireless Body Area Network Architecture

Three layers make up the WBAN architecture:

- Tier1: intra communication of WBAN, multiple sensors (nodes) used to send body signals to the personal server (hub) collected and vital classification data then transmitted to the gateway in tier2
- Tier2: inter WBAN communication, which is a link between WBAN and different network.
- Tier3: Beyond WBAN communication: store vital data and profile of the patient in the database DB server and create medical history used in treatment later accessed by authorized people (doctors, emergency, insurance companies ...etc.) [3, 28], The WBAN architecture as shown in Figure 2.

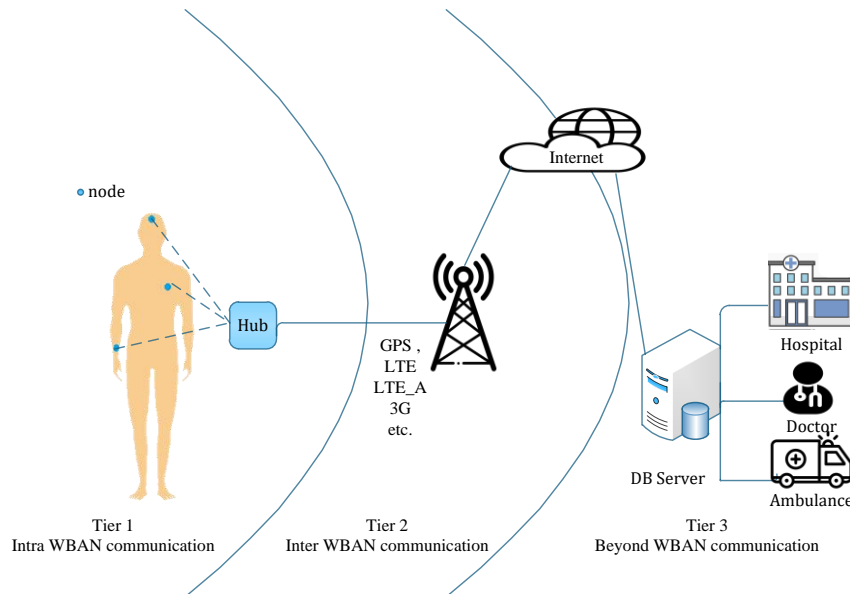


Figure 2. WBAN Architecture.

3.2 | Wireless Body Area Network Classification

A common example of WBAN sensor classification is shown in Table 2.

Table 2. Classification of WBAN examples.

Sensor Classification	Sensor Application	Sensor Examples
Wearable	On-Body Medical Application	ECG,SpO2, Blood Pressure
	On-Body Non-Medical Application	Social Networking , Music For Headset, Forgotten things Monitor
Implant	In Body Application	Glucose Sensor, Pacemaker end-scope, Capsule
External	Off-Body Application	Motion Sensor

3.3 | Wireless Body Area Network Communication

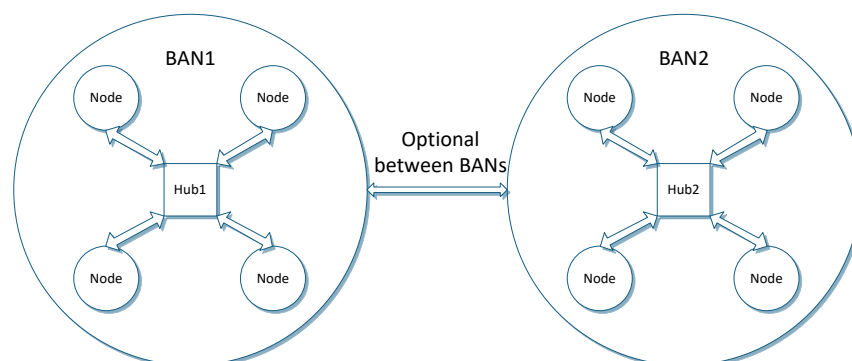
WBAN classifies as one of machine-to-machine M2M/IOT network in the healthcare sector; M2M devices can connect with a gateway used short-range communication network (IEEE 802.15.6, Bluetooth, ZigBee ...) Table 3 [6], from the gateway to DB server used long-range communication (LTE, LTE_A, Wimax) [4] This work primarily focused on short-range security challenges from an IEEE 802.15.6 perspective, which is evident if you are familiar with the WBAN architecture and have seen some application examples [7, 8].

Table 3. Communication used by WBAN.

Wireless Technology	Standard Adopted	Network Topology	Encryption	Authentication
Bluetooth	802.15.1	Piconet	E0 stream cipher	Shared Key
BLE	802.15.1	Star	AES block cipher	CBC-MAC
Zigbee	802.15.4	Mesh, a cluster tree, star	AES block cipher	CBC-MAC
IEEE 802.15.6	802.15.6	Star	Elliptic curve public key cryptography	AES-CCM
UWB	802.15.4a	Peer to Peer, Piconet	AES cipher CTR Counter Mode	CBC-MAC
Wi-Fi	802.11	Mesh	RC4 Stream Cipher	WPA2
Low Power Wi-Fi	802.11ah	Single Hop	128 bit AES	CBC-MAC
Ethernet	802.3/u/z/ab/an	Point-to-point, coaxial bus, star	Medium Access Control Security (MACSec)	Extensible Authentication Protocol (EAP)

3.4 | WBAN Topology

There are several nodes and one hub connected as star topology in one BAN, number of nodes from 0 to max size of BAN, in one-star node exchange frame directly with the hub; however, in two-hop star frame exchanges through relay cable node illustrated in Figure 3 [29].

**Figure 3.** Network topology.

3.5 | WBAN Layers

WBAN partition into the Physical layer (PHY), Medium Access Control (MAC) layer defined by IEEE 802.15.6, Network layer and Application layer defined by IEEE 802.15.4; many researchers focus on PHY/MAC IEEE 802.15.6 standard, but Network layer and Application layer have limited focus [30].

4 | WBAN Security

Despite the numerous benefits offered by WBANs, their open-access environment, portability, and design make them vulnerable to a wide range of security attacks. When proposing a new authentication scheme, most authors assess its security strength against various attacks, which are detailed below:

- **Data Sniffing/Eavesdropping:** This age-old security issue involves an attacker passively gaining access to data traffic between a WBAN node and the medical server by intercepting an unsecured network path. This can include critical health data, routing updates, and node ID numbers. Implementing random key distribution and strong encryption can ensure confidentiality and prevent sniffing.
- **Data Modification:** In this attack, an adversary alters or replaces data being transmitted among WBAN nodes, compromising data integrity. This can have severe consequences, especially if critical health data is falsified. Ensuring data origin authentication through digital signatures and keyed hash functions can prevent data modification.
- **Data Disclosure:** This attack compromises confidentiality and privacy by disclosing sensitive data to unauthorized entities. Access control and network layer encryption techniques are essential to prevent data disclosure.
- **Denial of Service (DoS):** This attack disrupts network availability by generating traffic beyond the network's capacity, thus denying services to WBAN users. Solutions include implementing authentication and anti-replay protection to mitigate DoS attacks.
- **Routing Attacks:** Here, an adversary poisons the routing table, directing packets to false destinations, causing severe network damage. Developing secure routing protocols and validation mechanisms can prevent routing attacks.
- **Masquerade/Impersonation/Spoofing:** An adversary impersonates a legitimate WBAN node to forge sensitive data or deceive the WBAN coordinator and other nodes. Using robust authentication mechanisms and intrusion detection can stop these attacks.
- **Replay:** In a replay attack, an attacker intercepts and retransmits legitimate messages to change the aggregate result. Nonces and time tokens can introduce fresh data to defend against replay attacks.
- **Node Subversion/Node Compromise:** An adversary captures a node, performs cryptanalysis to obtain stored data, and may input malicious data or extract vital health information. Minimizing stored data and frequently renewing secret keys, along with node revocation and tamper-proofing, can prevent node compromise.
- **Intrusion:** The adversary attempts to destabilize the network, gain unauthorized access, or exfiltrate data. Employing intrusion detection systems and secure group communication can mitigate intrusion attempts.
- **De-Synchronization:** This attack targets the transport layer by modifying authentic messages to create an infinite loop in the network. Packet authentication can defend against de-synchronization attacks.

- **Node Replication/Cloning Attack:** Following node subversion, an adversary may replicate a node's ID and reintroduce it into the network, gaining illegitimate access and injecting false data. Recognizing and revoking malicious nodes can resolve cloning attacks.

- **Attackers' Profile in WBAN**

Understanding the attacker's community, techniques, motives, extent, and targets is essential for addressing security and privacy issues in WBANs. The following profiles provide insight into potential attackers, shown as Table 4 :

- **Attack Community:**
 - **Internal Attackers:** Have some privileges and a thorough understanding of the system, enabling sophisticated attacks.
 - **External Attackers:** Treated as intruders with no administrative rights, they first gather information to carry out their attacks.
- **Attack Technique:**
 - **Active Attackers:** Intercept and alter information in wireless communications, causing significant damage.
 - **Passive Attackers:** Monitor the network to gain information without affecting it directly.
- **Attack Motive:**
 - **Malicious Attackers:** Aim to damage network operations without personal gain.
 - **Rational Attackers:** Driven by profit, their attacks are predictable based on their methods and targets.
- **Attack Extent:**
 - **Local Attackers:** Have a limited scope of attack.
 - **Extended Attackers:** Broaden their scope to control various entities within the network.

By understanding these profiles and implementing robust security measures, WBANs can better protect against potential threats and ensure secure, reliable healthcare data transmission [31].

Table 4. Common attacks on security.

Security Attacks	Compromised Services	Attack Community	Attack Technique	Attack Motive	Attack Extent	Attack Target
Data Modification	Authentication Availability Integrity Non-repudiation	Internal	Active	Rational	Extended	Hardware and Software
Denial of Service (DoS)	Authentication Availability Privacy	External	Active	Malicious	Extended	Infrastructure, Hardware, Software, Wireless interface
Eavesdropping	Confidentiality	Internal	Passive	Rational	Extended	Wireless interface
Impersonation / Masquerading	Authentication Integrity Non-Repudiation	Internal	Active	Rational	Local	Client wearing Sensors/ Infrastructure
Routing Attacks	Authentication Availability Confidentiality Integrity	Internal	Active	Malicious	Extended	Wireless interface
Replay attack	Authentication Integrity Non-repudiation	Internal	Active	Malicious	Extended	Hardware and Software

4.1 | Security Requirement

Security and privacy are critical components necessary to ensure the protection of sensitive and critical patient data. Security involves safeguarding data secrecy during transfer, storage, collection, and processing, while privacy focuses on preventing unauthorized usage and access to the data. Therefore, it is essential to provide robust security and privacy protections for patient-related information. This section provides a detailed overview of the security aspects required for WBANs.

- Security Essentials

To create a safe and reliable WBAN authentication scheme, it is essential to achieve the following security goals, which are commonly referenced by authors when designing such schemes:

- **Data Confidentiality:** Preventing data disclosure is vital to maintaining confidentiality. Adversaries may compromise WBAN nodes or capture transmission media, threatening confidentiality. Encryption methods using shared keys between WBAN nodes and the coordinator can protect sensitive health data from eavesdropping.
- **Data Integrity:** Ensuring data integrity involves safeguarding the accuracy and consistency of data. The lack of data integrity allows hostile entities to alter, delete, or replace vital patient information, which can have severe consequences. Integrity control mechanisms, such as digital signatures and keyed hash functions, can detect data alterations during storage or transmission.
- **Data Freshness:** Data freshness ensures the correct sequence and timeliness of data. It prevents adversaries from replaying captured data to confuse the WBAN coordinator. Two types of freshness are required: strong freshness, which ensures ordered frames and no delay, and weak freshness, which ensures ordered frames but not necessarily without delay.
- **Data Availability:** Ensuring that data is accessible whenever needed is crucial for healthcare applications. Attackers may attempt to impair network availability, depriving access to vital health data. Redundant operations and switching compromised nodes to operational ones can help maintain data availability.
- **Data Authentication:** Both WBAN nodes and the coordinator must verify that data is transmitted by a trusted entity. Symmetric techniques using a shared key can compute a Message Authentication Code (MAC) to ensure data integrity and authenticity.
- **Data Non-Repudiation:** Non-repudiation ensures that no entity can deny having sent or received data. In healthcare, tracking all operations with digital signatures and certificates maintains accountability for all data exchanges.
- **Authorization:** Authorization specifies permission levels for users (patients, doctors, nurses) to access the database and retrieve information. Access control rules and policies determine whether access requests are granted or denied.
- **Reliability:** Reliability in WBANs is essential for high-quality patient tracking. Attributes of reliability include security, Quality of Service (QoS), and fault tolerance. Using a MAC protocol based on TDMA can enhance reliability.
- **Anonymity:** Anonymity protects the patient's identity from adversaries. By using certificateless encryption, patients' names and identification numbers remain private, known only to doctors and nurses.
- **Unlinkability:** Ensuring unlinkability means that no one, except the user or healthcare provider, can link two authentication sessions from the same user.

- **Forward Secrecy:** Forward secrecy ensures that even if a user's secret key is compromised, previously established session keys remain secure.
- **Accountability:** Accountability means that any misuse of access rights can be tracked, and the responsible entity can be held accountable. This discourages illicit actions on patient data.
- **Revocability:** If a WBAN node or user is compromised, their access rights must be revoked to prevent further misuse.
- **Flexibility:** WBANs must allow patients to assign application providers in emergencies and provide on-demand authorization for doctors not on the permission list during urgent cases.
- **Dependability:** Dependability involves avoiding frequent failures and illicit modifications to node data. Combining reliability and availability ensures dependability, and error-correcting codes can help maintain it.
- **Secure Management:** Secure management at the coordinator's end involves distributing and managing cryptographic keys for WBAN nodes. This includes adding and removing nodes securely.
- **Secure Localization:** Accurate patient location tracking is necessary as WBANs support patient mobility. Secure localization methods prevent attackers from sending incorrect location details.
- **Location Privacy:** Protecting the patient's location information from adversaries is crucial. Using temporary pseudonyms for information exchange instead of hardware addresses can safeguard location privacy [1].

4.2 | Classification of Security Schemes in WBAN

To design a robust security mechanism for WBANs, it is crucial to understand their specific security and privacy needs. Traditional security mechanisms for other networks may not be suitable due to WBANs' resource constraints. Various well-known security schemes have been implemented in WBANs to protect against adversaries, and these are classified as follows (Figure 4):

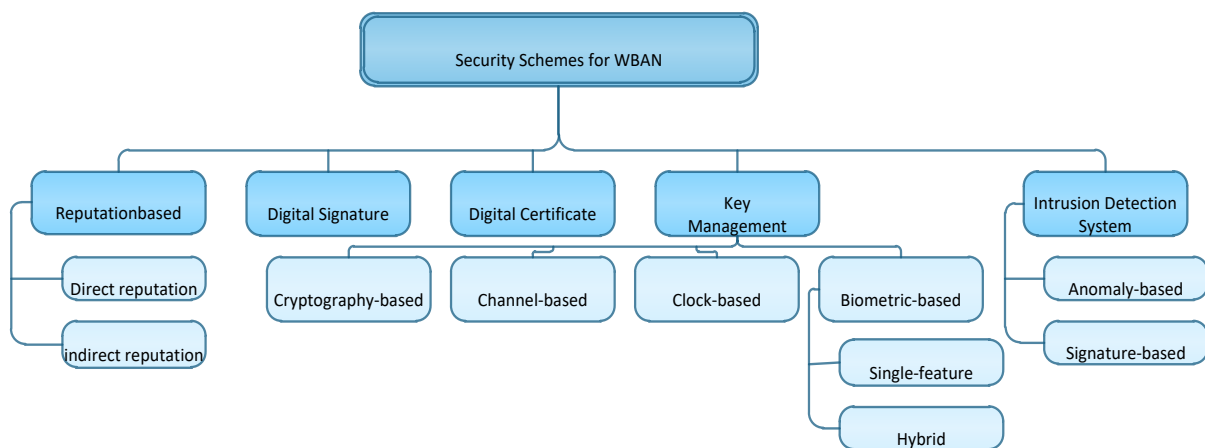


Figure 4. Security scheme classification for WBAN.

• Reputation-based Schemes

Reputation-based schemes rely on the past conduct of network nodes to evaluate their reliability numerically. Recommendations, both direct and indirect, form the basis of these evaluations:

- **Direct Reputation-based Schemes:** Evaluate node reliability based on local observations without relying on other nodes.
- **Indirect Reputation-based Schemes:** Evaluate node reliability based on both local observations and the observations of other nodes.

- Digital Signature Schemes

Digital signature schemes are cryptographic primitives used to achieve authentication, integrity, and non-repudiation for digital messages and documents. A hash function generates a message digest, which the sender signs using a private key. The receiver verifies the signature with the sender's public key.

- Digital Certificate Schemes

Digital certificate schemes use a digital certificate to bind an entity's public key with identifying information, validated by a trusted Certificate Authority (CA). These schemes, however, may be impractical for WBANs due to the resource constraints of the sensor nodes.

- Key Management Schemes

Key management schemes provide security by generating, renewing, agreeing on, distributing, and revoking cryptographic keys. These schemes can be categorized into:

- Cryptography-based Schemes: Utilize symmetric keys, asymmetric keys, or hash functions for key management.
- Channel-based Schemes: Classify nodes based on received signal strength variance.
- Clock-based Schemes: Use the sensor node's clock frequency to generate key pairs.
- Biometric-based Schemes: Extract or generate keys from physiological or behavioral biometric features.

- Intrusion Detection Systems (IDS)

- An IDS monitors the network for unauthorized access and manipulations. It gathers and analyzes information to detect inbound and outbound malicious activities.
- Anomaly-based IDS: Compares normal traffic performance baselines with sample network traffic to identify abnormal behavior.
- Signature-based IDS: Identifies intrusions by matching known attack patterns in its database.
- By implementing these security schemes, WBANs can protect against various adversarial attacks, ensuring secure and reliable healthcare data transmission.

- Security solution

- Bluetooth IEEE 802.15.1: This standard uses the initialization key as the link key. The initialization process is designed to protect key parameters during their transfer, ensuring secure communication.
- Biometrics: Biometric characteristics, such as fingerprints or heartbeat patterns, are increasingly used for secure communication. They are not only energy-efficient but also computationally lightweight, making them ideal for resource-constrained environments.
- Elliptic Curve Cryptography (ECC): ECC is well-suited for secure data exchange and key distribution in environments with limited resources. It has gained prominence as a more efficient alternative to RSA due to its lower computational requirements while maintaining strong security.
- Hardware Encryption: Hardware encryption can be implemented using a ChipCon 2420 ZigBee-compatible RF transceiver. This device executes IEEE 802.15.4 operations using 128-bit AES encryption keys, offering robust security for data transmission.

- IEEE 802.15.4: This standard supports short- and medium-range communication for ultra-low-power devices, ensuring secure transmission in energy-constrained scenarios.
- IEEE 802.15.6: This standard is specifically designed for low-power, short-range communication, typically used in body area networks (BANs), and focuses on efficient and secure data transmission.
- ZigBee: An enhancement of the IEEE 802.15.4 standard, ZigBee is used for short-range communication, providing improved security features for low-power devices in wireless sensor networks[2].

5 | WBAN IEEE 802.15.6 Standard

The IEEE 802.15.6 standard is a global benchmark for highly reliable, low-power wireless communication between devices located near or within the human body. While its primary focus is on providing secure communication for medical applications, it is versatile enough to be applied to non-medical uses as well, each with varying requirements. The standard offers a "default" mode suitable for both medical and non-medical applications, while a "high quality of service" mode is specifically reserved for critical medical use cases. It supports a wide range of data rates and can accommodate up to 64 nodes connected to a central hub[32].

5.1 | IEEE 802.15.6 Standard

Before a node can be associated with the hub, one of the three security levels defined by the IEEE 802.15.6 standard must be selected:

- Level 0 (insecure communication): Data is transmitted between the node and hub without any security measures.
- Level 1 (only authentication): Data is transmitted in a securely authenticated frame, but without encryption.
- Level 2 (authentication and encryption): Data frames are both authenticated and encrypted for maximum security.

After choosing the appropriate security level based on the specific requirements of the communication between the node and hub, the next step is to either activate the Pre-shared Master Key (PMK) or generate a new Master Key (MK). In unicast communication, either the node or the hub will create a Pairwise Temporal Key (PTK). In multicast communication, the hub will generate a Group Temporal Key (GTK), ensuring secure communication according to the IEEE 802.15.6 security model, shown in Figure 5.

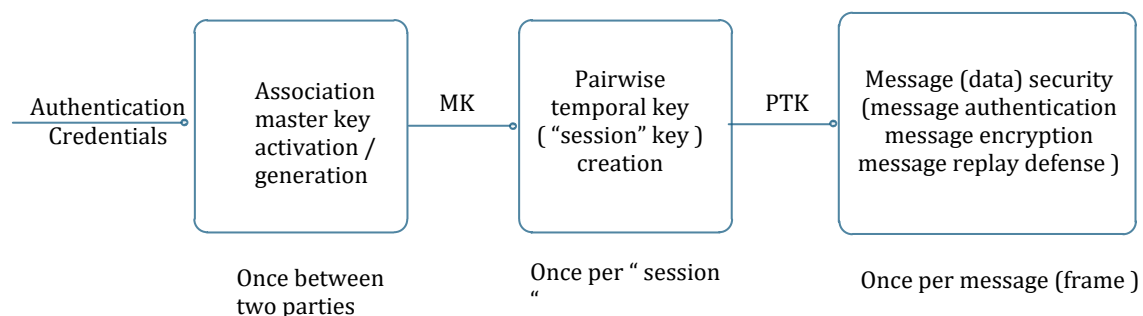


Figure 5. IEEE 802.15.6 security model.

5.2 | WBAN States

For secure communication, a node and a hub follow the MAC state diagram, as illustrated in Figure 6(a), when either party requires secure frame exchanges. The states are as follows:

- i. **Orphan State:** Initially, the node does not have a secure communication relationship with the hub. In this state, only Security Association and unsecured control frames can be exchanged between the node and the hub. The node can initiate a Security Association by exchanging frames to establish a security association, activate a pre-shared master key (MK), or generate a new MK. If successful, the node authenticates with the hub and transitions to the Associated state. Failure to establish a shared MK prevents the node from moving to the Associated state.
- ii. **Associated State:** In this state, the node has successfully established a shared MK with the hub, which is required to generate a pairwise temporal key (PTK). During this phase, only Security Disassociation, unsecured PTK, and control frames can be exchanged. The node and hub confirm the shared MK and generate the PTK, transitioning the communication to the Secured state. If they fail to create the PTK, the node returns to the Orphan state. The node or hub can also voluntarily return to the Orphan state by sending a Security Disassociation frame.
- iii. **Secured State:** Here, the node and hub use the established PTK to securely exchange frames. They can transmit Security Disassociation, Connection Request, Connection Assignment, and control frames (either secured or unsecured, depending on the association settings). Once a connection is established, the system transitions to the Connected state. If the connection cannot be established, the node returns to the Associated state. Missing or invalid PTK or Connected_NID will also force a return to the Associated state. Sending a Security Disassociation frame returns the node and hub to the Orphan state.
- iv. **Connected State:** In this state, the node holds an assigned Connected_NID, a wakeup arrangement, and optional allocations. The node engages in secured frame exchanges with the hub, except for Security Association frames, which are not included. Unsecured frames may only be used for control purposes if authentication was not selected during the association process. If the MK or PTK becomes invalid or missing, the node returns to either the Orphan or Associated state, depending on the error. Sending a Disconnection frame reverts the node to the Associated state.

For Unsecured Communication

For unsecured communication, a node and hub follow the MAC state diagram shown in Figure 6(b), which is used when neither party requires secure frame exchanges.

- i. **Orphan State:** Initially, the node has no unsecured communication relationship with the hub. Only Connection Request, Connection Assignment, and unsecured control frames can be transmitted. If a connection is successfully established, the node moves to the Connected state. Failure to establish a connection prevents the node from transitioning.
- ii. **Connected State:** In this state, the node holds an assigned Connected_NID, a wakeup arrangement, and optional allocations, engaging in unsecured frame exchanges with the hub. Security Association and Security Connection frames are excluded from this process. Sending a Disconnection frame returns the node to the Orphan state. If the node and hub wish to switch to secured communication, they must first disconnect, return to the Orphan state, and then follow the secured communication state diagram [33].

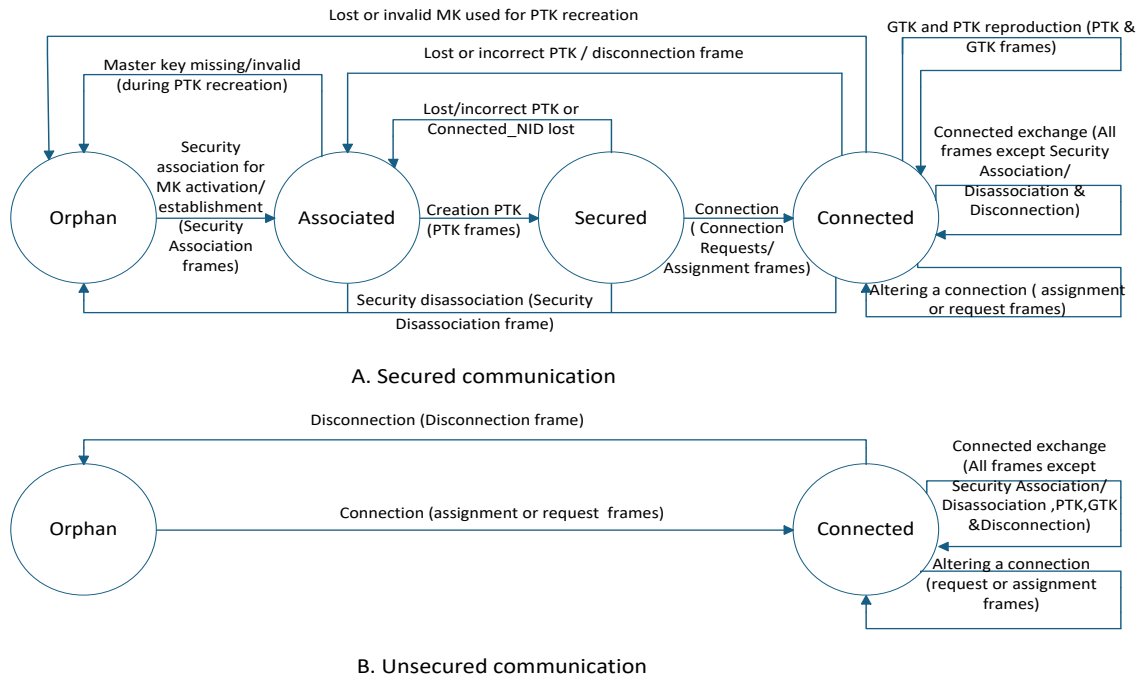


Figure 6. MAC security state diagrams.

5.3 | WBAN Frames Structure

The payload is contained inside a Security Association frame, as seen in Figure 7; a node and a hub exchange this frame during the execution of a security association protocol for generating a new shared MK or activating a pre-shared MK.

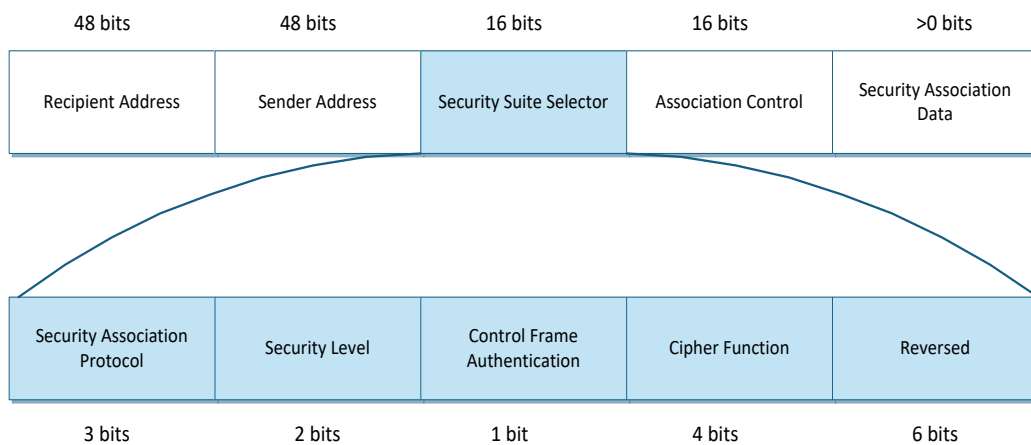


Figure 7. Security Association frame payload format.

- Recipient address
The current frame's receiver's address format is EUI-48 or set to zero if unknown.
- Sender address
The format of the sender's address, which is included in the current frame, used EUI-48.
- Security Suite Select (SSS)
Figure 6 presents the structure of SSS.
- Security association protocol

Set according to Table 5

Table 5. Field for the security association protocol.

The decimal value of the field	Field for the Security Association Protocol
0	An Organization with a Pre-Shared Master Key
1	Association Without Authentication
2	Coupling using a Secret Public Key
3	An Organization That Requires A Password To Join
4	Association Authentication Display
5-7	Reserved

- Security Level

In accordance with Table 6

Table 6. Field for security level.

The decimal value of the field	Field for Security Level
0	Level 0-insecure communication
1	Authentication at Level 1 without encryption
2	Level 2 encryption and authentication
3	Reserved

- Control frame authentication

A control frame is one entity that needs to be authenticated but not encrypted or zeroes if it needs neither authentication nor encryption, even at security levels 1 and 2.

- Cipher function

Set according to Table 7 as the sender indicates for performing security services.

Table 7. Cipher function field.

The decimal value of the field	Cipher Function
0	AES-128 Forward Cipher Function
1	Camellia-128 Forward Cipher Function
2-15	Reserved

- Association control

Estimate the security association frame's present location in specified standards for security association and its state (joined or aborted).

- Security association data

Based on the selected security association protocol, this field changes if MK pre-shared association is absent; otherwise, it will contain the x and y coordinates the public key for the elliptic curve of the sender, as well as the key message authentication code.

5.4 | IEEE 802.15.6 Security Analysis

In The IEEE 802.15.6 standard includes seven protocols focusing on security, as depicted in Figures 8 to 13. For simplicity, these will be referred to as protocols 1 through 7. In this context, the node is denoted as A, and the hub as B, with simpler notations than those used in the standard. Immediate Acknowledgement (I-Ack) messages, which B sends to A after receiving a frame, have been omitted from these protocols. I-Ack

messages contain the current allocation slot number (8 bits) and slot offset (16 bits) but are sent in clear text, making them vulnerable to modification by adversaries. Thus, they are excluded from the security analysis.

When A and B have a pre-shared master key (MK), protocol 1 can activate this MK or establish a new one. The key agreement process involves one of four two-party protocols (2 to 5), each varying slightly in details and requirements but fundamentally similar. Protocol 2 is an unauthenticated key agreement protocol with no special requirements. Protocol 3 requires an out-of-band transfer of A's public key to B, which must be stored securely. Protocol 4 same steps protocol 3 with requires a pre-shared password (PW), with nodes capable of entering this password. Protocol 5 requires both A and B to display a decimal number for user verification before accepting a new MK.

Once A and B agree on an MK, they transition from the Orphan state to the Associated state and can use the MK to execute protocol 6, establishing a pairwise temporal key (PTK). Successful execution of protocol 6 transitions them to the Secured state, where the PTK is used as a session key. Security disassociation, involving deletion of the MK and PTK, is managed by protocol 7, returning the nodes to the Orphan state.

Protocols 2 to 5 are based on elliptic curve public key cryptography, using domain parameters of an elliptic curve described by the Weierstrass Equation 2 over the finite field $GF(p)$ where p is a prime number. The curve must be nonsingular, satisfying $4a^3+27b^2 \neq 0$, to avoid known attacks. The base point G on the curve is of order n , with $n \times G = O$ (the point at infinity). The cofactor h is defined as $h = \#E(GF(p))/n$, where $\#E(.)$ is the order of the elliptic curve. The IEEE 802.15.6 standard recommends using Curve P-256 from FIPS Pub 186-3, with public parameters a, b, p, n and G .

Private keys, denoted by SKA and SKB for nodes A and B respectively, are 256-bit random integers. The corresponding public keys are points on the elliptic curve, generated as $PKA = (PKAX, PKAY) = SKA \times G$ and $PKB = (PKBX, PKBY) = SKB \times G$. Public key validation, although briefly mentioned in the standard, involves ensuring the received public key is a non-infinity point on the curve and satisfies the elliptic curve equation. The standard specifies key validity checks at the start of protocols, aborting if the keys are invalid.

In protocols 2 to 5, B always sends its public key PKB in clear text. Protocol 2 and 5 also involve A sending its public key in clear text, while Protocol 3 uses a pre-shared public key. Protocol 4 uses a masked public key $PK0A = PKA - Q(PW)$, where PW is derived from a pre-shared password. The IEEE 802.15.6 standard suggests using CMAC with AES (as specified in NIST SP800-38B and FIPS197) for message authentication, and includes various other technical specifications for handling keys and validating messages.

The network topology includes up to 256 nodes connected to a hub, which should ideally use a single public key for all nodes due to resource constraints. The standard does not specify the lifecycle of keys or whether they are accompanied by digital certificates, assuming nodes cannot store or validate certificates due to resource limitations.

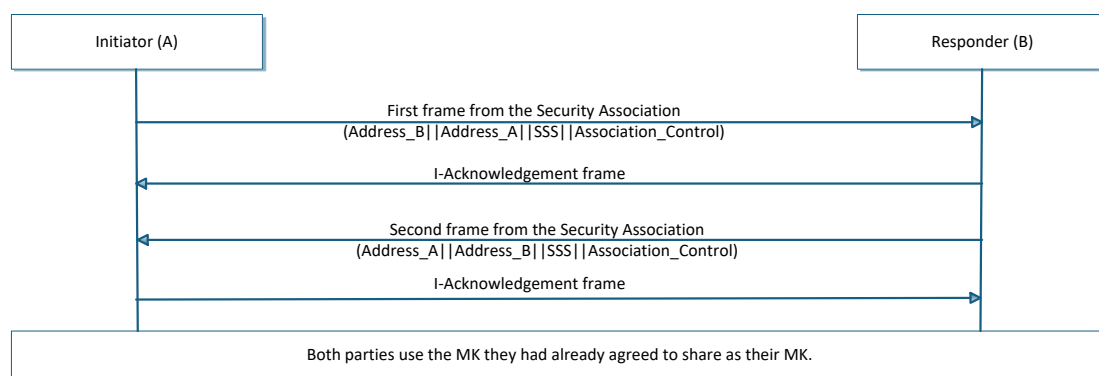


Figure 8. Activates or establishes a pre-shared MK (protocol 1).

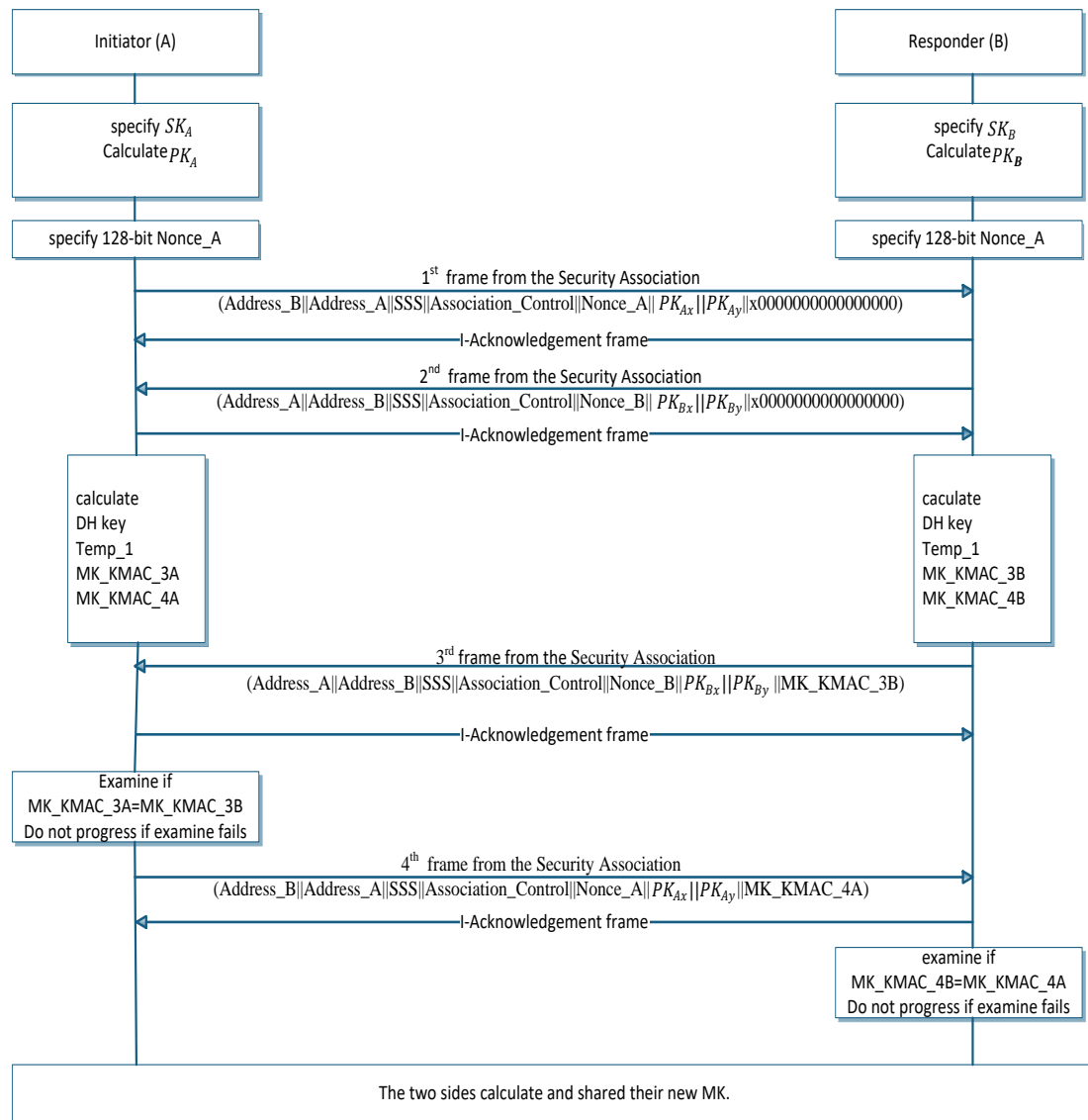


Figure 9. Unauthenticated key agreement (protocol 2).

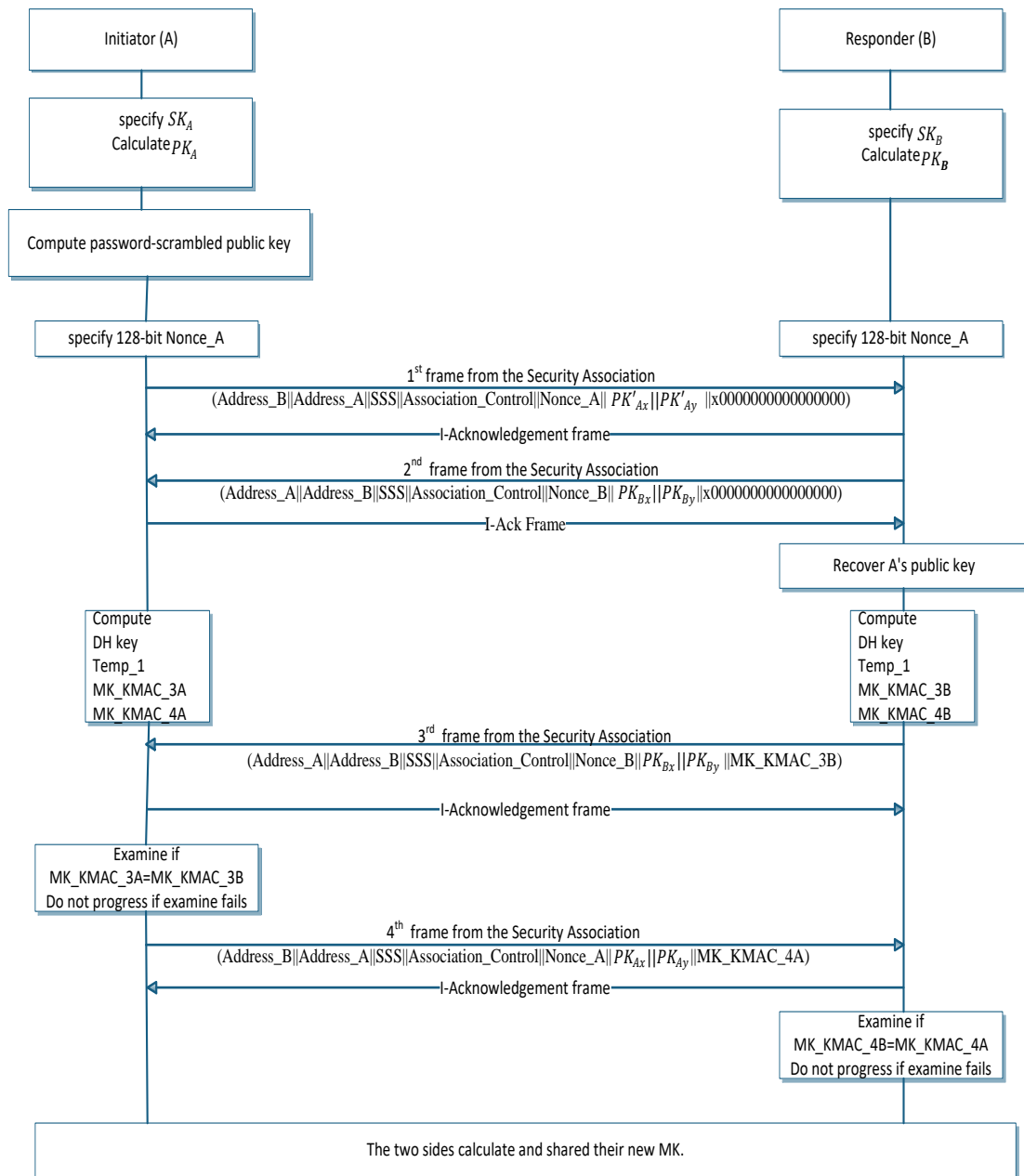


Figure 10. Uses a pre-shared password (protocol 3 & 4).

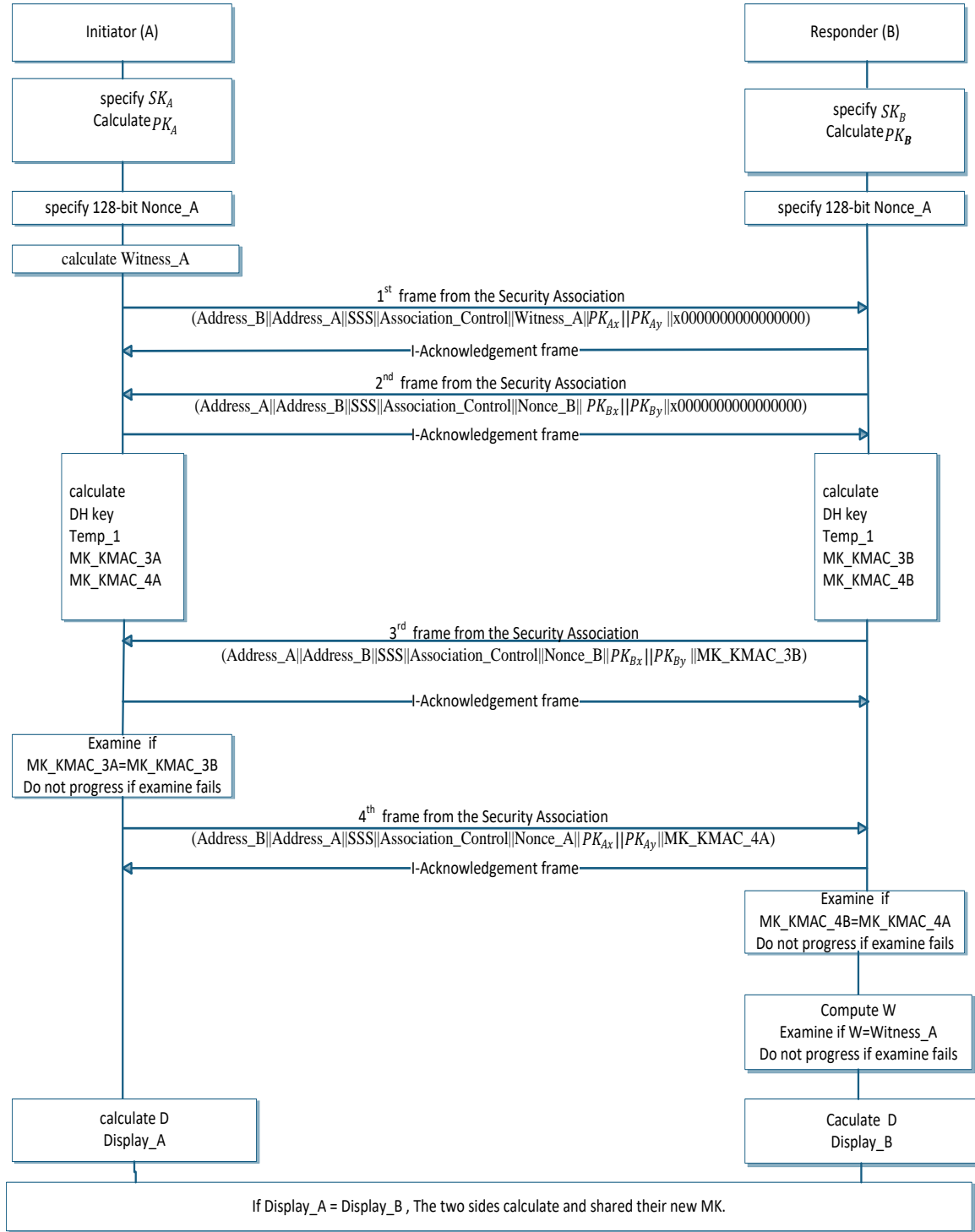


Figure 11. Requires user verification of a displayed number (protocol 5).

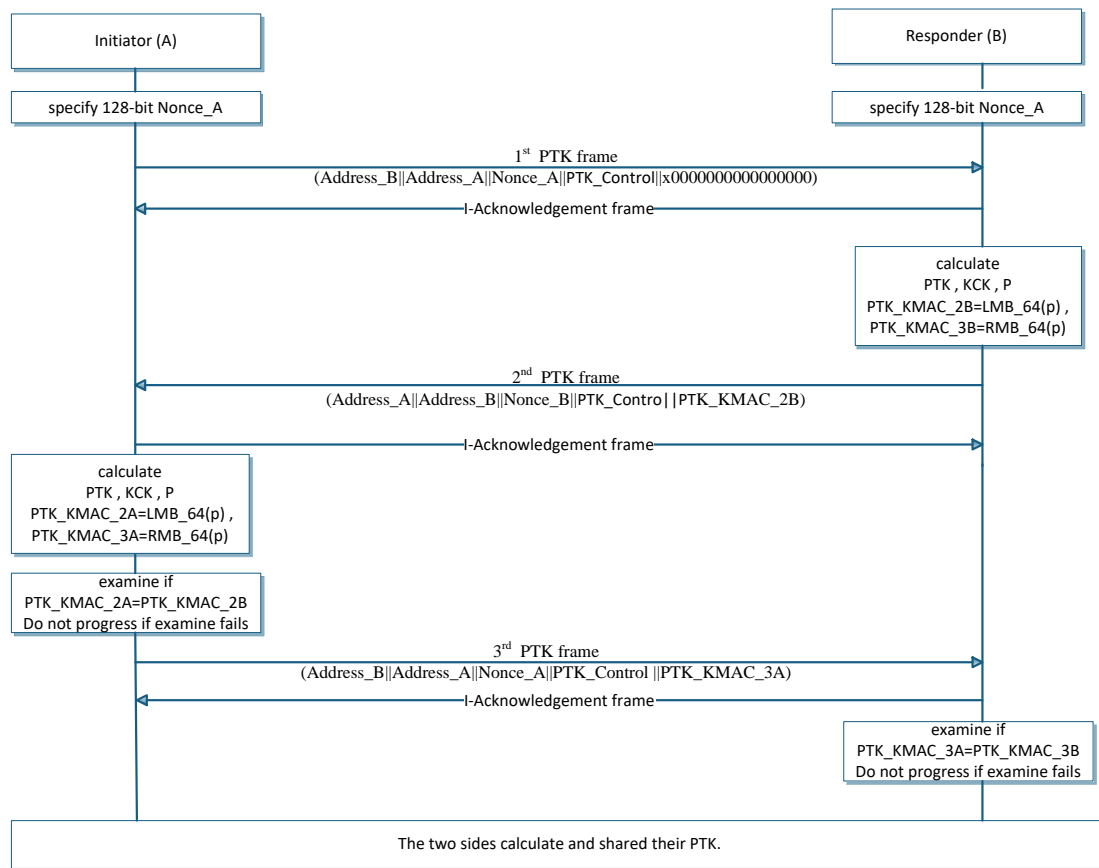


Figure 12. Establishes a PTK using the MK.

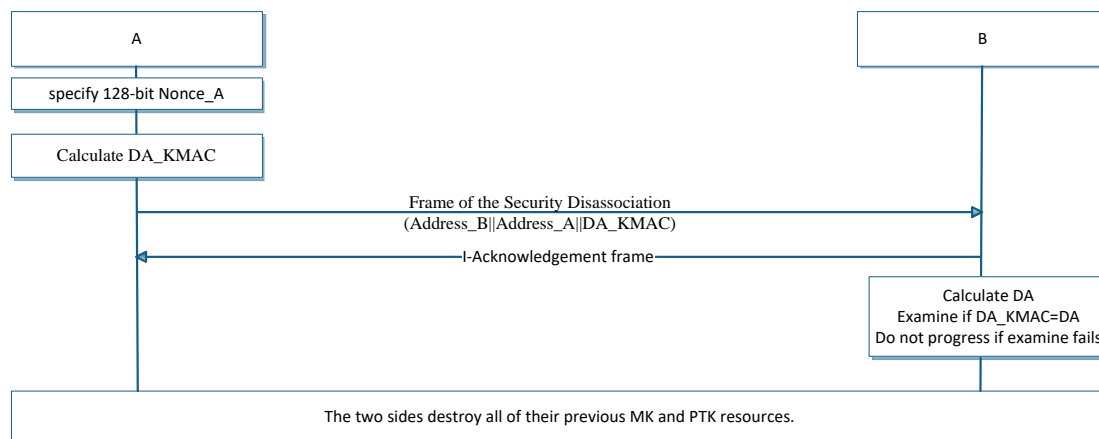


Figure 13. Manages security disassociation by deleting MK and PTK.

These protocols ensure secure communication and key management in WBANs, using elliptic curve cryptography.

5.5 | Security Analysis of the Security Association Protocol

The IEEE 802.15.6 standard aims to provide confidentiality, authentication, integrity, privacy protection, and defense against replay attacks. However, privacy preservation mechanisms are somewhat unclear, as node and hub identifiers are transmitted openly during protocol executions. Confidentiality is achieved by encrypting data using the PTK as the encryption key. The PTK creation procedure (protocol 6) uses an MK generated through one of the four protocols (2 to 5), three of which are authenticated.

In this section, we analyze the security protocols of the IEEE 802.15.6 standard and identify several security issues. Specifically, we demonstrate that all the protocols involved in the security association procedure (protocols 2 to 5) are insecure under almost any security model for these protocols. They are susceptible to key-compromise impersonation (KCI) attacks and do not provide forward secrecy. Furthermore, protocols 2, 4, and 5 are vulnerable to impersonation attacks, and protocol 4 is also vulnerable to an offline dictionary attack. The impersonation attacks are feasible because public keys are self-generated and not accompanied by digital certificates due to resource constraints. Even with a lightweight PKI for certifying public keys, these protocols would still be vulnerable to KCI attacks. Additional attacks are possible if public keys are not validated.

we denote a passive attacker as E and an active attacker as M. The numbering of protocols and attacks does not imply any preference or importance.

5.5.1 | Security Analysis of Protocol 2

Protocol 2 is an unauthenticated key exchange protocol, making it trivially vulnerable to impersonation attacks. This vulnerability is noted in the standard, which introduces Protocol 2 as a protocol "without the benefit of keeping third parties from launching impersonation attacks." Protocol 2 also lacks forward secrecy, a crucial attribute for key exchange protocols.

Impersonation Attack

Protocol 2 is vulnerable to an impersonation attack. Here is how M impersonates A:

- M selects a private key SK_M and generates the corresponding public key $PK_M = (PK_{MX}, PK_{MY}) = SK_M \times G$. M selects a 128-bit random number N_M and sends $\{ID_B || ID_A || SSS || AC || N_M || PK_{MX} || PK_{MY} || XX\}$ to B.
- B selects a 128-bit random number N_B and sends $\{ID_A || ID_B || SSS || AC || N_B || PK_{BX} || PK_{BY} || XX\}$ to M.
- B computes $DHKey = X(SK_B \times PK_M)$, $T_0 = RMB_{128}(DHKey)$, $T_2 = CMAC(T_0, ID_A || ID_B || N_M || N_B || SSS, 64)$, and $T_3 = CMAC(T_0, ID_B || ID_A || N_B || N_M || SSS, 64)$. B sends $\{ID_A || ID_B || SSS || AC || N_B || PK_{BX} || PK_{BY} || T_2\}$ to M.
- M computes $DHKey = X(SK_M \times PK_B)$, $T_1 = RMB_{128}(DHKey)$, $T_2 = CMAC(T_1, ID_A || ID_B || N_M || N_B || SSS, 64)$, and $T_3 = CMAC(T_1, ID_B || ID_A || N_B || N_M || SSS, 64)$. M sends $\{ID_B || ID_A || SSS || AC || N_M || PK_{MX} || PK_{MY} || T_3\}$ to B.
- M computes $T_4 = LMB_{128}(DHKey)$ and generates the master key $MK = CMAC(T_4, N_M || N_B, 128)$.
- B verifies that $T_3 = T_3$, computes $T_0 = LMB_{128}(DHKey)$, and generates the master key $MK = CMAC(T_0, N_M || N_B, 128)$.
- M and B thus share the same MK, allowing M to successfully impersonate A. A similar impersonation attack can be crafted where M impersonates B in communication with A.

KCI Attack

Protocol 2 remains vulnerable to KCI attacks even with certified public keys. Here is a KCI attack where M, upon disclosure of SKA, impersonates B and shares an MK with A:

- A selects a 128-bit random number N_A and sends $\{ID_B || ID_A || SSS || AC || N_A || PK_{AX} || PK_{AY} || XX\}$ to B. M intercepts the session and tries to impersonate B.

- M selects a 128-bit random number NM and sends $\{IDA||IDB||SSS||AC||NM||PKBX||PKBY||XX\}$ to A.
- M, having SKA, computes $DHKey=X(SKA \times PKB)$, $T01=RMB128(DHKey)$, $T02=CMAC(T01,IDA||IDB||NA||NM||SSS,64)$, and $T03=CMAC(T01,IDB||IDA||NM||NA||SSS,64)$. M sends $\{IDA||IDB||SSS||AC||NM||PKBX||PKBY||T02\}$ to A.
- A computes $DHKey=X(SKA \times PKB)$, $T1=RMB128(DHKey)$, and $T2=CMAC(T1,IDA||IDB||NA||NM||SSS,64)$. A verifies that $T2=T2$, and computes $T3=CMAC(T1,IDB||IDA||NM||NA||SSS,64)$. A sends $\{IDB||IDA||SSS||AC||NA||PKAX||PKAY||T3\}$ to M.
- A computes $T4=LMB128(DHKey)$ and generates the master key $MK=CMAC(T4,NA||NM,128)$.
- M computes $T4=LMB128(DHKey)$ and generates the master key $MK=CMAC(T04,NA||NM,128)$.
- M and A thus share the same MK, allowing M to successfully impersonate B. Similarly, upon disclosure of SKB, M can impersonate A and share an MK with B.

Lack of Forward Secrecy

Protocol 2 does not provide forward secrecy. An adversary E, having eavesdropped and saved all messages from previous protocol runs, can compromise the established MK if SKB or SKA is compromised:

- If SKB is compromised, E computes $DHKey=X(SKB \times PKA)$, $T4=LMB128(DHKey)$, and obtains the MK $CMAC(T04,NA||NB,128)$.
- If SKA is compromised, E computes $DHKey=X(SKA \times PKB)$, $T4=LMB128(DHKey)$, and obtains the MK $CMAC(T4,NA||NB,128)$.

5.5.2 | Security Analysis of Protocol 3

Protocol III requires the out-of-band transfer of a node's public key to the hub. It is vulnerable to the Key Compromise Impersonation (KCI) attack and lacks forward secrecy.

Key Compromise Impersonation Attack

Protocol III is susceptible to KCI attacks. Here is a scenario where attacker M possesses SKA and impersonates B. Since B's public key PKB is transmitted in clear text, M can obtain PKB by eavesdropping on a previous protocol run.

- A selects a 128-bit random number NA and sends $\{IDB||IDA||SSS||AC||NA||0||0||XX\}$ to B. M hijacks the session and attempts to impersonate B.
- M selects a 128-bit random number NM and sends $\{IDA||IDB||SSS||AC||NM||PKBX||PKBY||XX\}$ to A.
- M, possessing SKA, computes $DHKey=X(SKA \times PKB)$, $T1=RMB128(DHKey)$, $T2=CMAC(T01,IDA||IDB||NA||NM||SSS,64)$, and $T3=CMAC(T01,IDB||IDA||NM||NA||SSS,64)$. M sends $\{IDA||IDB||SSS||AC||NM||PKBX||PKBY||T2\}$ to A.
- A computes $DHKey=X(SKA \times PKB)$, $T1=RMB128(DHKey)$, and $T2=CMAC(T1,IDA||IDB||NA||NM||SSS,64)$. A verifies that $T2=T2$ and computes $T3=CMAC(T1,IDB||IDA||NM||NA||SSS,64)$. A sends $\{IDB||IDA||SSS||AC||NA||0||0||T3\}$ to M.

- A computes $T4 = \text{LMB128}(\text{DHKey})$ and generates the master key $\text{MK} = \text{CMAC}(T4, \text{NA} || \text{NM}, 128)$.
- M computes $T4 = \text{LMB128}(\text{DHKey})$ and generates the master key $\text{MK} = \text{CMAC}(T4, \text{NA} || \text{NM}, 128)$.
- M and A thus compute the same MK, allowing M to successfully impersonate B.

Lack of Forward Secrecy

Protocol 3 does not provide forward secrecy. Assuming that PKA has been securely shared with B, we consider the scenario where SKA is compromised. Here's how an adversary E can extract a previously established MK from eavesdropped messages, demonstrating the lack of forward secrecy:

- Eavesdropper E has captured PKB , NA , and NB from the messages exchanged in clear text.
- If SKA is compromised, E computes $\text{DHKey} = X(\text{SKA} \times \text{PKB})$, $T4 = \text{LMB128}(\text{DHKey})$, and obtains the MK as $\text{CMAC}(T4, \text{NA} || \text{NB}, 128)$.

5.5.3 | Security Analysis of Protocol 4

Protocol 4 is a Password-Authenticated Key Exchange (PAKE) protocol. It lacks forward secrecy and is vulnerable to impersonation and offline dictionary attacks.

Impersonation Attack

To perform an impersonation attack on Protocol 4, attacker M first eavesdrops on messages between A and B. M then obtains PK0A and PKA from messages (1) and (4) of the protocol. M computes $\text{Q0} = \text{PKA} -$ and uses Q0 for the impersonation attack. Here is an example of how M can impersonate A:

- M selects a private key SKM and generates the corresponding public key $\text{PKM} = (\text{PKMX}, \text{PKMY}) = \text{SKM} \times G$. M computes $\text{PK0M} = \text{PKM} - \text{Q0}$. If $\text{PK0M} = O$, M selects new private and public keys and continues until $\text{PK0M} \neq O$. M selects a 128-bit random number NM and sends $\{\text{IDB} || \text{IDA} || \text{SSS} || \text{AC} || \text{NM} || \text{PK0MX} || \text{PK0MY} || \text{XX}\}$ to B.
- B selects a 128-bit random number NB and sends $\{\text{IDA} || \text{IDB} || \text{SSS} || \text{AC} || \text{NB} || \text{PKBX} || \text{PKBY} || \text{XX}\}$ to M.
- B calculates $\text{PKM} = \text{PK0M} + \text{Q}(\text{PW})$ and computes $\text{DHKey} = X(\text{SKB} \times \text{PKM})$, $\text{T01} = \text{RMB128}(\text{DHKey})$, $\text{T02} = \text{CMAC}(\text{T01}, \text{IDA} || \text{IDB} || \text{NM} || \text{NB} || \text{SSS}, 64)$, and $\text{T03} = \text{CMAC}(\text{T01}, \text{IDB} || \text{IDA} || \text{NB} || \text{NM} || \text{SSS}, 64)$. B sends $\{\text{IDA} || \text{IDB} || \text{SSS} || \text{AC} || \text{NB} || \text{PKBX} || \text{PKBY} || \text{T02}\}$ to M.
- M computes $\text{DHKey} = X(\text{SKM} \times \text{PKB})$, $\text{T1} = \text{RMB128}(\text{DHKey})$, $\text{T2} = \text{CMAC}(\text{T1}, \text{IDA} || \text{IDB} || \text{NM} || \text{NB} || \text{SSS}, 64)$, and $\text{T3} = \text{CMAC}(\text{T1}, \text{IDB} || \text{IDA} || \text{NB} || \text{NM} || \text{SSS}, 64)$. M sends $\{\text{IDB} || \text{IDA} || \text{SSS} || \text{AC} || \text{NM} || \text{PKMX} || \text{PKMY} || \text{T3}\}$ to B.
- M computes $T4 = \text{LMB128}(\text{DHKey})$ and generates the master key $\text{MK} = \text{CMAC}(T4, \text{NM} || \text{NB}, 128)$.
- B verifies that $\text{T3} = \text{T03}$, computes $\text{T04} = \text{LMB128}(\text{DHKey})$, and generates the master key $\text{MK} = \text{CMAC}(\text{T04}, \text{NM} || \text{NB}, 128)$.
- M and B thus compute the same MK, allowing M to successfully impersonate A. A similar scenario can be crafted where M impersonates B in communication with A. This impersonation attack could be mitigated by using digital certificates from a lightweight PKI and verifying claimed identifiers with the certificates. However, even in this case, Protocol 4 remains vulnerable to KCI attacks.

KCI Attack

Here is a KCI attack scenario where M, upon disclosure of SKA, impersonates B and shares an MK with A. M does not need to know the password PW. Since B's public key PKB is sent in clear text, M can obtain PKB by eavesdropping on a previous protocol run.

- A selects a 128-bit random number NA and sends $\{IDB||IDA||SSS||AC||NA||PK0AX||PK0AY||XX\}$ to B. M intercepts the session and attempts to impersonate B.
- M selects a 128-bit random number NM and sends $\{IDA||IDB||SSS||AC||NM||PKBX||PKBY||XX\}$ to A.
- M, possessing SKA, computes $DHKey=X(SKA \times PKB)$, $T01=RMB128(DHKey)$, $T02=CMAC(T01, IDA||IDB||NA||NM||SSS, 64)$, and $T03=CMAC(T01, IDB||IDA||NM||NA||SSS, 64)$. M sends $\{IDA||IDB||SSS||AC||NM||PKBX||PKBY||T02\}$ to A.
- A computes $DHKey=X(SKA \times PKB)$, $T1=RMB128(DHKey)$, and $T2=CMAC(T1, IDA||IDB||NA||NM||SSS, 64)$. A verifies that $T2=T02$ and computes $T3=CMAC(T1, IDB||IDA||NM||NA||SSS, 64)$. A sends $\{IDB||IDA||SSS||AC||NA||PKAX||PKAY||T3\}$ to M.
- A computes $T4=LMB128(DHKey)$ and generates the master key $MK=CMAC(T4, NA||NM, 128)$.
- M computes $T04=LMB128(DHKey)$ and generates the master key $MK=CMAC(T04, NA||NM, 128)$.
- M and A thus compute the same MK, allowing M to successfully impersonate B.

Offline Dictionary Attack

Protocol 4 is a PAKE protocol with two-factor authentication, requiring both public keys and a shared password. For PAKE protocols, resilience to offline dictionary attacks is crucial. An adversary E can perform a dictionary attack on Protocol 4 by eavesdropping on messages between A and B. E then obtains PK0A and PKA from messages (1) and (4) of the protocol. E computes $PKA - PK0A = Q(PW) = (QX, QY)$. Since $QX = 232PW + MX$ and QX is known, it can be used as a verifier. E can then try probable passwords from a dictionary and check which password PW maps to QX. This process is fast, allowing E to find the shared password PW.

Lack of Forward Secrecy

Protocol 4 does not provide forward secrecy. Since PKB, NA, and NB are sent in clear text, they can be eavesdropped and saved by E. If SKA is compromised, E computes $DHKey=X(SKA \times PKB)$, $T4=LMB128(DHKey)$, and obtains the master key $MK=CMAC(T4, NA||NB, 128)$.

5.5.4 | Security Analysis of Protocol 5

Here is an impersonation attack on Protocol 5, where M impersonates A:

- M selects a private key SKM and generates the corresponding public key $PKM=(PKMX, PKMY)=SKM \times G$. M selects a 128-bit random number NM and computes $WM=CMAC(NM, IDA||IDB||PKMX||PKMY, 128)$. M sends $\{IDB||IDA||SSS||AC||WM||PKMX||PKMY||XX\}$ to B.
- B selects a 128-bit random number NB and sends $\{IDA||IDB||SSS||AC||NB||PKBX||PKBY||XX\}$ to M.
- B computes $DHKey=X(SKB \times PKM)$, $T01=RMB128(DHKey)$, $T02=CMAC(T01, IDA||IDB||WM||NB||SSS, 64)$, and

$T03 = \text{CMAC}(T01, \text{IDB} || \text{IDA} || \text{NB} || \text{WM} || \text{SSS}, 64)$. B sends $\{\text{IDA} || \text{IDB} || \text{SSS} || \text{AC} || \text{NB} || \text{PKBX} || \text{PKBY} || T02\}$ to M.

- M computes $\text{DHKey} = X(\text{SKM} \times \text{PKB})$, $T1 = \text{RMB128}(\text{DHKey})$, $T2 = \text{CMAC}(T1, \text{IDA} || \text{IDB} || \text{WM} || \text{NB} || \text{SSS}, 64)$, $T3 = \text{CMAC}(T1, \text{ID_B} || \text{ID_A} || \text{N_B} || \text{W_M} || \text{SSS}, 64)$. M sends $\{\text{IDB} || \text{IDA} || \text{SSS} || \text{AC} || \text{NM} || \text{PKMX} || \text{PKMY} || T3\}$ to B.
- Display M shows $\text{BS2DI}(D)$ where $D = \text{CMAC}(\text{NM} || \text{NB}, \text{NB} || \text{NM} || T1, 16)$.
- B verifies that $T3 = T03$, computes $W0M = \text{CMAC}(\text{NM}, \text{IDA} || \text{IDB} || \text{PKMX} || \text{PKMY}, 128)$, and verifies that $\text{WM} = W0M$. Display B shows $\text{BS2DI}(D0)$ where $D0 = \text{CMAC}(\text{NM} || \text{NB}, \text{NB} || \text{NM} || T1, 16)$. As Display M matches Display B, B computes $T04 = \text{LMB128}(\text{DHKey})$ and $\text{MK} = \text{CMAC}(T04, \text{NM} || \text{NB}, 128)$. M computes $T4 = \text{LMB128}(\text{DHKey})$ and $\text{MK} = \text{CMAC}(T4, \text{NM} || \text{NB}, 128)$.
- M and B compute the same MK, allowing M to successfully impersonate A. A similar scenario can be crafted where M impersonates B in communication with A. This impersonation attack could be mitigated by using digital certificates from a lightweight PKI and verifying the claimed identifiers with the certificates. However, it cannot prevent a KCI attack on Protocol 5.

Here is the KCI attack scenario where M, upon disclosure of SKA, impersonates B and shares a master key MK with A:

- A selects a 128-bit random number N and computes $\text{WA} = \text{CMAC}(\text{NA}, \text{IDA} || \text{IDB} || \text{PKAX} || \text{PKAY}, 128)$. A sends $\{\text{IDB} || \text{IDA} || \text{SSS} || \text{AC} || \text{WA} || \text{PKAX} || \text{PKAY} || \text{XX}\}$ to B. M intercepts the session and tries to impersonate B.
- M selects a 128-bit random number NM and sends $\{\text{IDA} || \text{IDB} || \text{SSS} || \text{AC} || \text{NM} || \text{PKBX} || \text{PKBY} || \text{XX}\}$ to A.
- M, possessing SKA, computes $\text{DHKey} = X(\text{SKA} \times \text{PKB})$, $T01 = \text{RMB128}(\text{DHKey})$, $T02 = \text{CMAC}(T01, \text{IDA} || \text{IDB} || \text{WA} || \text{NM} || \text{SSS}, 64)$, and $T03 = \text{CMAC}(T01, \text{IDB} || \text{IDA} || \text{NM} || \text{WA} || \text{SSS}, 64)$. M sends $\{\text{IDA} || \text{IDB} || \text{SSS} || \text{AC} || \text{NM} || \text{PKBX} || \text{PKBY} || T02\}$ to A.
- A computes $\text{DHKey} = X(\text{SKA} \times \text{PKB})$, $T1 = \text{RMB128}(\text{DHKey})$, and $T2 = \text{CMAC}(T1, \text{IDA} || \text{IDB} || \text{WA} || \text{NM} || \text{SSS}, 64)$. A verifies that $T2 = T02$ and computes $T3 = \text{CMAC}(T1, \text{IDB} || \text{IDA} || \text{NM} || \text{WA} || \text{SSS}, 64)$. A sends $\{\text{IDB} || \text{IDA} || \text{SSS} || \text{AC} || \text{NA} || \text{PKAX} || \text{PKAY} || T3\}$ to M.
- Display A shows $\text{BS2DI}(D)$ where $D = \text{CMAC}(\text{NA} || \text{NM}, \text{NM} || \text{NA} || T1, 16)$.
- Display M shows $\text{BS2DI}(D0)$ where $D0 = \text{CMAC}(\text{NA} || \text{NM}, \text{NM} || \text{NA} || T1, 16)$. As Display A matches Display M, A computes $T4 = \text{LMB128}(\text{DHKey})$ and $\text{MK} = \text{CMAC}(T4, \text{NA} || \text{NM}, 128)$. M computes $T04 = \text{LMB128}(\text{DHKey})$ and $\text{MK} = \text{CMAC}(T04, \text{NA} || \text{NM}, 128)$.
- M and A compute the same MK, allowing M to successfully impersonate B. In a similar scenario, upon disclosure of SKB, M can impersonate A and share a master key MK with B.

Lack of Forward Secrecy

Protocol 5 does not provide forward secrecy. Since PKA, PKB, NA, and NB are sent in clear text, they can be eavesdropped and saved by E.

- If SKB is compromised, E computes $\text{DHKey} = X(\text{SKB} \times \text{PKA})$, $T04 = \text{LMB128}(\text{DHKey})$, and obtains $\text{MK} = \text{CMAC}(T04, \text{NA} || \text{NB}, 128)$.

- If SKA is compromised, E computes $DHKey = X(SKA \times PKB)$, $T4 = LMB128(DHKey)$, and obtains $MK = CMAC(T4, NA || NB, 128)$.

6 | Future Work

Researchers continue to explore innovative solutions to overcome the current challenges of Wireless Body Area Networks (WBANs). By enhancing existing approaches and integrating emerging technologies such as Software Defined Networks (SDN), Blockchain, Big Data, Machine Learning, Energy Harvesting (EH), and Virtual Reality, significant improvements can be made in the performance and security of WBANs

SDN in WBAN

In recent years, both industry and academia have increasingly favored Software Defined Networks (SDN) over traditional networking solutions. SDN separates the data plane from the control plane, allowing for centralized network management and eliminating the need for multiple vendors to enforce policies. This programmatic controller makes the network simpler and more flexible. WBANs face challenges such as sensor limitations, difficulties in installing and configuring multi-vendor sensors, and the absence of efficient handover mechanisms. By implementing SDN in WBANs, these issues can be mitigated, supporting vendor independence and enabling patient mobility within the WBAN system.[4, 34-36].

Blockchain in WBAN

Blockchain technology has gained significant attention in recent years as a method to secure data transmission between different parties, especially in healthcare services. Its implementation in WBANs provides a structured platform where hospitals and caregivers can securely track patient history and access real-time information simultaneously. This ensures the integrity and confidentiality of sensitive medical data [4, 37-38].

EH in WBAN

Energy efficiency remains a critical concern in WBANs. Energy Harvesting (EH) technology offers a promising solution by converting energy from physiological processes (e.g., body temperature, glucose levels, blood pressure, and breathing) into electrical energy. This technology enables continuous real-time monitoring of patients without frequent battery changes, improving the operational lifespan of WBAN sensors [4, 39]

BigData in WBAN

The vast amount of semi-structured or unstructured medical data generated by WBAN sensors poses significant challenges in terms of storage, processing, and analysis. Big Data technologies are designed to handle large volumes of data with high velocity, variety, and veracity. These technologies enable more efficient data analysis and monitoring, reducing the computational load on traditional WBAN systems [40, 41].

Machine Learning in WBAN

Machine Learning, a subfield of artificial intelligence, has shown great potential in WBAN applications such as human behavior recognition and error detection. Unlike traditional systems that require explicit programming, machine learning algorithms can autonomously learn from data and improve over time. This capability makes them particularly useful for enhancing the accuracy and efficiency of WBAN systems [42, 43].

Virtual reality in WBAN

Virtual Reality (VR) technology offers immersive three-dimensional (3D) simulations that can be used in physical therapy to assist patients with exercises. By incorporating visual information, auditory feedback, and textual cues, VR can create engaging and effective rehabilitation environments for patients using WBANs [44].

7 | Conclusion

Wireless Body Area Networks (WBANs) are a relatively new but rapidly growing area of research in healthcare. This study provides a comprehensive review of the recent advancements in WBAN technology, exploring both medical and non-medical applications. A classification system is presented, highlighting the diverse use cases of WBANs, along with an in-depth analysis of the IEEE 802.15.6 standard, which governs the operation of these networks.

The insights offered by this study can help guide future researchers, professionals, and academics in understanding the evolving characteristics of WBANs according to the latest standards. These advancements promise to enhance the quality of life by enabling early diagnosis of medical conditions and reducing healthcare costs for patients.

Lastly, integrating cutting-edge technologies such as SDN, Blockchain, Big Data, Machine Learning, and Energy Harvesting with WBANs holds the potential to revolutionize healthcare. These innovations will provide stronger security, better data management, and more efficient operation, driving significant improvements in the future of WBAN-enabled healthcare systems.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

- [1] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Computers and Security*, vol. 104. Elsevier Ltd, May 01, 2021. doi: 10.1016/j.cose.2021.102211.
- [2] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113. Elsevier B.V., Feb. 01, 2021. doi: 10.1016/j.sysarc.2020.101883.
- [3] V. Gorbach, M. L. Ali, and K. Thakur, "A review of data privacy techniques for wireless body area networks in telemedicine," in *IEMTRONICS 2020 - International IOT, Electronics and Mechatronics Conference, Proceedings*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020. doi: 10.1109/IEMTRONICS51293.2020.9216361.
- [4] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, and M. S. Islam, "A comprehensive review of wireless body area network," *Journal of Network and Computer Applications*, vol. 143. Academic Press, pp. 178–198, Oct. 01, 2019. doi: 10.1016/j.jnca.2019.06.016.
- [5] R. Rani Chintala, N. Rao M R, and S. Venkateswarlu, "Review on the Security Issues in Human Sensor Networks for Healthcare Applications," *Int. J. Eng. Technol.*, vol. 7, no. 2.32, p. 269, May 2018, doi: 10.14419/IJET.V7I2.32.15582.

- [6] L. V. Morales, D. Delgado-Ruiz, and S. J. Rueda, "Comprehensive Security for Body Area Networks: A Survey," *Int. J. Netw. Secur.*, vol. 21, no. 2, p. 342, 2019, doi: 10.6633/IJNS.201903.
- [7] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Networks*, vol. 70, pp. 23–43, Mar. 2018, doi: 10.1016/J.ADHOOC.2017.11.006.
- [8] K. R. S. Bharathi and R. Venkateswari, "Security challenges and solutions for wireless body area networks," *Adv. Intell. Syst. Comput.*, vol. 810, pp. 275–283, 2018, doi: 10.1007/978-981-13-1513-8_29/TABLES/1.
- [9] R. Nidhya and S. Karthik, "Security and privacy issues in remote healthcare systems using wireless body area networks," *EAI/Springer Innov. Commun. Comput.*, pp. 37–53, 2019, doi: 10.1007/978-3-030-00865-9_3/FIGURES/1.
- [10] A. Joshi and A. K. Mohapatra, "Authentication protocols for wireless body area network with key management approach," *J. Discret. Math. Sci. Cryptogr.*, vol. 22, no. 2, pp. 219–240, Feb. 2019, doi: 10.1080/09720529.2019.1582869.
- [11] S. Chaudhary and A. Singh, "Wireless Body Sensor Network (WBSN) Security and Privacy Issues: A Survey | Request PDF." https://www.researchgate.net/publication/335421430_Wireless_Body_Sensor_Network_WBSN_Security_and_Privacy_Issues_A_Survey (accessed Dec. 14, 2022).
- [12] M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, "Authentication Techniques and Methodologies used in Wireless Body Area Networks," *J. Syst. Archit.*, vol. 101, Dec. 2019, doi: 10.1016/J.SYSARC.2019.101655.
- [13] M. Roy, C. Chowdhury, and N. Aslam, "Security and privacy issues in wireless sensor and body area networks," *Handb. Comput. Networks Cyber Secur. Princ. Paradig.*, pp. 173–200, Jan. 2019, doi: 10.1007/978-3-030-22277-2_7/FIGURES/10.
- [14] S. Saleem, S. Ullah, and H. Yoo, "On the Security Issues in Wireless Body Area Networks," *J. Digit. Content Technol. its Appl.*, vol. 3, no. 3, 2009, doi: 10.4156/JDCTA.VOL3.ISSUE3.22.
- [15] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A Review on Body Area Networks Security for Healthcare," *ISRN Commun. Netw.*, vol. 2011, pp. 1–8, Jun. 2011, doi: 10.5402/2011/692592.
- [16] A. Rehman, "A Review on Authentication Schemes for Wireless Body Area Networks." Jan. 01, 2013. Accessed: Dec. 14, 2022. [Online]. Available: https://www.academia.edu/31238118/A_Review_on_Authentication_Schemes_for_Wireless_Body_Area_Networks
- [17] S. S. Javadi and M. A. Razzaque, "Security and Privacy in Wireless Body Area Networks for Health Care Applications," pp. 165–187, 2013, doi: 10.1007/978-3-642-36169-2_6.
- [18] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egypt. Informatics J.*, vol. 18, no. 2, pp. 113–122, Jul. 2017, doi: 10.1016/J.EIJ.2016.11.001.
- [19] J. Kang and S. Adibi, "A Review of Security Protocols in mHealth Wireless Body Area Networks (WBAN)," *Commun. Comput. Inf. Sci.*, pp. 61–83, 2015, Accessed: Dec. 14, 2022. [Online]. Available: https://www.academia.edu/33477265/A_Review_of_Security_Protocols_in_mHealth_Wireless_Body_Area_Networks_WBAN
- [20] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Secur. Commun. Networks*, vol. 9, no. 17, pp. 4777–4803, Nov. 2016, doi: 10.1002/SEC.1642.
- [21] M. R. K. Naik and P. Samundiswary, "Wireless body area network security issues — Survey," 2016 *Int. Conf. Control. Instrumentation, Commun. Comput. Technol.*, pp. 190–194, Jul. 2016, doi: 10.1109/ICCICCT.2016.7987943.
- [22] I. A. Sawaneh, I. Sankoh, and D. K. Koroma, "A survey on security issues and wearable sensors in wireless body area network for healthcare system," 2017 14th *Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process.*, vol. 2018-February, pp. 304–308, Oct. 2017, doi: 10.1109/ICCWAMTIP.2017.8301502.
- [23] S. Zou, Y. Xu, H. Wang, Z. Li, S. Chen, and B. Hu, "A Survey on Secure Wireless Body Area Networks," *Secur. Commun. Networks*, vol. 2017, 2017, doi: 10.1155/2017/3721234.
- [24] J. A. Aman and A. S. Shah, "Routing and Security Issues in U-Healthcare Mobile, Ubiquitous and Wireless Body Area Network (WBAN)," *Int. J. Adv. Sci. Technol.*, vol. 109, pp. 23–34, 2017, Accessed: Dec. 14, 2022. [Online]. Available: https://www.academia.edu/35329146/Routing_and_Security_Issues_in_U_Healthcare_Mobile_Ubiquitous_and_Wireless_Body_Area_Network_WBAN
- [25] B. Narwal and A. K. Mohapatra, "A review on authentication protocols in wireless body area networks (WBAN)," *Proc. 3rd Int. Conf. Contemp. Comput. Informatics, IC3I 2018*, pp. 227–232, Oct. 2018, doi: 10.1109/IC3I44769.2018.9007303.
- [26] M. ; Usman et al., "Security in wireless body area networks: from in-body to off-body communications," *IEEE Access*, vol. 6, pp. 58064–58074, Oct. 2018, doi: 10.1109/ACCESS.2018.2873825.
- [27] M. S. Arshad Malik, M. Ahmed, T. Abdullah, N. Kousar, M. N. Shumaila, and M. Awais, "Wireless body area network security and privacy issue in E-healthcare," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, pp. 209–215, 2018, doi: 10.14569/IJACSA.2018.090433.
- [28] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014, doi: 10.1109/SURV.2013.121313.00064.
- [29] L. A. N. Man, S. Committee, and I. Computer, *IEEE Standard for Local and metropolitan area networks - Wireless Body Area Networks*, no. February. 2012.
- [30] S. A. Salehi, M. A. Razzaque, I. Tomeo-Reyes, and N. Hussain, "IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view," *Proc. - Asia-Pacific Conf. Commun. APCC 2016*, pp. 523–528, 2016, doi: 10.1109/APCC.2016.7581523.

- [31] “Artificial Intelligence for Disease Diagnosis and Prognosis in Smart Healthcare - Google Books.” https://books.google.com.sg/books?hl=en&lr=&id=iemuEAAAQBAJ&oi=fnd&pg=PA255&dq=wban+attacks+survey&ots=CaZJ1EkQff&sig=hW7bzcMpurmEaksIs8_-ttoMkaE&redir_esc=y#v=onepage&q=wban+attacks+survey&f=false (accessed Mar. 08, 2023).
- [32] “802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6 : Wireless Body Area Networks.” 2012.
- [33] O. León, J. Hernández-Serrano, and M. Soriano, “Securing cognitive radio networks,” *Int. J. Commun. Syst.*, vol. 23, no. 5, pp. 633–652, 2010, doi: 10.1002/dac.
- [34] K. Hasan, X. W. Wu, K. Biswas, and K. Ahmed, “A Novel Framework for Software Defined Wireless Body Area Network,” *Proc. - Int. Conf. Intell. Syst. Model. Simulation, ISMS*, vol. 2018-May, pp. 114–119, Mar. 2019, doi: 10.48550/arxiv.1903.09285.
- [35] M. Al Shayokh, A. Abeshu, G. B. Satrya, and M. A. Nugroho, “Efficient and secure data delivery in software defined WBAN for virtual hospital,” undefined, pp. 12–16, Jan. 2016, doi: 10.1109/ICCEREC.2016.7814973.
- [36] J. L. Sarkar et al., “I-Health: SDN-Based Fog Architecture for IIoT Applications in Healthcare,” *IEEE/ACM Trans. Comput. Biol. Bioinforma.*, 2022, doi: 10.1109/TCBB.2022.3193918.
- [37] R. Kumari, P. Nand, and R. Astya, “Integration of Blockchain in WBAN,” undefined, vol. 2019-January, pp. 144–149, Oct. 2019, doi: 10.1109/ICCCIS48478.2019.8974478.
- [38] “(PDF) Challenges of Integrating Blockchain in Wireless Body Area Network.” https://www.researchgate.net/publication/328891054_Challenges_of_Integrating_Blockchain_in_Wireless_Body_Area_Network (accessed Dec. 12, 2022).
- [39] F. Akhtar and M. H. Rehmani, “Energy Harvesting for Self-Sustainable Wireless Body Area Networks,” *IT Prof.*, vol. 19, no. 2, pp. 32–40, Mar. 2017, doi: 10.1109/MITP.2017.34.
- [40] M. U. H. Al Rasyid, W. Yuwono, S. Al Muharom, and A. H. Alasiry, “Building platform application big sensor data for e-health wireless body area network,” *Proc. - 2016 Int. Electron. Symp. IES 2016*, pp. 409–413, Feb. 2017, doi: 10.1109/ELECSYM.2016.7861041.
- [41] A. Jamthe and D. P. Agrawal, “Harnessing Big Data for Wireless Body Area Network Applications,” *Proc. - 2015 Int. Conf. Comput. Intell. Commun. Networks, CICN 2015*, pp. 868–875, Aug. 2016, doi: 10.1109/CICN.2015.172.
- [42] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, “Anomaly detection in medical wireless sensor networks using SVM and linear regression models,” *E-Health Telemed. Concepts, Methodol. Tools, Appl.*, vol. 1, pp. 466–486, Sep. 2015, doi: 10.4018/978-1-4666-8756-1.CH024.
- [43] T. Ali, M. Nauman, and S. Jan, “Trust in IoT: dynamic remote attestation through efficient behavior capture,” *Cluster Comput.*, vol. 21, no. 1, pp. 409–421, Mar. 2018, doi: 10.1007/S10586-017-0877-5/TABLES/2.
- [44] S. Žulj, G. Šeketa, D. Džaja, L. Celić, and R. Magjarević, “Virtual reality system for assisted exercising using wban,” *IFMBE Proc.*, vol. 45, pp. 721–722, 2015, doi: 10.1007/978-3-319-11128-5_179/COVER.