HAJAR, M.S., KALUTARAGE, H.K. and AL-KADRI, M.O. 2023. Security challenges in wireless body area networks for smart healthcare. In Mostefaoui, G.K., Islam, S.M.R. and Tariq, F. (eds.) *Artificial intelligence for disease diagnosis and prognosis in smart healthcare*. Boca Raton: CRC Press [online], chapter 15, pages 255-286. Available from: https://doi.org/10.1201/9781003251903-15

Security challenges in wireless body area networks for smart healthcare.

HAJAR, M.S., KALUTARAGE, H.K. and AL-KADRI, M.O.

2023

CHAPTER 1

Security Challenges in Wireless Body Area Networks for Smart Healthcare

Muhammad Shadi Hajar

School of Computing, Robert Gordon University, Aberdeen, UK.
Email: m.hajar@rgu.ac.uk

Harsha Kumara Kalutarage

School of Computing, Robert Gordon University, Aberdeen, UK.
Email: h.kalutarage@rgu.ac.uk

M. Omar Al-Kadri

School of Computing & Digital Tech, Birmingham City University, Birmingham, UK.
Email: omar.alkadri@bcu.ac.uk

CONTENTS

In the era of communication technologies, wireless healthcare networks enable innovative applications to enhance the quality of patients' lives, provide useful monitoring tools for caregivers, and allow timely intervention. However, security concerns are still holding back the widespread adoption of this promising technology. Insecure data communication violates the patients' privacy and may endanger their lives due to improper medical diagnosis or treatment. Although traditional security countermeasures, including authentication, encryption and data integrity are essential to protect the network from external adversaries, more advanced AI-based security schemes are necessary to protect the network from internal threats.

This chapter starts with a concise introduction about Wireless Body Area Network (WBAN) complies with the IEEE 802.15.6 standard, which provides the reader with the necessary information to understand the rest of the contents in this chapter. Then, WBAN threats and countermeasures are comprehensively researched with a particular focus on AI enabled methods. The potential attacks are widely investigated. Finally, traditional security countermeasures are discussed, followed by Intrusion Detection Systems (IDS) and Trust Management System (TMS).

1.1 INTRODUCTION

A Wireless Body Area Network (WBAN) is a special kind of Wireless Sensor Network (WSN) used mainly to monitor the body's physiological signs. It consists of tiny biomedical sensor nodes that are distributed either on the human body or implanted inside it. The first and the only international standard for WBAN is defined in IEEE 802.15.6 [33], which was released in 2012. This standard defines reliable, low power and short range wireless communications with a vast range of data rates for a variety of healthcare applications. WBAN supports data rates starting from tens of Kbps (narrowband) up to 10 Mbps (ultra-wideband).

WBAN provides a promising technology to revolutionize future healthcare applications by providing real-time monitoring tools for caregivers and allowing timely medical interventions. Different kinds of sensor nodes, wearable, Implantable Medical Devices (IDMs) and surrounding nodes are designed to sense the physiological signals of the human body and forward them to a remote medical server. These periodical medical readings include a vast range of bio-signals depending on the sensing unit of the Sensor Node (SN), such as blood pressure, glucose level, Electrocardiogram (ECG), heart rate, Electromyogram (EMG), body temperature and oxygen satura-

tion (SpO2). This continuous awareness of the patient's vital functions provides more flexibility and mobility to patients and enhances their life quality.

The widespread adoption of this revolutionized technology is driven by several factors. The rapid growth of the aging population across the globe where it is projected to reach around 1.5 billion in 2050, which is more than double the number in 2019 [78]. In the UK, for instance, the aging population over 85 is expected to double by the mid of 2041 [59]. Moreover, the overall expenditure of healthcare systems is increasing significantly, and the proportion of overloaded health professionals is also overgrowing. For instance, around 15% of the health budget is dedicated to diabetes, which will be one of the most causes of death by 2030 [83]. These reasons push firmly towards the adoption of this neoteric technology. However, security and privacy challenges are still holding back the wide adoption of this technology because any compromise could violate the patient's privacy and endanger their life. For instance, a sensor node with an insulin pump capability could receive a compromised order to inject an insulin overdose into the bloodstream. WBAN is vulnerable to vast kinds of security attacks and misbehavior activities. Although traditional security countermeasures, such as authentication, encryption and integrity validation, are essential to protect the network from different kinds of threats, they are not enough to ensure a high level of security and privacy. Therefore, more advanced AI-based security countermeasures such as Intrusion Detection System (IDS) and Trust Management System (IDS) are introduced in the literature to enhance the overall security and protect the network from potential innovative attacks which will be discussed further throughout this chapter [23].

This chapter sets off by providing an overview of AI in healthcare in section 1.2, followed by a brief background about WBAN technology in section 1.3. Then, section 1.4 comprehensively presents the WBAN threats and vulnerabilities, while section 1.5 explores different security countermeasures, including secure communication, intrusion detection, and trust management.

1.2 AI IN HEALTHCARE

The tremendous development in the field of Artificial Intelligence (AI) opens the door wide to think about adopting this revolutionized technology for healthcare applications. Body Sensor Nodes (BSNs) empowered by the advancements of AI are now able to collect the physiological signs of the human body and provide high-frequency and high-resolution remote monitoring tools. This technique helps physicians to diagnose, predict and intervene when necessary. Moreover, the collected healthcare data is used to spot patterns, predict outcomes, verify hypotheses and optimize operations. For instance, AI-based prediction models outperform doctors in predicting skin cancers by analyzing skin lesions using deep Convolutional Neural Networks (CNNs) [15]. Another example, the researcher in [64] built a prediction model to predict bacterial Urinary Tract Infection (UTI) using a random forest algorithm. They also built a prescribing policy based on their prediction model to evaluate the physicians' prescriptions. The prediction model's performance had an AUC of 0.731, and the results showed a decrease of 7.42% of antibiotic use in Denmark, a one of the conserva-

tive countries of antibiotic use, which gives an indicator to better results for other countries.

Moreover, AI is widely used in protecting healthcare networks from security breaches [29, 9]. Supervised, unsupervised, and reinforcement learning are all introduced to enhance the overall security of healthcare networks. Supervised algorithms, such as Support Vector Machine (SVM), random forest and K-Nearest Neighbors (KNN) are introduced to detect network intrusions and spoofing attacks. The unsupervised learning algorithm, such as k-means clustering, has been used to detect Denial of Service (DoS) attacks. Furthermore, reinforcement learning is widely adopted for security and routing applications.

1.3 WIRELESS BODY AREA NETWORK

The standardization process of wireless sensor networks for healthcare applications is triggered by projecting its importance and critical role in the near future. Therefore, the Physical (PHY) and Medium Access Control (MAC) layers are defined in the IEEE 802.15.6 [33] in order to ensure interoperability amongst devices from different vendors. The standard supports three kinds of physical layers Narrowband (NB) PHY, Ultra-wideband (UWB) PHY and Human Body Communication (HBC) PHY, which support different frequency bands and data rates in order to meet the requirements of different potential applications.

1.3.1 WBAN Topology

Each Body Area Network (BAN) consists of one single sink node and a set of sensor nodes. The maximum number of nodes within one BAN is specified by 64 in the IEEE 802.15.6 standard. The star topology is adopted in the standard with two kinds of communications, simple and extended. In the simple one-hop star topology, all nodes should be within the direct communication range of the sink, while in the extended two-hop star topology, some nodes relay traffic to others as shown in Fig. 1.1.

WBAN nodes could be classified according to their role, deploying location and functionality [7]. Based on their roles, sensor nodes could be classified into:

- *Hub*: It could also be called sink or coordinator. It is the gateway of BAN's nodes to other BANs and networks. It usually has superior resources compared to other nodes as all BAN traffic goes through it.
- *Relay node*: In the extended star topology, some nodes have the relaying capability to help nodes that are not in the direct communication range.
- *End node*: These nodes are designed to sense the bio-signals and report them to the sink either directly if they are in the direct communication range, or via relay nodes.

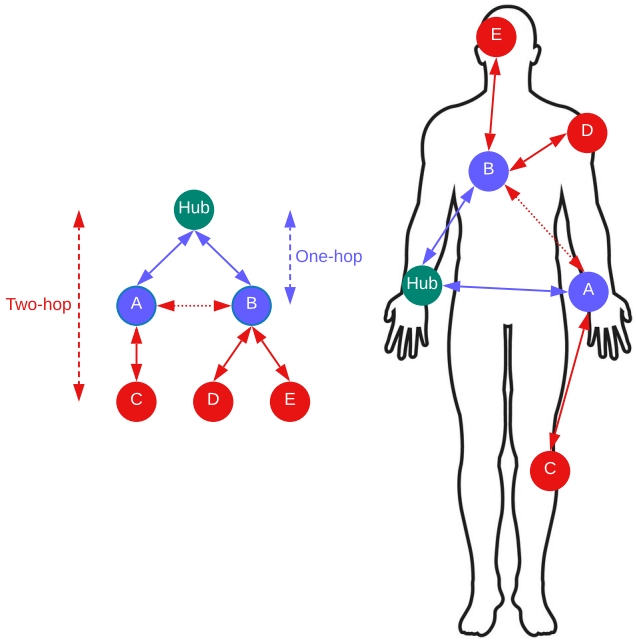

Figure 1.1 WBAN Topology

1.3.2 WBAN Communication Architecture

There are different tiers of communication in the WBAN ecosystem where AI has been utilized for security in all these layers. Generally speaking, there are three tiers of communication although few researchers suggested adding a new tier of communication between nano and micro nodes [79]. However, generally, three tiers of communication are recognized in the standard of WBAN as follows [54]:

- *Tier-1 intra-BAN communication*: All the communication within the BAN itself is regarded as a tier-1 communication, including the communication between the sensor nodes and the sink, and the communication between the sensor nodes themselves. The used frequency and data rates vary depending on the used physical layer.
- *Tier-2 inter-BAN communication*: The communication between BANs and the Access Points (APs), and between BANs themselves are regarded as a tier-2 of communication.
- *Tier-3 beyond BAN communication*: The communication beyond the WBAN ecosystem is regarded as a tier-3 of communication, which includes all the communication between the APs and the remote medical server.

The three tiers of communication are illustrated in Fig. 1.2. The figure shows a set of in-body and on-body sensor nodes forming two BANs. All sensor nodes can communicate with the hub directly if they are in the direct communication range or via relaying nodes.

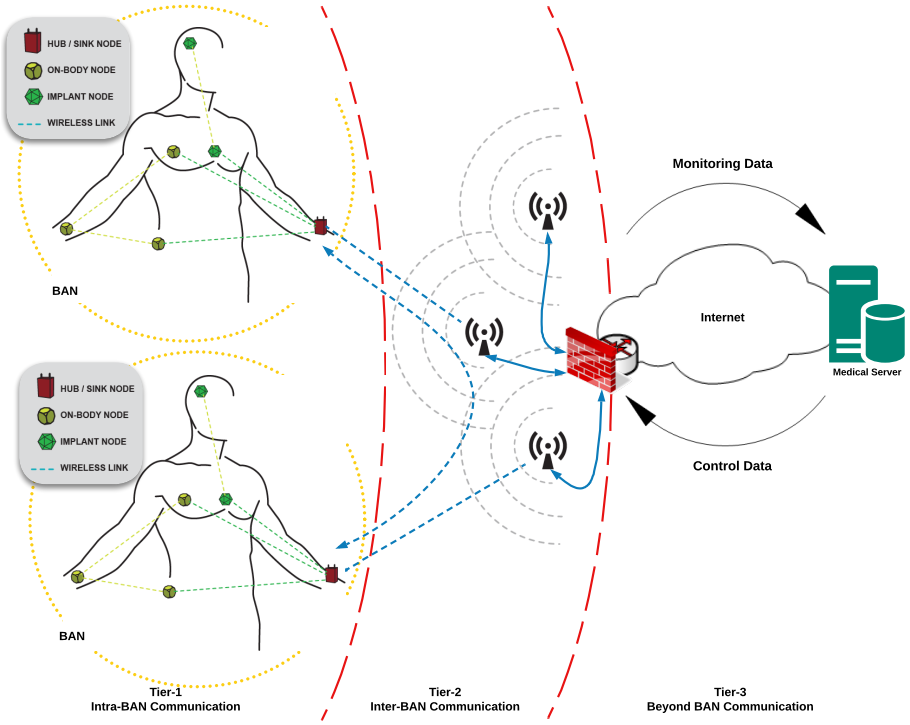

Figure 1.2 WBAN Architecture

1.3.3 Security in WBAN

Ensuring a high level of security and privacy in WBAN plays a pivotal role in adopting this technology on a large scale. The sensitive information must be protected during all phases from sensing bio-signals to storage. Any compromise could disclose patient's health records, and it even endangers the patient's life. WBAN inherits many security vulnerabilities and concerns from WSN. These inherited security concerns, in addition to the strict resource constraints impose unprecedented security requirements, and open the way to further scientific research to meet these requirements. The basic security requirements of WBAN are outlined as follows:

- *Confidentiality*: Data must be protected from being disclosed to any unauthorized party [10]. Adopting a proper encryption algorithm could protect data during transmission and storage phases. Unprotected data can be readily disclosed during transmission in open channels by eavesdropping attacks, or when stored in plain format when medical servers or nodes got compromised.

- *Integrity*: The attacker can intercept the data during the transmission phase and delete, inject or modify the transmitted packet. Confidentiality alone can not protect the data from alteration. Therefore, the receiver must be able to ensure that the received data is original and has not been modified on its way [62].

- *Availability*: WBAN provides critical services. The adversary may launch an attack to disrupt the communication between the caregivers and the sensor nodes [3]. Disrupting the network operation may endanger the patient's life. Therefore, maintaining the ability to access the required data under any circumstances is a crucial requirement.

- *Data Authentication*: When the integrity requirement is fulfilled, the receiver can ensure that the received data is intact and has not been modified during the transmission phase. However, the receiver can not verify that the received message is sent by the original sender, which is believed to be [13]. Therefore, to achieve data authentication, IEEE 802.15.6 standard defines the Message Authentication Code (MAC) in order to ensure that the received message is sent by the original sender.

- *Data Freshness*: Data freshness is an essential requirement to ensure that no adversary can capture messages and replay them later [41]. A replay attack may cause instability and confusion in the network and could make the physicians take wrong decisions based on inaccurate information. Two levels of freshness can be achieved, strong and weak freshness. In strong freshness, the received message must be in order and on time; however, there is no guaranteed delay in the weak freshness.

- *Secure Management*: Cryptographic security countermeasures, such as authentication, encryption and integrity validation require security keys. Therefore, secure management is essential to ensure that the security keys are distributed in a secure manner [40].

There are three levels of security defined in the IEEE 802.15.6 standard. All nodes, including the sink, have to choose one of these levels in accordance with their application requirements.

- *Level-0 unsecured communication*: In the first security level, there is no security countermeasure applied. Unsecured frames are transmitted without authentication, encryption, integrity, or even replay defence.

- *Level-1 authentication*: In the second security level, authenticated frames are exchanged but not encrypted. Moreover, integrity validation and replay defence are provided; however, no confidentiality and privacy protection.

- *Level-2 authentication and encryption*: The third security level provides the highest security. Authenticated and secured frames are exchanged at this level. Moreover, confidentiality, privacy protection, replay defence and integrity validation are all provided at this level.

During the association process, each node and the hub need jointly to select one of the aforementioned levels based on their respective requirements. The security key generation is shown in Fig. 1.3. A pre-shared Master Key (MK) is activated or

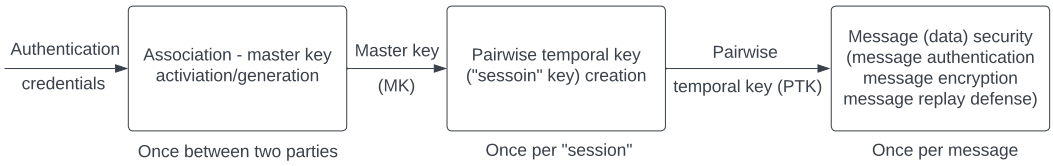

Figure 1.3 Security Structure

established during the association process for secure unicast communication. Afterward, Pairwise Temporal Key (PTK) is created by calling the PTK creation procedure, which is used for a communication session between two nodes. Moreover, the hub generates a Group Temporal Key (GTK) and shares it with the corresponding multicast group nodes in a unicast manner in order to establish multicast secured communication.

On the other hand, recent research shows that despite all the incorporated security measures in the IEEE 802.15.6 standard, it still has some vulnerabilities. For example, analyzing the key agreement protocols to establish the pre-shared MK shows that four protocols are vulnerable to Key Compromise Impersonation (KCI) and do not fulfill the forward secrecy requirement. Furthermore, one protocol is prone to offline dictionary attack [76].

1.4 WBAN THREATS

WBAN is vulnerable to different kinds of attacks and malicious activities. There are different classifications for attacks. Based on the attack origin, they could be classified into internal and external as follows [1]:

- *Internal attacks:* These attacks are launched by internal intruders. For instance, when a node got compromised. Internal attacks are more complicated and challenging to defeat as compromised nodes have already passed the traditional security countermeasure and could have a copy of the keys. Therefore, more advanced security measures are required to protect the network [22].
- *External attacks:* These attacks are sourced from outside the network by external adversaries.

Attacks on WBAN could also be classified into passive and active as follows: [1]

- *Passive attacks:* Information gathering is the main goal of passive attacks. Although it is less harmful than active attacks, it violates the patient's privacy. Attackers could take advantage of the gathered data to launch more advanced attacks.
- *Active attacks*: A vast range of attacks are regarded as active attacks, such as DoS attacks, packet alteration attacks and route poisoning attacks. Attackers can target the network operation to deplete the resources and degrade the overall performance.

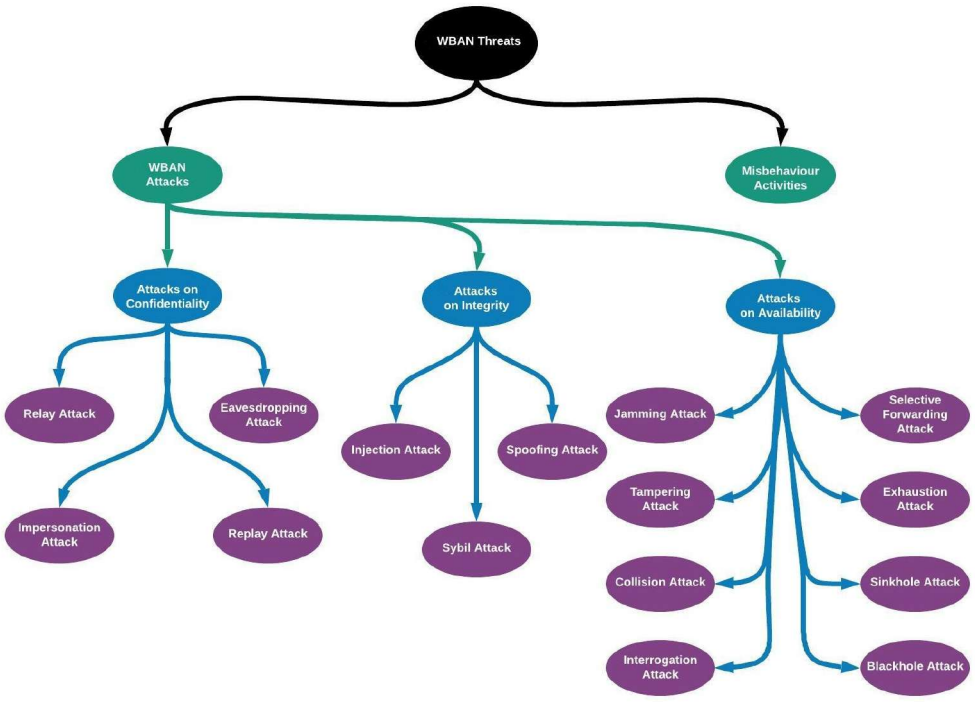

Figure 1.4 WBAN Threats Taxonomy

Moreover, WBAN is also vulnerable to different kinds of malicious activities launched by WBAN nodes. Different reasons are behind these malicious activities. Nodes could launch internal attacks when they got compromised. Moreover, even benign nodes could act selfishly in order to save resources. For example, when a relay node stops relaying packets to save power, it could disrupt the network operation. Therefore, misbehaving activities launched even by legitimate nodes are very deleterious and dangerous because cryptographic security measures are not able to defeat them. However, some advanced countermeasures, such as AI based TMS [22, 21], which will be discussed later in this chapter, can detect malicious activities like dropping attacks.

In what follows, a wide range of attacks is discussed and grouped based on CIA (Confidentiality, Integrity and Availability) security requirements they violate. It is worth mentioning that this list of attacks is not exhaustive.

1.4.1 Attacks on Confidentiality

There are many attacks to compromise the confidentiality as listed below:

- *Eavesdropping Attack:* It is a passive attack where the adversary can sniff on the transmission media to capture the exchanged packets with a view to getting access to sensitive information [2]. According to the IEEE 802.15.6 security levels, no encryption service is provided in security level-0 and level-1, which

allows the adversary to readily capture and analyze the exchanged plain frames. Moreover, even at the third security level, intelligent adversaries can capture the secret keys in the key exchange phase.

- *Replay Attack:* It is an active attack where the adversary capture and store the exchanged frames to be replayed later into the network [50]. Replay attack is a severe attack in WBAN because the replayed frames are still valid, which may cause serious consequences when a decision is made based on these messages. Therefore, a replay defence mechanism has been incorporated in security level-1 and security level-2 in the IEEE 802.15.6 standard. The first octet of the MAC frame body, namely, "Low-Order Security Sequence Number" is used to verify message freshness and detect replay attacks [33].
- *Relay Attack:* It is a kind of Man-In-The-Middle (MITM) attack. The attacker tries to intercept the communication between the sender and the receiver [41]. Thus, while the two parties think they are in direct communication with each other, the attacker can intercept all the exchanged messages.
- *Impersonation Attack:* The attacker can exploit the sniffed messages to impersonate a legal node. Successful impersonation attacks can cause deleterious consequences [67].

1.4.2 Attacks on Integrity

Integrity attacks are regarded as active attacks as the attacker tries to delete, inject or modify the exchanged frames.

- *Spoofing Attack:* Spoofing attacks can be launched in different ways to disrupt the network operation. Attackers try to alter messages to get legitimate access to resources [50]. The IEEE 802.15.6 standard supports exchanging authenticated frames. The Message Integrity Code (MIC) field is set to the Message Authentication Code (MAC) with a view to verify the authenticity and the integrity of the received frames.
- *Modification/Injection Attack:* Modification and injection attacks are kinds of MITM attacks. The attacker tries to inject new frames or alter the exchanged frames before replaying them [2]. When no integrity validation service is running, such a simple attack could cause severe consequences and affect the patient's life. For instance, the altered message could contain an emergency biosignal sent to the physicians, or it could be a command from a remote healthcare center to an insulin pump to release an insulin dose. In both scenarios, frame modification could endanger the patient's life.
- *Sybil Attack:* The attacker in this kind of attack impersonates fake identities. Then, the adversary uses the illegitimate identity to launch attacks until got detected. Once got detected, the attacker generates a new fake identity to appear as a benign node [48]. Meanwhile, the attacker has the opportunity to intercept the exchanged messages and continue the malicious activities.

1.4.3 Attacks on Service Availability

The most common attacks that impact the service availability are the Denial-of-Service attacks, in which the adversary disrupts the network operation and deprives other entities of accessing the required resources. DoS attacks can target different stack layers. The most common DoS attacks are discussed below:

- *Jamming Attack:* Jamming attacks are targeting the physical layer. It was first discussed in the literature in 1982 [80]. Since then, wireless networks are always vulnerable to jamming attacks. The adversary blocks legitimate communication within the network by intentionally interfering with the used frequency, which notably decreases the Signal-to-Interference-plus-Noise ratio (SINR). In WBAN, jammers can easily degrade the network performance, which could delay urgent and critical bio-signal messages or medication commands. Moreover, it could deplete the batteries of the sensor nodes because of the re-transmissions attempts.

- *Tampering Attack:* A tampering attack can occur when the adversary can access WBAN nodes physically. The attacker can cause hardware damage or get access to critical data, such as encryption keys [50]. Although sensor nodes are usually close to the human body, raising awareness among patients about who is authorized to handle these sensor nodes can help defeat tampering attacks.

- *Collision Attack:* A collision attack is a data link attack that occurs when more than one node transmit at the same time [36]. When an overlapped transmission happens, senders enter the re-transmission phase, which depletes the node's resources and degrade the network performance. The attacker overlaps the other's transmission intentionally, which results in a collided frame. This causes the Cyclic Redundancy Check (CRC) process on the receiver side to fail verifying the received frame and discarding it.

- *Selective Forwarding Attack:* It is one of the dropping attacks in which malicious or selfish nodes drop received frames instead of forwarding them. In a selective forwarding attack, the malicious or the selfish node selectively forwards some packets and drops others [35]. For example, in extended two-hop star topology in WBAN, relay nodes could drop all the frames sourced from a particular node.

- *Exhaustion Attack:* It is a sort of DoS attack in which the attacker tries to deplete the resources of the victimized node. For instance, in the denial of sleep attack, the victim's battery gets depleted significantly [66].

- *Sinkhole Attack:* It is a packet dropping attack in which the adversary tries to attract all the traffic within the WBAN and drop it [21]. It can be launched by sending fake routing updates showing the attacker as the best route.

- *Blackhole Attack:* It is similar to selective forwarding attacks; however, in a blackhole attack, the malicious node drop all the received messages [57].

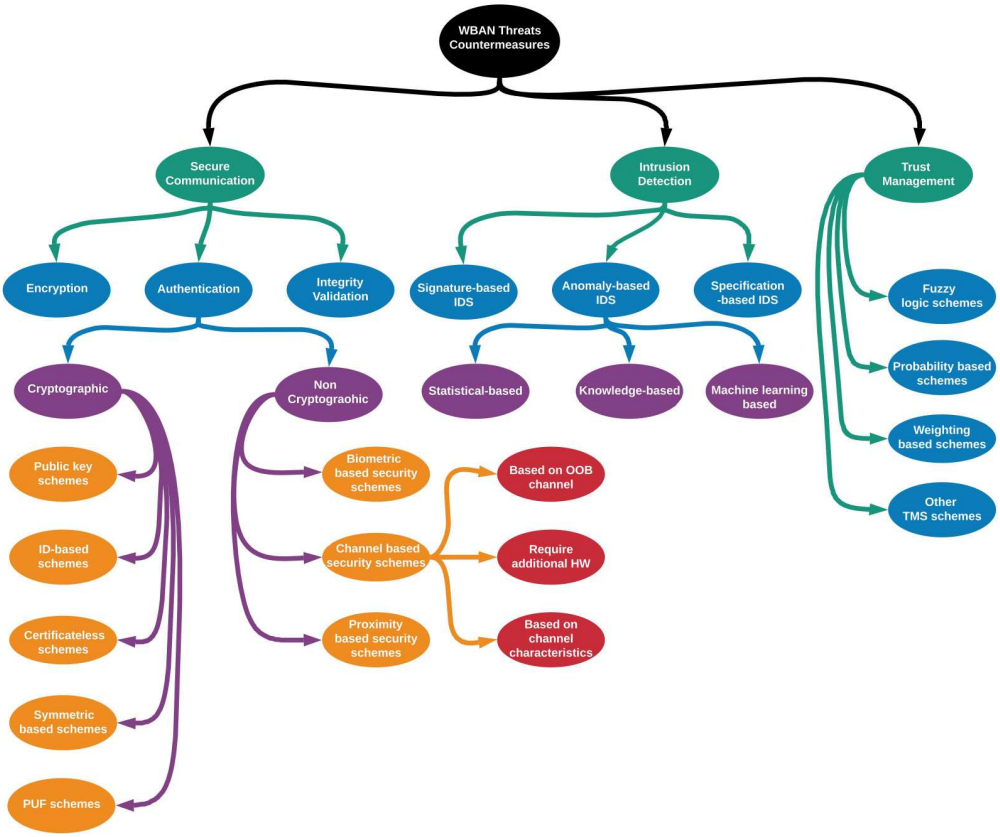

Figure 1.5 WBAN Security Countermeasures Taxonomy

1.5 WBAN THREATS COUNTERMEASURES

The WBAN nature and its critical health applications impose achieving a high level of security and privacy. Data must be protected during collection, transfer, processing, and storing. Any kind of vulnerabilities could be exploited by adversaries to launch a fatal attack. On the other hand, any proposed security measures must take into account the security requirements of WBAN and the strict resource limitations. In this section, various security countermeasures will be discussed at different levels. It is worth mentioning that WBAN security is still an open area of research and there is a limited number of WBAN-specific schemes proposed in the literature. Therefore, some security schemes discussed throughout this section are generally proposed for WSN, which have a high potential to fit WBAN requirements; however, further investigation before the adoption is highly recommended. Fig. 1.5 shows a high-level perspective of the security countermeasures discussed throughout this section.

1.5.1 Secure Communication

Secure communication is regarded as the cornerstone to guarantee the confidentiality, privacy and integrity of the WBAN. Therefore, in this subsection, the security

requirements, authentication and key establishment, integrity validation and encryption have been discussed.

1.5.1.1 Security Requirements

To ensure an end-to-end secure communication, there are some security requirements to be met by any proposed scheme that provides authentication, encryption and integrity validation.

- *Lightweight:* As WBAN has limited resources, any security scheme must be computationally lightweight [63].
- *Anonymity:* To ensure that privacy is guaranteed, outsiders should not be able to identify the involved parties in the authentication process [68].
- *Mutual authentication:* In mutual authentication, the two parties can authenticate each other with a view to protecting from impersonation attacks [84].
- *Unlinkability:* Unlinkability is a critical requirement to prevent the attacker from tracing the identity of the nodes. Moreover, the unlinkability must still be maintained even if the attacker is able to capture two frames belonging to the same sender, which means it should not be any link or association between the captured frames and the sender [46].
- *Session key establishment:* Once the authentication process is achieved successfully, a session key should be created and exchanged in a secure manner for subsequent communication between the nodes [84].
- *Forward secrecy:* It implies that the session key must still be secured in case of one or both the communicating parties get compromised. Moreover, it should still be secure even when the attacker gets one or both private keys [27]
- *Revocability:* Revocability requirement allows revoking any malicious node effectively to keep the network secure [84].
- *Non-repudiation:* By fulfilling non-repudiation requirement, senders can not deny their messages [68].
- *Resilience to well-known attacks:* Security schemes must be resilient to well-known attacks, such as replay attacks and impersonation attacks [13].

1.5.1.2 Authentication and Key Establishment

Authentication is the cornerstone to secure the network on all tiers of communication in WBAN. Considerable research has been put forward to fill this research gap in the literature. However, the majority of the proposed schemes are vulnerable to specific attacks or do not fulfill all the security requirements [60] which makes proposing a practical and secure authentication scheme for WBAN an open area for further research [46]. In what follows, the potential authentication schemes will be presented.

Non-cryptographic security schemes: The non-cryptographic authentication schemes take advantage of some physical characteristics of the targeting network, such as the human physiological signals. They have been classified as non-cryptographic because of the used technique; however, many proposed schemes are able to create secret keys to encrypt the exchanged messages.

1. *Biometric based security schemes:* Many lightweight authentication schemes are proposed in the literature based on the body bio-signals because there is a thought that these signals are difficult to be forged. A novel security scheme is proposed for WBAN in [65]. The proposed scheme is able to generate and distribute symmetric keys by sensing the ECG signal. The authors used time synchronization to avoid broadcasting the ECG signal. Moreover, the study proves the robustness of the proposed method by running informal and formal security analyses.

2. *Channel based security schemes:* Another approach to use the physical characteristics to authenticate nodes is built on the assumption that the communication channel qualities between two nodes are the same. The proposed schemes in the literature could be categorized into:

    - Security schemes based on an out-of-band (OOB) communication channel: Some schemes introduce the use of an auxiliary channel to authenticate nodes assuming that this out-of-band channel is not prone to eavesdropping attacks. For example, a visual OOB channel is introduced in [45] to help the patient authenticates sensor nodes by comparing LED blinking patterns.
    - Security schemes that require additional hardware: Few studies introduced adding additional hardware to facilitate the authentication process, such as the Good Neighbor scheme where the authors used multiple antennas at the receiver side [12].
    - Security schemes based on channel characteristics measurements: Many schemes considered the channel characteristics measurements, such as Received Signal Strength (RSS) measurements. Authors in BANA [69] and MASK-BAN [70] proposed lightweight authentication schemes based on RSS. In such schemes, there are some nodes distribution restrictions where the nodes are usually distributed within the half-wavelength range.

3. *Proximity based security schemes:* In proximity schemes, the secret key could be extracted by taking advantage of the small-scale fading variations and a third-party Radio Frequency (RF) source [51].

Cryptographic security schemes: Cryptographic security schemes vary depending on the key types, and they could be classified into the following categories.

1. *Public key signature schemes:* The Public Key Cryptography (PKC) is a robust security approach to provide authentication. It could be mathematically

implemented as an integer factorization problem like RSA or a discrete logarithmic problem like in Elliptic Curve Cryptography (ECC). However, both approaches are still regarded as greedy in consuming the limited resources of WBAN. Authors in [81] proposed a hybrid multiplication method to reduce the memory access rate, which results in speeding up the process around seven times. Moreover, an ECC-PKC library is introduced to be used for WSN [81].

2. *ID based signature schemes:* It is a kind of PKC where the public key includes identity information, and the private key is generated by a Trusted Third Party (TTP), namely, Private Key Generator (PKG). ID-PKC schemes do not meet all the security requirements of WBAN [86]. They are vulnerable to key escrow problem because of the existing TTP. Moreover, as PKG has all the private keys, it can easily decrypt all the exchanged messages and forge any signature.

3. *Certificateless signature schemes:* It is a kind of PKC that has been introduced to reduce the resource consumption of PKC and the key escrow problem of ID-PKC [4]. The inborn key escrow problem in ID-PKC has been resolved by introducing the Key Generator Center (KGC), which holds a master key instead of the private keys. The KGC is responsible for sending a partial private key (D_A) to nodes, which in turn can create their private keys. Many remote authentication schemes between the hub and the application providers have been introduced in the literature [67]. However, further research is still going on to produce a security scheme that meets all the security requirements and is not vulnerable to attacks.

4. *Symmetric based schemes:* Authors in [46] proposed a symmetric based authentication scheme using a pre-shared key and unique IDs to achieve mutual authentication, unlinkability and forward secrecy security requirements. However, the adversary can take advantage of the unmasked value (γ) to link two sessions to the same node. Therefore, a modification has been suggested by authors in [38] to fulfill the unlinkability and forward secrecy. However, this security scheme still has key escrow problem because the hub still has all the IDs in addition to the master key.

5. *Physical Unclonable Function (PUF) schemes:* Some security schemes consider the unavoidable uniqueness difference between nodes, which naturally appears during semiconductor manufacturing. Authors in [82] proposed a mutual authentication scheme between two WBAN sensor nodes with the help of the coordinator. Another security scheme is introduced in [73] for multi-hop BAN. A hierarchical authentication method has been used for nodes that are not in the communication range of the hub. The Challenge-Response Pairs (CRPs) are stored on the cloud in order to minimize storage consumption.

1.5.1.3 Integrity Validation

Integrity validation allows the receiver to ensure that the received message is intact and has not been manipulated during the transmission. A vast range of manipulation

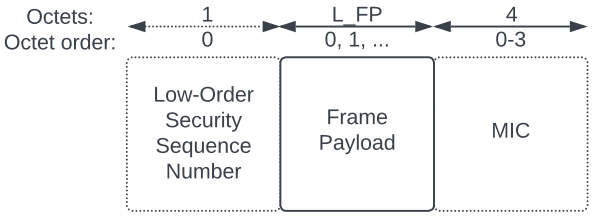

Figure 1.6 MAC Frame Body Format

can occur during the transmission, which changes the message content, whether it is caused by malicious activities or transmission errors. Changing content may include adding, removing or transposing fragments. Deploying an integrity validation module can be feasibly achieved after generating cryptographic keys [14]. However, this task is still challenging for WBAN because of its resource scarcity [49].

As discussed earlier, IEEE 802.15.6 has three levels of security where integrity validation is provided in the second and third levels [33]. Fig. 1.6 shows the WBAN MAC frame body. The length is variable and can expand to a maximum of 255 octets. WBAN entities can exchange secured and unsecured frames. Sensor nodes are to choose a security level that fulfills their security requirements during the association process. Two additional fields are used in the secured frames, Message Integrity Code (MIC) and "Low-Order Security Sequence Number". The latter is used to verify message freshness to detect replay attacks, while the MIC field is used to validate message integrity by setting it the Message Authentication Code [33].

1.5.1.4 Encryption

WBAN data plays a critical role in diseases diagnosis and treatment. Confidentiality is essential to protect this sensitive information either during transmission or storage. Abundant encryption algorithms are introduced in the literature, such as 3-DES [55] and RSA [61]. However, not all of them could fit the rigid resource constraints of WBAN. For example, encryption algorithms with long keys, countless number of rounds and huge block sizes are inapplicable to WBAN. Therefore, in 2015, the National Institute of Standards and Technology (NIST) started the process to standardize a lightweight encryption algorithm for constrained devices such as WBAN sensor nodes [52]. To design a lightweight encryption algorithm that is resource and energy efficient, the following aspect must be taken into account [71]:

- Key size: Constrained devices have minimal storage capacity. MICAz, for example, has only 4 KB storage [30]. Therefore, the small key size is an essential factor for such devices. Authors in [85] proposed SIMECK, an encryption algorithm with encryption key size that could be 64, 96, or 128 bits. It is a hardware-oriented block encryption algorithm inspired by SIMON's algorithm design [8].

- Block size: Smaller block size is another essential factor in building a lightweight

and resource efficient encryption algorithm. Authors in [8] proposed two lightweight block based encryption algorithms SPECK and SIMON. SPECK is built on Addition-Rotation-XOR (ARX) structure and supports different block sizes ranging between 32 and 128 bits. On the other hand, SIMON belongs to the same family as SPECK, but it is software-oriented.

- Number of rounds: Lightweight encryption algorithm tends to use simple operations in order to meet the stringent resource limitations. However, using simple operations like in the ARX structure requires increasing the number of rounds. Therefore, choosing an algorithm that needs a fewer number of rounds is desirable for constrained devices. Authors in [77] introduced LWE, a 3-round block cipher encryption algorithm. it uses 64 bits for key and block size with a view to fit the resource constraints of the medical sensors. Furthermore, it has been contrasted with well-know lightweight algorithms such as Rectangle [88] and TWINE [72]. The performance results show that LWE performed better in encryption/decryption rates without creating a heavy load on the infrastructure.

1.5.2 Intrusion Detection System

IDS is a vital cyber security tool to monitor the network and detect any malicious activities. It is able to resist inside attacks launched by nodes that have passed the traditional cryptographic security measures. It is regarded as an additional layer of protection to detect and defeat internal and external abuses. Different methods are proposed in the literature to achieve an effective IDS scheme which could be classified based on the detection method into:

1.5.2.1 Signature based IDS

It is also called rule based IDS. In this kind of IDS, a profile (signature) is created for each previously known attack. This signature is then used to detect any malicious activity that matches the pre-defined attack pattern. The main disadvantage of this kind of detection method is the inability to detect unknown attacks. This requires updating the signature database periodically in order to detect new attacks. Authors in [5] proposed a lightweight IDS inspired by the human immune system for resource constrained networks. It adopted the properties of the immune cells with a signature database. For example, the detection nodes represent the Dendritic cells and similarly, T-cell and B-cell are mapped to appointed nodes in the detection process. The detection node is able to stimulate other members in the detection process.

1.5.2.2 Anomaly based IDS

In this kind of IDS, the normal network operation and nodes behaviour are profiled. The detection engine is then able to report anomalies when there is a certain amount of variation. Authors in [11] suggested a classification of anomaly based IDS as follows:

Statistical based: The statistical based anomaly IDS builds a reference profile for the normal network operation without malicious activities. Afterward, the IDS monitors the network, periodically generates a profile and compares it with the reference profile to compute the anomaly score. If the anomaly score exceeds a certain threshold, then an anomaly is detected. Authors in [29], proposed a sink assistant statistical IDS for WBAN. The proposed scheme is successfully able to detect replay attacks, jamming attacks, data forging attacks, exhausting DoS attacks and selective forwarding attacks. The detection performance shows high true positive and low false positive rates. Another statistical IDS is proposed in [31]. The proposed scheme used a variety of statistics, such as Forward Percentage (FP), Maximum Sequence Counter (MSC), malicious flooding on a specific target, Global Forward Percentage (GFP) and Local Forward Percentage (LFP), to detect abnormal behaviour. Moreover, the proposed scheme is able to provide more details about the attack, such as the attack type and source. The performance results show high accuracy in detecting selfish activities and less accuracy in detecting blackhole and spoofing attacks.

Knowledge based: Knowledge based anomaly IDS depends on having prior knowledge about the network conditions in both cases normal operation and under certain attacks. Different techniques could be used in this kind of IDS, such as expert systems, description languages, finite state machine, data clustering and outlier detection [5, 11].

Machine learning based: Machine learning based IDS is an intelligent approach to detect abnormal activities in the network. A detection model is built using a machine learning algorithm and trained using example patterns from a real network. The advantage of this data-driven detection engine is the ability to detect even unknown attacks. Many machine learning algorithms have been used to build a detection model, such as SVM [9] and Random Forest [47]. The authors in [74] proposed iDetect, a distributed intelligent IDS to detect WBAN attacks. The model is built using a multi-objective genetic algorithm to make a trade-off between high detection performance and resource consumption. The performance results show a good detection accuracy against jamming attacks, random jamming attacks and selective forwarding attacks. A distributed IDS framework with a mobile agent is introduced in [75] for WBAN. The detection process migrates from one sensor node to another in the WBAN, which allows all sensor nodes to share the detection overhead. The results show that the proposed framework was able to reduce power consumption. Authors in [58] used also the mobile agent technique. They proposed a hierarchical and distributed IDS with autonomous mobile agents. The proposed framework has been evaluated for the following machine learning algorithms Decision Tree (DT), SVM, RF, Naive Bayes Classifier (NBC) and K-Nearest Neighbor (KNN). The reported performance results showed a rise of 6% in the consumed power. HEKA IDS is proposed in [56], which is a passive IDS that can monitor and detect anomalies. The authors first launched several attacks on medical devices to find out vulnerabilities. They run eavesdropping attacks, MITM attacks, replay attacks and DoS attacks. The

proposed model is evaluated for four machine learning algorithms, SVM, RF, DT and KNN. The performance results show an accuracy around 98% for the aforementioned attacks. Furthermore, they evaluated the proposed scheme for the composite attacks, false data injection attack with MITM attack, and replay attack with MITM attack. The results show an accuracy of around 95%. Authors in [20] built a healthcare monitoring testbed. They built a dataset of 16000 records of normal and malicious conditions. A combination of network and biometrics features are used to train and test four machine learning algorithms KNN, ANN, SVM and RF. The performance results show that using combined features can improve the accuracy between 7% and 25% in some cases.

1.5.2.3 Specification based IDS

It is somehow located between the anomaly based IDS and the signature based IDS. First, the specifications and the constraints which describe a program or a protocol are defined. Then the system will monitor the running program or protocol with respect to the defined specifications and constraints [11].

1.5.3 Trust Management System

Cryptographic security measures are imperative to protect WBAN from security breaches and privacy violations. However, internal attacks, malicious activities and selfish behaviour could not be detected and defeated using this kind of security countermeasures. For instance, a sensor node, which passed all cryptographic measures and is regarded a legitimate node, could stop relaying frames for others and consequently disrupt the network operation. Therefore, a trust relationship between WBAN nodes could enhance the overall security and protect the network from malicious activities. Therefore, it is necessary to deploy an effective TMS that can continuously monitor the behaviour of sensor nodes with a view to differentiate between trustworthy nodes and untrustworthy ones. The trust relationship could be defined as follows *Node X trusts node Y if and only if X has adequate confidence in Y's behavior and performance in the future* [23]. As with other security schemes, deploying a trust management scheme in WBAN is a challenging task [34]. Thus, more consideration must be given to the WBAN architecture, resource limitation, communication overhead and TMS attacks. In addition to its desirable security protection, trust management has been introduced in different applications, such as trust based routing protocols [87], access control and role assignment [53].

The trust relationship is usually evaluated using two components based on the source of information, direct trust and indirect trust. In direct trust, the trustor directly monitors the trustee and records the successful and unsuccessful interactions. The indirect trust component is evaluated based on the received recommendations from other nodes in the network. The trustor could always consider this second-hand information, or may only consider them when no sufficient observations history is available to assess the trustee. Unfortunately, the indirect trust process is resource consuming and prone to dishonest recommendation attacks [24].

Although TMS is introduced to enhance the overall security, it could be vulnerable to some internal attacks, which makes designing a robust TMS a challenging task.

- On-off attack: in an on-off attack, the smart adversaries change their behaviour alternately to keep themselves undetected and their trust values above the trust threshold. This kind of attack can manipulate the TMS and disrupt the network operation [43].
- Bad-mouthing attack: One of the dishonest recommendations attacks. In this kind of attack, the recommender tends to give negative recommendations about a trustworthy node to destroy its reputation [26].
- Ballot stuffing attack: Another type of dishonest recommendations attacks, in which the recommender gives positive recommendations about malicious nodes to promote them [39].
- Collusion attack: Unlike bad-mouthing and ballot stuffing attacks where just one malicious node provides dishonest recommendations, in collusion attacks, a group of malicious nodes colludes to provide dishonest recommendations. Collusion attacks are challenging to detect and could mislead the system to make unfair decisions [25].
- Selective forwarding attack: Discussed in section 1.4.

The trust management schemes could be divided into four main groups based on their trust evaluation method:

1.5.3.1 Fuzzy logic based TMS

The trust relationship is evaluated in this kind of TMS using fuzzy logic and predefined criteria that have a fuzzy-nature. The authors in [28] proposed DTMS, a distributed fuzzy logic based trust management scheme. Each node inside the network monitors the others' behaviour and forecasts their trustworthiness with a view to remove malicious, compromised and selfish nodes. DTMS used two weighting techniques. The first is used to estimate the current trust based on direct observations and second-hand information from neighbor nodes, while the second is used to evaluate overall trust based on the current trust and the trust history. DTMS shows superior performance compared with benchmark schemes. However, using trust matrices and tables in addition to considering many factors to estimate the trust produce a significant network overhead [37]. FTM-IoMT [6] is another fuzzy based TMS. It has been proposed for the Internet of Medical Things (IoMT) to protect from Sybil attacks. The authors adopted a centralized approach that uses features like integrity, receptivity and compatibility to evaluate the trust value. The performance results show a good detection accuracy. However, it also shows a noticeable processing overhead. Therefore, further investigation is required to reduce the server-side overhead and enhance the packet delivery delay.

1.5.3.2 Probability based TMS

The probability distribution theory is widely used in the literature to infer the trust value from former estimations. The beta probability distribution is approximately the most used one. However, few schemes are built on different probability distributions such as exponential probability distribution and binomial probability distribution [89, 17]. RFSN [19] is regarded the first beta trust management scheme in the literature [23]. The authors used the watchdog technique to monitor the behaviour of adjacent sensor nodes and collect observations which are then used to update the posterior reputation value. The authors in [22] proposed a lightweight trust management scheme for Wireless Medical Sensor Network (WMSN). LTMS provided two algorithms to evaluate the trust relationship. The first is proposed to fit the strict resource limitations of in-body sensor nodes, while the second is provided by further protection from on-off attacks and proposed to fit on-body and off-body sensor nodes. The two proposed algorithms have contrasted with benchmark trust schemes and showed superior performance in terms of attack detection and processing overhead. ETRES [89] is another probability based trust scheme. The authors used the exponential distribution to evaluate the trust relationship, assuming that the future behaviour should have the same mode as the old one. The authors suggest using the entropy theory to evaluate the uncertainty to reduce the overhead caused by considering an indirect trust module. Moreover, the authors used a weighting technique to emphasize the most reputable recommenders and the recent observations. The performance results of ETRES showed a slight improve compared to RFSN [18] and BTMS [16].

1.5.3.3 Weighting based TMS

In this kind of TMS, the trust relationship is evaluated by weighting the performance of other sensor nodes over time. It is easy to implement and deploy; however, it does not have a solid statistical or mathematical foundation [34]. The authors in [42] proposed a weighting based trust scheme with a risk assessment to ensure a quick reaction to malicious activities. The risk assessment module makes destroying the trust easier than building it, which enhances the reliability of the proposed scheme. The overall trust value is evaluated using direct trust, received recommendations, risk factor and the previous trust value. Another weighting based TMS is RaRTrust [44]. The authors used both reputation and risk to evaluate the trust relationship with a view to defeat on-off attacks. Moreover, they adopted a timing window for ratings to reduce network congestion and delay. As a result, RaRTrust shows resiliency to on-off attacks and bad-mouthing attacks, while TMR is just able to defeat on-off attacks.

1.5.3.4 Other TMSs

Some trust management schemes do not fall within the previous classification. For instance, in [32], the authors proposed a cluster based with a 3-tier architecture trust management scheme. Tier-1 only considers nodes registration, while tier-2 defines five levels of misbehaviour activities to secure the data communication between nodes,

and the third tier is to monitor the energy consumption and migrate the cluster head process to another node. The proposed scheme evaluates the trust relationship using previous information and second-hand information to find out malicious nodes.

1.6 CONCLUSION

In this chapter, the current research on WBAN has been comprehensively investigated with a particular focus on security. A brief introduction about WBAN and its architecture and topology was presented first to provide the reader with the required information to comprehend the chapter's content readily. Next, attacks on WBAN and security requirements have been widely discussed. Finally, security countermeasures at different levels have been investigated, including secure communication, intrusion detection, and trust management.

Due to the sophisticated nature of modern attacks on WBAN, traditional signature-based methods would not be sufficient to mitigate them effectively. Instead, more advanced methods supported by recent developments in AI should be implemented. AI systems are trained to identify malware, recognize network traffic patterns and detect APT attacks before reaching the target. Therefore, integrating AI into WBAN security would be the greatest method to detect and respond to WBAN attacks in real-time and provide authenticity protection.

Bibliography

[1] Farhan Abdel-Fattah, Khalid A Farhan, Feras H Al-Tarawneh, and Fadel Al-Tamimi. Security challenges and attacks in dynamic mobile ad hoc networks manets. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pages 28–33. IEEE, 2019.

[2] Moshaddique Al Ameen, Jingwei Liu, and Kyungsup Kwak. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, 36(1):93–101, 2012.

[3] Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar, and Shahaboddin Shamshirband. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, 18(2):113–122, 2017.

[4] Sattam S Al-Riyami and Kenneth G Paterson. Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security*, pages 452–473. Springer, 2003.

[5] Vishwa Teja Alaparthy and Salvatore Domenic Morgera. A multi-level intrusion detection system for wireless sensor networks based on immune theory. *IEEE Access*, 6:47364–47373, 2018.

[6] Ahmad Almogren, Irfan Mohiuddin, Ikram Ud Din, Hisham Al Majed, and Nadra Guizani. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *IEEE Internet of Things Journal*, 2020.

[7] Deena M Barakah and Muhammad Ammad-uddin. A survey of challenges and applications of wireless body area network (wban) and role of a virtual doctor server in existing architecture. In *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, pages 214–219. IEEE, 2012.

[8] Ray Beaulieu, Stefan Treatman-Clark, Douglas Shors, Bryan Weeks, Jason Smith, and Louis Wingers. The simon and speck lightweight block ciphers. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2015.

[9] Mohammadreza Begli and Farnaz Derakhshan. A multiagent based framework secured with layered svm-based ids for remote healthcare systems. *arXiv preprint arXiv:2104.06498*, 2021.

[10] KR Siva Bharathi and R Venkateswari. Security challenges and solutions for wireless body area networks. In *Computing, Communication and Signal Processing*, pages 275–283. Springer, 2019.

[11] Ismail Butun, Salvatore D Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 16(1):266–282, 2014.

[12] Liang Cai, Kai Zeng, Hao Chen, and Prasant Mohapatra. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In *NDSS*, 2011.

[13] Sravani Challa, Mohammad Wazid, Ashok Kumar Das, and Muhammad Khurram Khan. Authentication protocols for implantable medical devices: taxonomy, analysis and future directions. *IEEE Consumer Electronics Magazine*, 7(1):57–65, 2017.

[14] Djamel Djenouri, Lyes Khelladi, and Nadjib Badache. Security issues of mobile ad hoc and sensor networks. In *IEEE Communications Surveys Tutorials*, volume 7, pages 2–28. IEEE Communications Society, 2005.

[15] Andre Esteva, Brett Kuprel, Roberto A Novoa, Justin Ko, Susan M Swetter, Helen M Blau, and Sebastian Thrun. Dermatologist-level classification of skin cancer with deep neural networks. *nature*, 542(7639):115–118, 2017.

[16] W Fang, X Zhang, Z Shi, Y Sun, and L Shan. Binomial-based trust management system in wireless sensor networks. *Chin J Sens Actuat*, 28(5):703–708, 2015.

[17] Weidong Fang, Chunsheng Zhu, Wei Chen, Wuxiong Zhang, and Joel JPC Rodrigues. Bdtms: Binomial distribution-based trust management scheme for healthcare-oriented wireless sensor network. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 382–387. IEEE, 2018.

[18] Saurabh Ganeriwal, Laura K Balzano, and Mani B Srivastava. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(3):15, 2008.

[19] Saurabh Ganeriwal and Mani B. Srivastava. Reputation-based framework for high integrity sensor networks. In *Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 66–77. ACM, 2004.

[20] Anar A Hady, Ali Ghubaish, Tara Salman, Devrim Unal, and Raj Jain. Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, 8:106576–106584, 2020.

[21] Muhammad Shadi Hajar, M Omar Al-Kadri, and Harsha Kalutarage. Etaree: An effective trend-aware reputation evaluation engine for wireless medical sensor networks. In *2020 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2020.

[22] Muhammad Shadi Hajar, M Omar Al-Kadri, and Harsha Kalutarage. Ltms: A lightweight trust management system for wireless medical sensor networks. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1783–1790. IEEE, 2020.

[23] Muhammad Shadi Hajar, M Omar Al-Kadri, and Harsha Kumara Kalutarage. A survey on wireless body area networks: architecture, security challenges and research opportunities. *Computers & Security*, page 102211, 2021.

[24] Muhammad Shadi Hajar, Harsha Kalutarage, and M Omar Al-Kadri. Trustmod: A trust management module for ns-3 simulator. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2021.

[25] Guangjie Han, Jinfang Jiang, Lei Shu, Jianwei Niu, and Han-Chieh Chao. Management and applications of trust in wireless sensor networks: A survey. *Journal of Computer and System Sciences*, 80(3):602–617, 2014.

[26] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V Vasilakos. Retrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE transactions on information technology in biomedicine*, 16(4):623–632, 2012.

[27] Debiao He and Sherali Zeadally. Authentication protocol for an ambient assisted living system. *IEEE Communications Magazine*, 53(1):71–77, 2015.

[28] J Hossein, RA Mohammad, et al. A fuzzy fully distributed trust management system in wireless sensor networks. *International Journal of Electronics and Communications*, 9(17):1–10, 2016.

[29] Xuyang Hou, Jingjing Wang, Chunxiao Jiang, Sanghai Guan, and Yong Ren. A sink node assisted lightweight intrusion detection mechanism for wban. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.

[30] CMT. http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet t.pdf. Micaz. Accessed: 07-11-2019.

[31] Yi-an Huang and Wenke Lee. A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 135–147. ACM, 2003.

[32] Syed Asad Hussain, Imran Raza, and Muhammad Mohsin Mehdi. A cluster based energy efficient trust management mechanism for medical wireless sensor networks (mwsns). In *2018 5th International Conference on Electrical and Electronic Engineering (ICEEE)*, pages 433–439. IEEE, 2018.

[33] IEEE. Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks. *IEEE Std 802.15.6-2012*, pages 1–271, Feb 2012.

[34] Farruh Ishmanov, Aamir Saeed Malik, Sung Won Kim, and Bahodir Begalov. Trust management system in wireless sensor networks: design considerations and research challenges. *Transactions on Emerging Telecommunications Technologies*, 26(2):107–130, 2015.

[35] Saeideh Sadat Javadi and MA Razzaque. Security and privacy in wireless body area networks for health care applications. In *Wireless networks and security*, pages 165–187. Springer, 2013.

[36] Minho Jo, Longzhe Han, Nguyen Duy Tan, and Hoh Peter In. A survey: energy exhausting attacks in mac protocols in wbans. *Telecommunication Systems*, 58(2):153–164, 2015.

[37] Farwa Kazmi, Muazzam A Khan, Ayesha Saeed, Nazar Abbas Saqib, and Muhammad Abbas. Evaluation of trust management approaches in wireless sensor networks. In *2018 15th International Bhurban conference on applied sciences and technology (IBCAST)*, pages 870–875. IEEE, 2018.

[38] Haibat Khan, Benjamin Dowling, and Keith M Martin. Highly efficient privacy-preserving key agreement for wireless body area networks. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 1064–1069. IEEE, 2018.

[39] Tayyab Khan, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P Singh, Manisha Manjul, et al. A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *IEEE Access*, 7:58221–58240, 2019.

[40] Nesrine Khernane, Maria Potop-Butucaru, and Claude Chaudet. Banzkp: A secure authentication scheme using zero knowledge proof for wbans. In *2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pages 307–315. IEEE, 2016.

[41] Marko Kompara and Marko Hölbl. Survey on security in intra-body area network communication. *Ad Hoc Networks*, 70:23–43, 2018.

[42] Nabila Labraoui. A reliable trust management scheme in wireless sensor networks. In *2015 12th International Symposium on Programming and Systems (ISPS)*, pages 1–6. IEEE, 2015.

[43] Nabila Labraoui, Mourad Gueroui, and Larbi Sekhri. On-off attacks mitigation against trust systems in wireless sensor networks. In *IFIP International Conference on Computer Science and its Applications*, pages 406–415. Springer, 2015.

[44] Nabila Labraoui, Mourad Gueroui, and Larbi Sekhri. A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications*, 87(3):1037–1055, 2016.

[45] Ming Li, Shucheng Yu, Joshua D Guttman, Wenjing Lou, and Kui Ren. Secure ad hoc trust initialization and key management in wireless body area networks. *ACM Transactions on sensor Networks (TOSN)*, 9(2):18, 2013.

[46] Xiong Li, Maged Hamada Ibrahim, Saru Kumari, Arun Kumar Sangaiah, Vidushi Gupta, and Kim-Kwang Raymond Choo. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks*, 129:429–443, 2017.

[47] Chao Liu, Zhaojun Gu, and Jialiang Wang. A hybrid intrusion detection system based on scalable k-means+ random forest and deep learning. *IEEE Access*, 9:75729–75740, 2021.

[48] Ruixia Liu and Yinglong Wang. A new sybil attack detection for wireless body sensor network. In *2014 Tenth International Conference on Computational Intelligence and Security*, pages 367–370. IEEE, 2014.

[49] Vikash Mainanwal, Mansi Gupta, and Shravan Kumar Upadhayay. A survey on wireless body area network: Security technology and its design methodology issue. In *2015 international conference on innovations in information, embedded and communication systems (ICIIECS)*, pages 1–5. IEEE, 2015.

[50] Mohammad Masdari and Safiyeh Ahmadzadeh. Comprehensive analysis of the authentication methods in wireless body area networks. *Security and Communication Networks*, 9(17):4777–4803, 2016.

[51] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th international conference on Mobile systems, applications, and services*, pages 211–224. ACM, 2011.

[52] Kerry McKay, Lawrence Bassham, Meltem Sönmez Turan, and Nicky Mouha. Report on lightweight cryptography. Technical report, National Institute of Standards and Technology, 2016.

[53] Sudip Misra and Ankur Vaish. Reputation-based role assignment for role-based access control in wireless sensor networks. *Computer Communications*, 34(3):281–294, 2011.

[54] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. Wireless body area networks: A survey. *IEEE Communications surveys & tutorials*, 16(3):1658–1686, 2014.

[55] Aamer Nadeem and M Younus Javed. A performance comparison of data encryption algorithms. In *2005 international conference on information and communication technologies*, pages 84–89. IEEE, 2005.

[56] AKM Iqtidar Newaz, Amit Kumar Sikder, Leonardo Babun, and A Selcuk Uluagac. Heka: A novel intrusion detection system for attacks to personal medical

devices. In *2020 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2020.

[57] Pejman Niksaz and Mashhad Branch. Wireless body area networks: attacks and countermeasures. *International Journal of scientific and engineering research*, 6(19):565–568, 2015.

[58] Adedayo Odesile and Geethapriya Thamilarasu. Distributed intrusion detection using mobile agents in wireless body area networks. In *2017 Seventh International Conference on Emerging Security Technologies (EST)*, pages 144–149. IEEE, 2017.

[59] Office of National Statistics. National population projections: 2016-based statistical bulletin, 2016. Accessed: 14-05-2019.

[60] Anyembe Andrew Omala, Kittur P Kibiwott, and Fagen Li. An efficient remote authentication scheme for wireless body area network. *Journal of medical systems*, 41(2):25, 2017.

[61] B Padmavathi and S Ranjitha Kumari. A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution. *IJSR, India*, 2:2319–7064, 2013.

[62] Pangkaj Chandra Paul, John Loane, Gilbert Regan, and Fergal McCaffery. Analysis of attacks and security requirements for wireless body area networks-a systematic literature review. In *European Conference on Software Process Improvement*, pages 439–452. Springer, 2019.

[63] Monalisha Polai, Sujata Mohanty, and Shreeya Swagatika Sahoo. A lightweight mutual authentication protocol for wireless body area network. In *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 760–765. IEEE, 2019.

[64] Michael A Ribers and Hannes Ullrich. Battling antibiotic resistance: can machine learning improve prescribing? 2019.

[65] Amal Sammoud, Mohamed Aymen Chalouf, Omessaad Hamdi, Nicolas Montavont, and Ammar Bouallegue. A new biometrics-based key establishment protocol in wban: energy efficiency and security robustness analysis. *Computers & Security*, page 101838, 2020.

[66] Vladimir V Shakhov. Protecting wireless sensor networks from energy exhausting attacks. In *International Conference on Computational Science and Its Applications*, pages 184–193. Springer, 2013.

[67] Jian Shen, Shaohua Chang, Jun Shen, Qi Liu, and Xingming Sun. A lightweight multi-layer authentication protocol for wireless body area networks. *Future Generation Computer Systems*, 78:956–963, 2018.

[68] Jian Shen, Ziyuan Gui, Sai Ji, Jun Shen, Haowen Tan, and Yi Tang. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications*, 106:117–123, 2018.

[69] Lu Shi, Ming Li, Shucheng Yu, and Jiawei Yuan. Bana: body area network authentication exploiting channel characteristics. *IEEE Journal on selected Areas in Communications*, 31(9):1803–1816, 2013.

[70] Lu Shi, Jiawei Yuan, Shucheng Yu, and Ming Li. Mask-ban: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. *IEEE Internet of Things Journal*, 2(1):52–62, 2015.

[71] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–18, 2017.

[72] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. Twine: A lightweight, versatile block cipher. In *ECRYPT Workshop on Lightweight Cryptography*, volume 2011, 2011.

[73] Xiao Tan, Jiliang Zhang, Yuanjing Zhang, Zheng Qin, Yong Ding, and Xingwei Wang. A puf-based and cloud-assisted lightweight authentication for multi-hop body area network. *Tsinghua Science and Technology*, 26(1):36–47, 2020.

[74] Geethapriya Thamilarasu. idetect: an intelligent intrusion detection system for wireless body area networks. *International Journal of Security and Networks*, 11(1-2):82–93, 2016.

[75] Geethapriya Thamilarasu and Zhiyuan Ma. Autonomous mobile agent based intrusion detection framework in wireless body area networks. In *2015 IEEE 16th international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pages 1–3. IEEE, 2015.

[76] Mohsen Toorani. Security analysis of the ieee 802.15. 6 standard. *International Journal of Communication Systems*, 29(17):2471–2489, 2016.

[77] Sezer Toprak, Akhan Akbulut, Muhammet Ali Aydɹn, and Abdŭl Haim Zaim. Lwe: An energy-efficient lightweight encryption algorithm for medical sensors and iot devices. *Electrica*, 20(1):71–81, 2020.

[78] United Nations, Depatment of Economic and Social Affairs. World population ageing 2019, 2019. Accessed: 07-11-2021.

[79] Muhammad Usman, Muhammad Rizwan Asghar, Imran Shafique Ansari, and Marwa Qaraqe. Security in wireless body area networks: From in-body to off-body communications. *IEEE Access*, 6:58064–58074, 2018.

[80] Satish Vadlamani, Burak Eksioglu, Hugh Medal, and Apurba Nandi. Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*, 172:76–94, 2016.

[81] Haodong Wang and Qun Li. Efficient implementation of public key cryptosystems on mote sensors (short paper). In *International Conference on Information and Communications Security*, pages 519–528. Springer, 2006.

[82] Weichao Wang, Xinghua Shi, and Tuanfa Qin. Encryption-free authentication and integrity protection in body area networks through physical unclonable functions. *Smart Health*, 2018.

[83] World Health Organization. Global status report, 2010. Accessed: 14-05-2019.

[84] Hu Xiong and Zhiguang Qin. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. *IEEE transactions on information forensics and security*, 10(7):1442–1455, 2015.

[85] Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D Aagaard, and Guang Gong. The simeck family of lightweight block ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 307–329. Springer, 2015.

[86] Jen-Ho Yang and Chin-Chen Chang. An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. *Computers & security*, 28(3-4):138–143, 2009.

[87] Guoxing Zhan, Weisong Shi, and Julia Deng. Design and implementation of tarf: A trust-aware routing framework for wsns. *IEEE Transactions on dependable and secure computing*, 9(2):184–197, 2012.

[88] Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, and Ingrid Verbauwhede. Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, 58(12):1–15, 2015.

[89] Jin Zhao, Jifeng Huang, and Naixue Xiong. An effective exponential-based trust and reputation evaluation system in wireless sensor networks. *IEEE Access*, 7:33859–33869, 2019.