A Survey on Wireless Body Area Networks: Architecture, Security Challenges and Research Opportunities

Muhammad Shadi Hajar*, M. Omar Al-Kadri and Harsha Kumara Kalutarage

School of Computing, Robert Gordon University, Garthdee House, Garthdee Road, Aberdeen, AB10 7GJ, Scotland, UK

ARTICLE INFO

Keywords:
Wireless Body Area Networks, IEEE 802.15.6, Security, Privacy, Intrusion Detection, Trust Management, Authentication, Encryption, Integrity, Key Establishment, Survey, Attacks

ABSTRACT

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 allows timely intervention. However, due to the sensitive information within the Wireless Body Area Networks (WBANs), insecure data violates the patients' privacy and may consequently lead to improper medical diagnosis and/or treatment. Achieving a high level of security and privacy in WBAN involves various challenges due to its resource limitations and critical applications. In this paper, a comprehensive survey of the WBAN technology is provided, with a particular focus on the security and privacy concerns along with their countermeasures, followed by proposed research directions and open issues.

1. Introduction

A Wireless Body Area Network (WBAN) is a wireless network that consists of a set of tiny bio-medical nodes distributed on the body surface, underneath the skin, inside the body, or in the vicinity of the body. WBAN, also known as Wireless Body Sensor Network (WBSN), is defined in IEEE 802.15.6 [51], which is a particular type of Wireless Sensor Networks (WSNs). IEEE 802.15.6, which has been released in 2012, is the only standard available for WBAN. IEEE 802.15.6 provides a reliable, short range of communications and a wide range of data rates to fit different types of applications. The extremely low power sensor nodes have the ability to monitor the vital physiological signs of the body, and some nodes are able to inject a medicine dosage directly into the body.

Both the wearable devices and the Implantable Medical Devices (IDMs) are designed to send real-time readings of the body bio-signals to a remote server or a sink node. The monitored signals vary considerably depending on the node type and could be body temperature, blood pressure, respiration measurement, heart rate, blood glucose level, Electrocardiogram (ECG) or Electromyogram (EMG). Monitoring these physiological parameters of the elderly or those with chronic diseases provides more flexibility and freedom to patients and allows quick intervention when necessary. At present, the aging population is increasing dramatically across the globe [94]. For instance, the number of people aged over 85 in the United Kingdom is heading to double by mid-2041 [94]. Additionally, according to World Health Organization (WHO) [136], diabetes will be among the leading causes of death by 2030, where up to 15% of the overall national healthcare budget is dedicated to diabetes care. Consequently, the total expenditure of health systems and the percentage of the overloaded medical staff are expected to increase significantly. This incentivizes taking advantage of the latest advancements of WBAN to enhance the quality of patients' lives, improve monitoring procedures, make timely intervention decisions, and reduce the overall cost of health systems along with the long operational hours of medical staff.

Security and privacy concerns are the major challenges facing the widespread adoption of WBAN. Sensor nodes send very critical and sensitive data. Any compromise would not only violate the patients privacy but may also endanger their lives. For instance, when a false ECG sensor reading is provided to physicians, it may lead to incorrect interventions that could be harmful to patients. Similarly, when an automated insulin pump receives a wrong or compromised command, it may inject an insulin overdose into the patients' bloodstream. WBAN is prone to various types of attacks ranging from internal to external and passive to active attacks. On the other hand, security countermeasures vary from traditional security solutions like authentication and encryption to Intrusion Detection Systems (IDSs) and Trust Management Systems (TMSs) in order to address potential security vulnerabilities.

Several survey papers on WBAN are available in the literature. However, since the first WBAN draft was published in 2010, survey papers on or before 2010 are not considered in this survey. WBAN architecture has been widely discussed in [5, 25, 71, 85, 130, 132]. Also, the three tiers of communication (explained in section 2.3) are discussed in many papers [5, 25, 85, 132]. However, authors in [132] suggest four tiers of communication in order to include the nano communication between nano nodes and nano-micro nodes in the in-vivo domain. The PHY and MAC layers of the standard have been presented in [4, 20, 25, 71, 85, 131], while the WBAN design issues are discussed in [20]. WBAN applications are presented in [2, 20, 109, 115, 130], whereas routing protocols applicable to WBAN are stated in [2, 71, 109, 130]. In contrast to the aforementioned work, this paper provides a holistic description of the WBAN architecture, topology and tiers of communication, in addition to presenting the security levels defined in the standard. Although survey papers before the first standard draft have not been considered, some

*Corresponding author

m.hajar@rgu.ac.uk (M.S. Hajar); o.alkadri@rgu.ac.uk (M.O. Al-Kadri); h.kalutarage@rgu.ac.uk (H.K. Kalutarage)

ORCID(s): 0000-0002-5455-6931 (M.S. Hajar); 0000-0002-1146-1860 (M.O. Al-Kadri); 0000-0001-6430-9558 (H.K. Kalutarage)

conflicting information still exists in the literature; therefore, to the best of our abilities, all related information presented in this paper are verified to comply with the IEEE 802.15.6 standard. Some WBAN applications have been mentioned throughout this paper, while routing protocols are out of the scope of this paper.

The security of WBAN has been reviewed in several surveys recently. Many of which propose different classification approaches of threats and vulnerabilities of WBAN. The common denominator between them is discussing the security threats and the required countermeasures against these threats. The basic security requirements provided by the Confidentiality, Integrity and Availability (CIA) model are widely discussed in the literature [5, 80, 132], whereas more general security requirements have been discussed in [5], such as data freshness and secure management. Furthermore, WBAN attacks are also discussed in the literature. The authors in [13] present a set of potential attacks categorized based on the protocol stack layers, while passive and active attacks are discussed in [65] in addition to a list of 18 different types of attacks. Additionally, traditional countermeasures such as authentication are briefly reviewed in [5, 80, 132], while further authentication schemes have been discussed in [23]. In [65], a detailed survey of key agreement schemes is provided; moreover, authors present an overview of security evaluation methods in addition to a performance analysis discussion based on power consumption, memory and computational cost. The authors in [132] discuss the security challenges on different tiers of communication, including the nanodomain, in addition to listing generic challenges of WBAN. In contrast to the aforementioned work, this survey paper investigates the major security threats and vulnerabilities and categorizes them into three different groups based on the CIA security requirements they violate. Unlike other survey papers, in addition to the traditional security countermeasures, countermeasures at different security levels of defense have also been considered. Additionally, more specific requirements have been discussed for different security countermeasures.

The main contributions of this survey can be summarized as follows:

- Provide a brief background of WBAN technology and architecture that complies with the IEEE 802.15.6 standard. This concise introduction offers the readers an entry-level to the research area.
- Investigate the major WBAN threats and vulnerabilities at different levels of defense.
- Discuss the security requirements and challenges of WBAN, especially at tier-1 and tier-2 of communication. Furthermore, additional requirements have been specified when needed for different security solutions.
- Present the potential countermeasures to protect the security and privacy of WBAN at different levels of defense.
- Authentication and key establishment schemes have been discussed comprehensively. Moreover, a suggested classification has been proposed.
- IDSs and TMSs have been discussed along with their related attacks.
- Further research opportunities, directions and open issues have been proposed.

The remainder of this paper is organized into seven sections that proceed as follows. An overview of the WBAN technology is presented in section 2. This is followed by general security requirements and approaches in section 3. In section 4, the vulnerabilities and threats of WBAN are comprehensively explored, while section 5 presents different types of security countermeasures and approaches. Future research opportunities and directions of WBAN are stated in section 6. Finally, the paper is concluded in section 7.

2. Wireless Body Area Networks

The importance of WBAN and its critical role in the healthcare systems motivate the standardization process to enable the interoperability of different products from different vendors. IEEE 802.15.6 defines the Physical (PHY) and the Medium Access Control (MAC) layers of WBAN [51]. The extremely rigorous requirements of WBAN transceivers, such as power efficiency, force IEEE Task Group 6 (TG6) to adopt three types of physical layers in order to satisfy different types of applications [144]. These physical layers could be summarized as follows [66]:

- Narrowband (NB) PHY: supports seven frequency bands with different data rates [51].
- Ultra-wideband (UWB) PHY: supports two different frequency bands, low and high, with a different number of channels, while having the same bandwidth. The design of UWB PHY provides durable implementation with lower complexity and power consumption.
- Human body communication (HBC) PHY: supports one low-frequency band centered at 21 MHz, where the data transmission is conducted through the patient's body using Electric Field Communication (EFC) technology.

2.1. WBAN Design Characteristics

The overall design characteristics of IEEE 802.15.6 standard are as follows [51, 118, 142]:

- Recoverable in case of any link or node failure.
- The ability to support a vast range of data rates starting from tens of Kbps and up to around 10 Mbps in order to meet all potential applications.
- Provides efficient power consumption mechanisms that allow power source to last for several years.

- Provides reliable communication with acceptable jitter and latency values for both medical and non-medical applications.
- Supports the coexistence of both in-body and on-body sensor nodes.
- Able to support authentication, encryption and integrity security mechanisms.
- Able to address node adding and removing within a relatively short time.
- Supports operation in a heterogeneous wireless environment.
- Complies with Specific Absorption Rate (SAR) regulations.
- Supports scalability up to 64 nodes.

In the literature, there is some conflicting information regarding the characteristics of WBAN. For instance, some papers suggest that WBAN is scalable up to 256 nodes [118, 142], whereas the IEEE 802.15.6 standard defines it as a maximum of 64 nodes. Therefore, the information of the IEEE 802.15.6 standard is adopted throughout the paper to avoid such conflicts.

2.2. WBAN Topology

The IEEE 802.15.6 defines the Body Area Network (BAN) as a logical set consisting of sensor nodes and a single hub. It adopts the star topology with two different types of communications, simple one-hop and extended two-hop star topology. In simple one-hop star topology, nodes exchange frames directly with the hub of BAN, whereas in the extended two-hop topology, a relay node is introduced and nodes are able to communicate directly with the hub or via a relay node as illustrated in Fig. 1. The total number of nodes within a single BAN is specified by the MAC sublayer parameter mMaxBANSize, which has been set to 64. Nodes in BAN could be classified based on their role into:

- *Hub*: The hub node, the sink node or the coordinator are different names for the same node type. The hub acts as a gateway to another BAN or external networks. It controls the BAN and all the external communications go through it. It has better resources compared to normal nodes inside the BAN.
- *Relay node*: Some nodes have the relay capability to relay messages from end nodes to the hub. They are located in the hub's direct communication range. Relaying is required in the extended star topology of WBAN.
- *End node*: Other nodes in WBAN are considered as end nodes. They are designed to perform specific tasks and exchange messages with the hub directly if they are in the direct communication range or via relay nodes if they are out of the direct communication range.

In addition to the aforementioned classification of nodes in WBAN, different types of classifications are available in the literature, such as node deploying location (in-body or on-body, etc.) and node functionality (sensor nodes or actuator nodes, etc.) [10].

2.3. WBAN Communication Architecture

Considering the whole WBAN ecosystem, data communication could be divided into different tiers of communication. The authors in [132] divided it into four levels of communication in order to consider the communication between nano-nodes and micro-nodes. However, generally, three tiers of communication are recognized in the standard of WBAN [71, 80, 85] as follows:

- *Tier-1 Intra-BAN communication*: The data communication in the first tier includes the communication between sensor nodes themselves and between sensor nodes and the hub. Both sender and receiver are located in the body range in this tier of communication. This includes in-body, on-body and off-body sensor nodes. The data rate depends on the characteristics of the sensor nodes as well as the physical layer and the used frequency.
- *Tier-2 Inter-BAN communication*: Tier-2 communication includes the communication between two different BANs and the communication between the hub and the Access Points (APs).
- *Tier-3 Beyond BAN communication*: Tier-3 communication represents all the communications that take place beyond the BAN. Tier-3 includes communication between the APs and the medical servers via the internet. All the protocols in this tier of communication are well defined in the TCP/IP stack.

Fig. 2 depicts all WBAN communication tiers. In the figure, two BANs are shown in tier-1 of communication, where the on-body nodes and the implanted nodes are distributed across the body. All nodes are connected to the hub via direct communication or via a relay node.

3. Security in WBAN

Security and privacy issues are critical concerns in all types of networks. However, WBAN, which processes critical data that, if compromised, may affect patients' health or endanger their lives, requires more efficient security mechanisms to protect patients from all types of malicious activities. Although security in WBAN is very crucial and has a high priority, there are still many open areas to research due to the strict resource restrictions of WBAN, in addition to a wide range of security and privacy vulnerabilities inherited from Wireless Sensor Networks (WSNs).

In order to ensure a high level of security and privacy in WBAN, security at each tier of communication must be guaranteed. The basic security requirements of WBAN are outlined as follows:

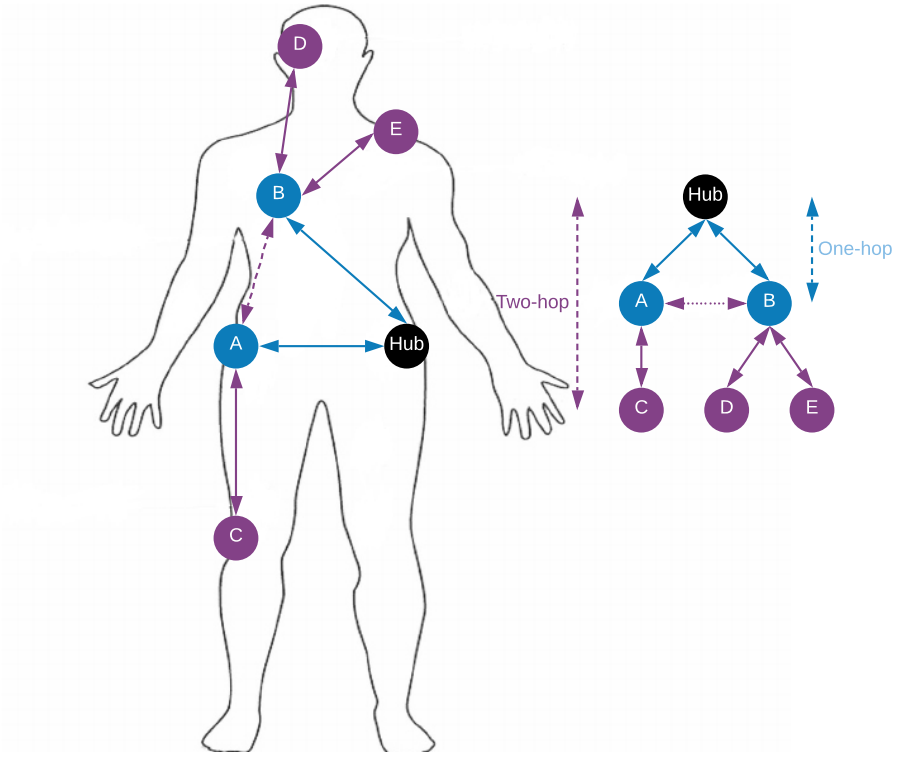

Figure 1: WBAN Topology

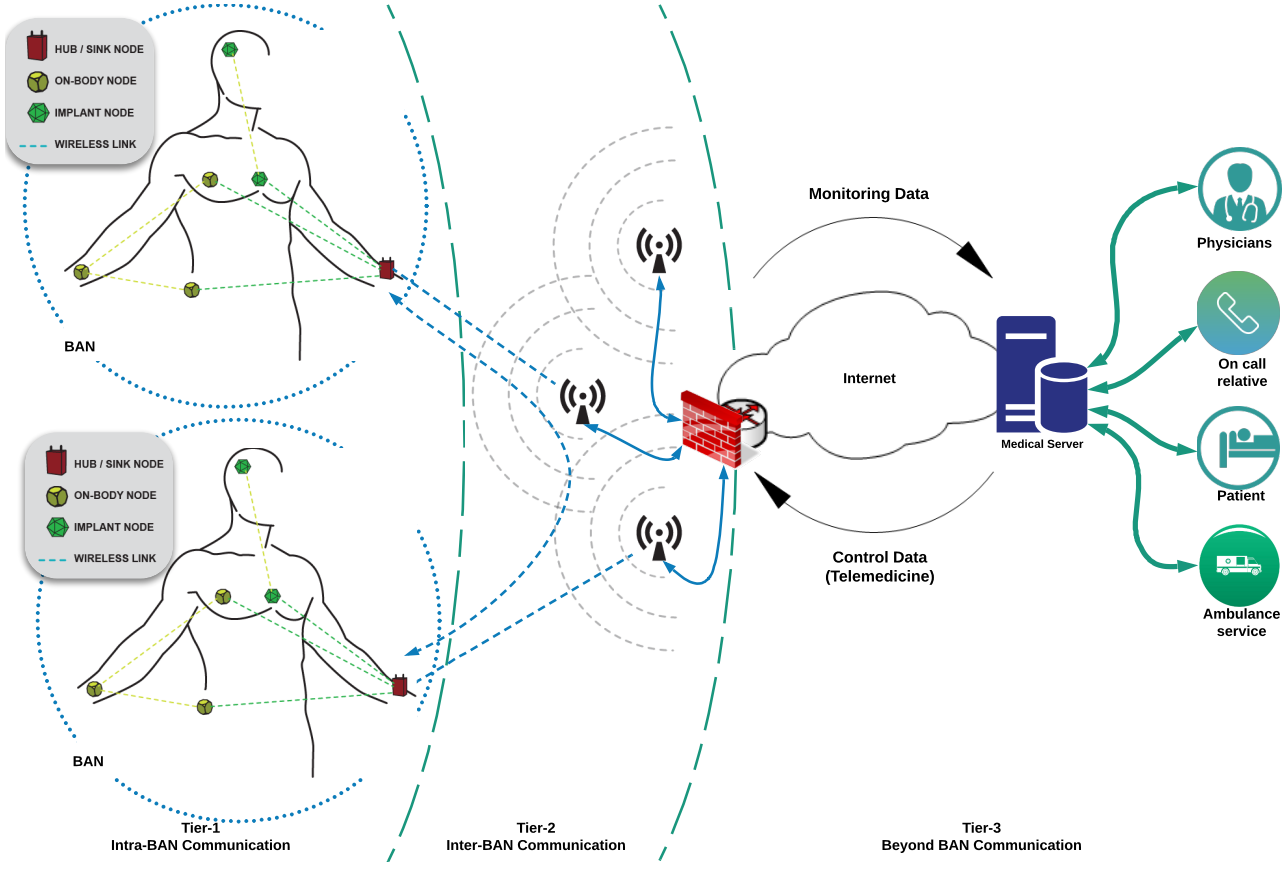

Figure 2: WBAN Architecture

- *Confidentiality*: Data must be protected from being disclosed to any unauthorized parties during data transmission as well as during the storage phase [13]. Data in WBAN contains very sensitive information about the health of the patient. It could be disclosed during transmission in an open channel by eavesdropping or could be disclosed when it is stored in a plain format when the node gets compromised. Therefore, hiding data using proper encryption is a must.
- *Integrity*: When data is received, the receiver party has to ensure that the received information is original and have not been altered during the transmission phase [99]. Confidentiality measures cannot protect data from modification, which can be easily done by intercepting data in the transmission phase to inject, delete, or modify the sent message.
- *Availability*: Adversary can breach the availability and prevent authorized entities from accessing the required data [5]. Considering the critical applications of WBAN, disrupting the communication between the caregivers and the sensor nodes may threaten the patient's life. Therefore, maintaining the ability to access the required data under any circumstances is a crucial requirement for this application type.
- *Data Authentication*: While data integrity aims to save data from being modified during the transmission, data authentication aims to ensure that the received message came from the origin node, which is believed to be [22]. IEEE 802.15.6 defines the Message Authentication Code (MAC) to verify that the received message is sent by the original sender.
- *Data Freshness*: Adversary may intend to capture the transmitted messages and replay them afterward in which it causes confusion and instability in WBAN [65]. Therefore, a mechanism to ensure that the received message is recent and no adversary replay old messages is a must. Ensuring that the received messages are in order and on time is referred to as strong freshness, whereas there is no latency guarantee in weak freshness.
- *Secure Management*: Many security mechanisms such as encryption, decryption, and data authentication requires keys, which must be distributed in a secure manner [63].

Security at tier-3 of communication has been widely investigated in the literature since it is a common tier between different networks, whereas many research opportunities are still open at tier-1 and tier-2 of communication. Therefore, this survey will mainly consider the security and privacy concerns on the first two tiers of communication for their uniqueness to WBAN.

IEEE 802.15.6 defines three levels of security, where the hub and the sensor nodes can choose from. Each one of these security levels has different security characteristics as follows:

- *Level-0 Unsecured Communication*: No security measures are used at this level of security. Messages are exchanged in unsecured frames without confidentiality, authentication, integrity validation or replay defense.
- *Level-1 Authentication*: Messages, at this security level, are exchanged in secured authenticated frames that ensure message authenticity, replay defense and integrity validation. However, no measures are applied to provide confidentiality and privacy protection.
- *Level-2 Authentication and Encryption*: The highest level of security proposed in the standard. Messages are exchanged in secured authenticated and encrypted frames. Therefore, confidentiality, message authenticity, integrity, and replay defense are all provided at this security level.

Nodes and hub are to choose the suitable security level during the association process based on their security requirements. Fig. 3 shows the security structure to generate security keys and provide security services. A preshared Master Key (MK) has to be activated or established between the hub and every node during the association process to achieve secured unicast communication, then a Pairwise Temporal Key (PTK) is created and shared between the two parties to be used per communication session. On the other hand, for secured multicast communication, a Group Temporal Key (GTK) is generated in the hub and subsequently shared with corresponding multicast group members by the hub.

Although the IEEE 802.15.6 standard provides three security levels, recent research shows that the security mechanisms introduced in the standard are still vulnerable to different types of attacks. The author in [127, 128] analyses the key agreement protocols of the WBAN standard for MK establishment. He states that four protocols for key establishment defined in the standard are vulnerable to Key Compromise Impersonation (KCI) attacks and do not meet the forward secrecy requirement. Additionally, one of the protocols is vulnerable to offline dictionary attacks.

4. WBAN Threats

Considering WBAN as a special type of WSN, it inherits all security threats from WSN. Moreover, the special type of applications that WBAN provides and the stringent resource constraints increase the threats and security concerns to WBAN deployment. The security concerns in WBAN could be divided into attacks and misbehavior activities. While attacks involve any malicious activities that intend to damage the network or affect its operation, misbehavior threats occur when an internal node acts in an improper way that affects the operation or the network's performance. Fig. 4 shows the WBAN threats taxonomy discussed throughout this survey.

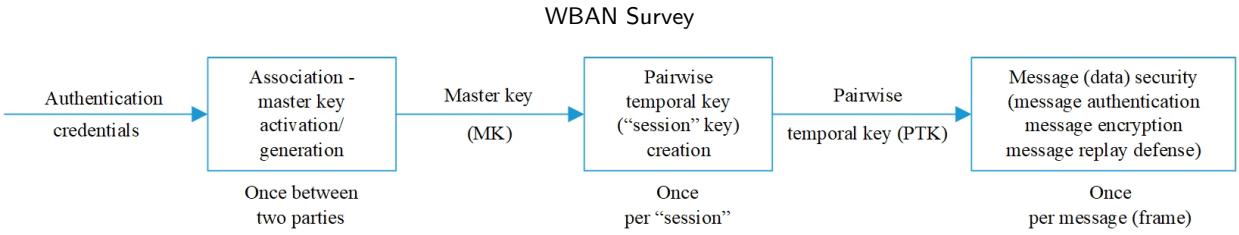

Figure 3: Security Structure

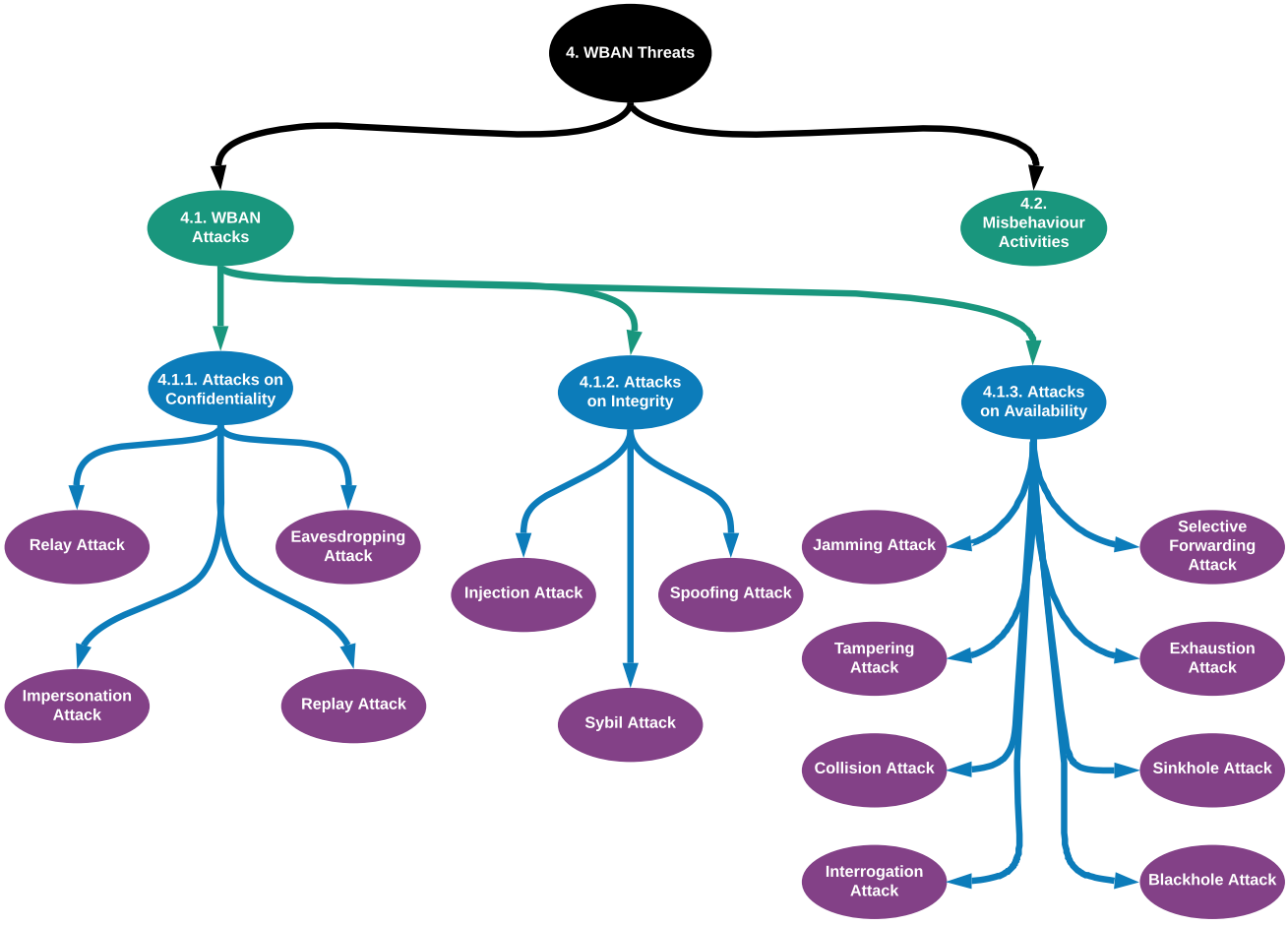

Figure 4: WBAN Threats Taxonomy

4.1. WBAN Attacks

WBAN is susceptible to different types of attacks, which could be classified based on the origin of the attack into internal and external attacks as follows [1],

- *Internal attacks:* This kind of attack is sourced from inside the WBAN by a malicious or compromised node. The main challenge in this type of attack is that the traditional security measures, which are considered the first line of defense, are not able to protect the network from this type of attack.
- *External attacks:* This kind of attack is launched by outsiders, which may involve external nodes or any other types of adversaries.

Another method proposes classifying attacks based on the nature of the attack into passive or active attacks as follows [1],

- *Passive attacks:* The main aim of passive attacks is to gather data rather than threaten the network, such as eavesdropping attacks. This type of attack violates the confidentiality and privacy requirements. Furthermore, adversaries could take advantage of the gathered information to launch active attacks later.
- *Active attacks*: This kind of attack contains a various range of malicious activities such as data alteration and route poisoning. DoS attacks, for instance, target the operation of the network in order to degrade the performance of the network and deplete the resources as well.

To provide a logical sequence across this survey, we classify the attacks based on the CIA security requirements model. Note that the below list of attacks is not exhaustive. It covers the widely-known types of attacks related to WBAN.

4.1.1. Attacks on Confidentiality

The attacks on confidentiality are listed as follows:

- *Eavesdropping Attack:* An eavesdropping attack is a monitoring attack where the adversary snoops on the medium to capture the transmitted frames in order to extract sensitive information in the absence of a victim's awareness [3]. In the security level 0 (unsecured communication) and security level 1 (authentication but not encryption) where no confidentiality or privacy protection is available [51], the adversary can easily gather sensitive and private information. On the other hand, in the security level 2, where authentication and encryption are provided, the adversary still has the chance to eavesdrop and get the secret keys during the key exchange phase.

- *Replay Attack:* Attackers may capture and store messages and then replay them into the BAN [81]. This may lead to confusion and in some circumstances, lead to a significant problem when an action is taken based on these replayed messages because the late received messages are still valid ones. IEEE 802.15.6 provides a replay defense mechanism to detect replay attacks in both security levels 1 and 2, where the first octet of the MAC frame body, which is the "Low-Order Security Sequence Number", is used for data freshness and replay detection [51].

- *Relay Attack:* It is a sort of the Man-in-the-middle attack where the malicious node intercepts the communication between two nodes [65]. The two victimized nodes believe that they are in direct communication with each other; however, the malicious node can intercept all exchanged frames.

- *Impersonation Attack:* The attacker can take advantage of the eavesdropped messages to impersonate a legitimate node in order to receive more private information, which causes more harmful effects [110].

4.1.2. Attacks on Integrity

All integrity attacks are active attacks where the adversary injects or manipulates the transmitted messages over the network.

- *Spoofing Attack:* There are different types of spoofing attacks where adversaries in all of them aim to alter or modify messages to have legitimate access or even to interrupt the operation of the network [81]. The communication in security levels 1 and 2 of IEEE 802.15.6 transfers authenticated messages between nodes by setting the MIC field of the Media Access Control (MAC) frame body to the Message Authentication Code (MAC) in order to ensure the integrity and authenticity of the received messages [51].

- *Modification/Injection Attack:* It is a sort of Man-In-The-Middle (MITM) attack where the adversary not just relays messages between the victims, but also injects new messages or modifies the exchanged ones [3]. What makes it worse is that the exchanged messages may convey critical or urgent biometric signals. For example, the message may reflect an emergency case or contain a command from the healthcare center to the respective node to increase the insulin dosage that has to be injected into the patient's body and in both cases, this attack may affect the patient's life.

- *Sybil Attack:* In the Sybil attack, the adversary impersonates fake identities illegitimately. He can use the fake identity to attack the network until got detected and then generates a new identity and continues his malicious activities [78].

4.1.3. Attacks on Service Availability

The main attack against service availability is the Denial of Service (DoS) attacks. DoS attacks can be performed at any stack layer. Below are the most common DoS attacks:

- *Jamming Attack:* Since it is explored in the literature in 1982 [133] to this date, transmitting data wirelessly is always liable to jamming attack. The attacker intentionally interferes with the frequencies used by other nodes in the networks, and as a consequence, the Signal-to-Interference-plus-Noise ratio (SINR) decreases significantly. As the jamming attack is very detrimental, WBAN has to address this serious threat in order to save computational and energy resources.

- *Tampering Attack:* A tampering attack is a physical attack where the adversary is able to access the node physically and cause damage to the hardware components of the node or acquire critical information like cryptographic keys [81]. Although nodes in WBAN are either implanted underneath the skin or in direct touch with the human body, the patient still has to have adequate awareness about who is authorized to handle the nodes physically in order to defeat this type of attack.

- *Collision Attack:* The collision occurs when two or more nodes transmit at the same time [56]. This overlapped transmission degrades network performance and depletes the nodes' energy. Adversary intentionally overlaps other nodes' transmission to create a collision. This signal interference leads to receiving a collided frame, and consequently, Cyclic Redundancy Check (CRC) fails to verify the received frame. Hence it will be discarded. By continuing the adversary to collide with the transmitted frames, the performance degrades dramatically. For example, colliding with acknowledgment frames like I-Ack or B-Ack may double

the Contention Window (CW) up to reach CWmax[UP] [51].

- *Interrogation Attack:* In this kind of attack, the adversary or the compromised node takes advantage of the RTS/CTS (Request To Send/ Clear To Send) mechanism, which is usually used with the CSMA/CA protocol to overcome the hidden terminal problem [106]. The attacker frequently sends an RTS message in order to obtain a CTS response from the targeted nodes, and consequently, all nodes abstain from using the network [30, 97, 104]. To the best of our knowledge, RTS/CTS mechanism is not used in IEEE 802.15.4 nor IEEE 802.15.6 [51, 52]; however, authors in [11, 90] evaluate RTS/CTS mechanism in conjunction with the CSMA/CA protocol for both IEEE 802.15.4 and IEEE 802.15.6, respectively. The simulation results show a tangible enhancement in the overall performance. Therefore, the interrogation attack still has to be considered.
- *Selective Forwarding Attack:* Selective forwarding attack is a well-known attack in WSN where a compromised node drops some packets or selectively forwards some of them [55]. For instance, forwarding packets to a specific destination and dropping others. According to the WBAN architecture, the intra-BAN communication can be an extended two-hop star topology where the sink node is not necessarily in a direct communication range with all nodes in BAN [51]; hence relay nodes' cooperation is mandatory to ensure WBAN operation [100].
- *Exhaustion Attack:* It is a kind of attack in which the adversary attempts to deplete the victim's resources, such as the denial of sleep attack where the adversary depletes the battery of the victim [107].
- *Sinkhole Attack:* The malicious or the compromised node attempts to attract all the traffic inside the WBAN and then drop it [41]. The adversary can run this kind of attack by sending fake routing updates showing itself as the shortest path to the medical server.
- *Blackhole Attack:* This kind of internal attack is a special type of selective forwarding attack. However, in the blackhole attack, malicious relay nodes drop all incoming frames instead of forwarding them [92].

4.2. Misbehaviour Activities

The second type of WBAN threat is the misbehaving activities, which are an unexpected behavior of an internal node. It is usually a selfish activity to gain extra resources unfairly or to save power. For instance, a relay node could refuse to forward frames in order to save energy. Misbehaving is very harmful because traditional security mechanisms usually fail to detect or prevent this type of internal threats. TMSs, which is discussed later in section 5.3, is an effective measure to assess nodes' behavior with an aim to identify untrustworthy and misbehaved nodes.

5. WBAN Threats Countermeasures

Security and privacy in WBAN are essential due to the detrimental effects of its vulnerabilities. However, achieving a high level of security and privacy is a challenging task. This is because of the specific nature of WBAN, notably, the resource limitations and the vital applications it provides. In order to ensure an end-to-end high level of security, three different types of security countermeasures need to be considered. It is worth mentioning that due to the scarcity of WBAN-specific schemes in the literature, some security schemes presented in this section are generally proposed for WSN, which has a high potential of deployment on WBAN; however, these potentials are worthy of further investigations before direct adoption. Fig. 5 shows a high-level perspective of the security countermeasures discussed throughout this survey, associated with the corresponding sections where they are presented.

5.1. Secure Communication

More attention needs to be paid to security and privacy in military and medical applications due to the dangerous consequences of their vulnerabilities. This section states the security requirements related to WBAN communications in section 5.1.1. This is followed by a review of the security countermeasures, which are authentication and key establishment in section 5.1.2, integrity validation in section 5.1.3, and encryption in section 5.1.4.

5.1.1. Security Requirements

In order to defend against well-known attacks and achieve a high level of security, the following security requirements have to be met in any proposed scheme:

- *Lightweight:* Any proposed security solution must be computationally lightweight to fulfill the constraints of resource limitations [101].
- *Anonymity:* It ensures that no outsider will be able to know the identity of the two parties during the authentication process, which enhances the privacy [111].
- *Mutual authentication:* It means that the involved parties are able to authenticate each other; therefore, the authentication process is secured from any impersonate attack [139].
- *Unlinkability:* It ensures that the hidden identity of the nodes still be maintained even if the adversary could capture two transmitted messages belong to the same node because it is impossible to link or associate the captured messages to find out the identity of the sender [74].
- *Session key establishment:* After a successful authentication process between two nodes, a secure session key should be generated and exchanged securely in order to secure the subsequent communications [139].

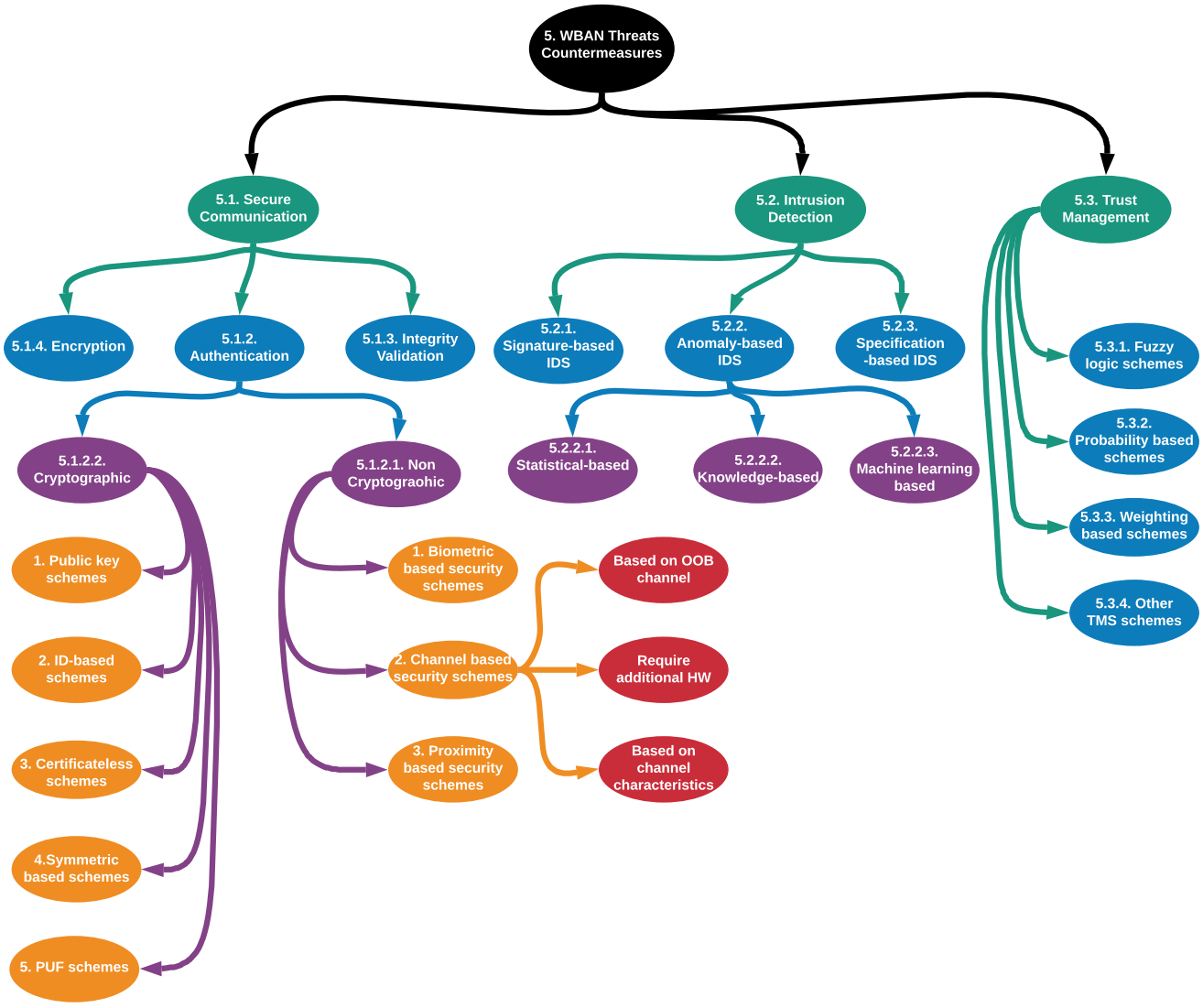

Figure 5: WBAN Survey Taxonomy

- *Forward secrecy:* It ensures that the session key is still secured even if one or the two communicating parties are compromised; moreover, even when the adversary has one or both the private keys [46].
- *Revocability:* It is the ability to revoke any misbehaved node effectively [139].
- *Non-repudiation:* It is imperative that the transmitted messages in WBAN are not repudiated; therefore, the sender cannot deny his sent messages [111].
- *Resilience to well-known attacks:* Any proposed security solution must be immune to the well-know attacks. For instance, resilience to replay attack, resilience to impersonation attack, resilience to verifying attack, resilience to modification attack and resilience to man-in-the-middle attack [22].
- *Key escrow resilience:* Generating keys by Private Key Generator (PKG) raise a key escrow problem in both Public Key Infrastructure (PKI) and ID-based infrastructure as well [75].

5.1.2. Authentication and Key Establishment

Authentication and the key establishment form one of the essential foundations of securing the communication of WBAN. Many research has been proposed in the literature to address this issue. However, many of the proposed schemes fail to meet the aforementioned security requirements or are vulnerable to certain attacks [95], [138]. Therefore, authentication and the key establishment is still an open area for research in WBAN [74]. Authentication gives the receiver the ability to verify the origin of the received messages in order to identify any malicious sender claiming legitimacy. These authentication and key establishment schemes could be classified as follows:

5.1.2.1. Non-cryptographic security schemes All non-cryptographic security schemes are based on assumptions

related to the physical characteristics of the network. It is worth mentioning that this type of security scheme is classified as non-cryptographic due to the used technique to achieve authentication; however, this does not mean that they are unable to generate keys. For instance, some biometric security schemes are able to generate keys, which could be used later to encrypt the exchanged messages. Non-cryptographic security schemes could be classified as follows:

1. *Biometric based security schemes:* Many research in the literature uses unique data from the body domain to achieve lightweight authentication. This trend of research emerges because of the thought that it is difficult to forge the physiological body signs. The authors in [150] propose a novel approach for key generation between neighbour nodes based on electrocardiogram (ECG) signals. Although the proposed ECG-based key generation is able to secure intra-BAN communication without key establishment costs, it has some drawbacks. For instance, it is applicable just in case that all the nodes are located on the surface of the human body, while in WBAN, nodes could be implanted underneath the skin or in the vicinity of the body. Therefore, biometric-based security schemes could be considered as scope specific schemes. Moreover, most of the physiologically based security schemes proposed in the literature do not meet the aforementioned requirements. Neither ESKAS [103] nor OPFKA [48] meets the unlinkability and mutual authentication requirements. Furthermore, not all the nodes have the ability or the hardware to collect the required authentication data. The authors in [105] proposed a symmetric security scheme to generate and distribute the cryptographic keys using the ECG signal for WBAN. WBAN nodes should be able to sense the ECG signal using a time synchronization method in order to generate the security key. Informal and formal security analysis are used to prove the robustness of the proposed method.
2. *Channel based security schemes:* It is another security scheme trend, which takes advantage of the physical characteristics to authenticate nodes, and in some cases, to extract keys. It is built on the assumption that channel characteristics between two nodes are the same. Channel-based security schemes could be categorized into three types based on the use of physical characteristics:
    - Security schemes based on an out-of-band (OOB) communication channel: Some research proposes using a new auxiliary channel to facilitate node authentication by assuming the resilience of the new out-of-band channel to eavesdropping attack. The proposed OOB channel varies from audio to ultrasound channels. For instance, authors in [73] introduce a way of authentication by using visual OOB and with the patient's help. By comparing the blinking LED patterns, the user is able to accept or deny the authentication process. Although the proposed security scheme in [73] meets mutual authentication, forward secrecy and revocation requirements, it is still regarded as a scope specific scheme as some nodes could be implanted inside the body of the patient. Moreover, the modular exponentiation operations used in the proposed scheme does not fit the tough resource limitations of WBAN.
    - Security schemes that require additional hardware: One of the channel-based schemes that requires using additional hardware, which is not recommended from the WBAN perspective due to the tough resource limitations. For instance, Good Neighbor [17] is a proposed solution for pairing two devices using multiple antennas at the receiver side.
    - Security schemes based on channel characteristics measurements: the authors in [112, 113] propose a lightweight authentication scheme based merely on Received Signal Strength (RSS) measurements. Because of the wireless channel correlation, a condition raises for nodes placements, which must be distributed on the half-wavelength range. BANA [112] solely provides an authentication mechanism for on-body devices, which are on the Line of Sight (LOS) and does not extract any keys, whereas MASK-BAN [113], which considers the channel variations of heterogeneous nodes and their reflection on RSS, provides authentication and keys extraction mechanism as well.

    As most of the proposed security solutions are for on-body nodes, channel-based security schemes are scope specific and may not apply to in-body nodes. Furthermore, many physical parameters could affect RSS, such as the surrounding environment, nodes' positions and mobility.
3. *Proximity-based security schemes:* By exploiting the small-scale fading variations on wireless channels when two wireless devices are close to each other and with the help of a third party RF source, the authors in [82] introduce their proximity based scheme to extract the secret key. However, the central dilemma in such schemes is that the two involved parties must reside inside the half-wavelength in order to have the same small scale fading variation and it is recommended to be 0.1λ or less while the adversary should reside on 0.4λ or more. It is worth mentioning that [82] is a generic security scheme that could be used for sensor networks as well.

5.1.2.2. Cryptographic security schemes Cryptographic security schemes vary depending on the types of keys and could be classified into the following categories.

1. *Public key signature schemes:* Public key cryptography (PKC) is based on generating two non-identical

keys. One key is used for encryption or signature generation, whereas the other is used for decryption or signature verification. There is a clear consensus that conventional PKC is not applicable to be used in wireless healthcare applications because of the restricted resources. The main idea of PKC is completely based on two mathematical problems. The first one is a straightforward mathematical problem to generate the public and private keys, while the second one is the reverse operation to calculate one key knowing the other one, which must be extremely hard. However, the extreme hardness of this mathematical operation still needs to be proved [58]. The first mathematical problem could be either an integer factorization problem like in (Rivest, Shamir and Adelman) RSA or a discrete logarithmic problem like in Elliptic Curve Cryptography (ECC). However, both of them are impractical for WBAN applications because they are voracious in using minimal resources. Thus, some research focuses on improving the performance of the inherited algorithms such as authors in [134] where a hybrid multiplication method is used in order to limit the number of memory access, and this speeds up the process around seven times. On the other hand, the traditional cryptographic algorithm RSA still uses a longer key 1024-bit than ECC 160-bit for the same security level, which is still memory voracious. Therefore, ECC based PKC seems more interesting than RSA. A pre-configurable library based on ECC-PKC for wireless sensor networks has been proposed in [77].

2. *ID-based signature schemes:* it is a public-key cryptography that was first proposed in 1984 [108]. In Identity-based Public Key Cryptography (ID-PKC), the node's public key is built from a combination of identity information like a network address, whereas the private key is generated by a Trusted Third Party (TTP) named Private Key Generator (PKG), hence there is no need for Certificate Authority (CA). Since then, many ID-based signature schemes proposed in the literature [19, 54, 141]. However, all these solutions are designed for client-server infrastructure, so it can not meet all the security requirements of WBAN. Moreover, in addition to their vulnerability to some well-known attacks, all ID-based signature schemes face the same key escrow problem because of the TTP entity. Problems of having one PKG could be summarized into: First, PKG is able to decrypt any transmitted message. Second, because of having all private keys, PKG is able to forge any node's signature.
3. *Certificateless signature schemes:* A new public-key cryptography that lies between PKC where the heavy computational overhead of verifying certificates with CA and ID-PKC schemes, which suffer form key escrow problem. This new concept was first proposed in the literature by authors in [6]. Although Certificateless Public Key Cryptography (CL-PKC) solves the inborn key escrow problem in ID-PKC because of using PKG as a TTP, it still uses a TTP entity. However, this TTP entity, named Key Generator Center (KGC) in CL-PKC, does not hold any nodes' private keys, but a master key instead of it. KGC is just responsible for providing the partial private key (D_A), which is sent to the other entities to produce their own keys [6]. In addition to having a partial private key, KGC also generates and holds a master key. Afterward, many certificateless authentication schemes have been proposed in the literature [59, 110, 117, 139, 146]; however, most of which focus just on a remote authentication, which is the authentication between the coordinator node and the Application Providers (APs). Although some schemes like in [110] propose a multi-layer authentication scheme, it is still considered a certificateless signature scheme just beyond the intra-BAN domain. Moreover, the author in [114] finds out that the proposed scheme in [139] is vulnerable to impersonation attack; therefore, neither mutual authentication nor non-repudiation requirements are satisfied.
4. *Symmetric based schemes:* In this kind of authentication scheme, a pre-shared master key in addition to a unique identifier for each node are used to achieve mutual authentication as well as key establishment between two nodes like in [74]. Although the authors claim that their proposed algorithm fulfills the unlinkability and forward secrecy requirements, it is clear that it is not, as the adversary can easily calculate the value (γ), which is unmaskable in the proposed scheme. The authors in [61] suggest a modification to [74] in order to fulfill the forward secrecy and unlinkability requirements. However, there is still a key escrow problem where the coordinator node saves the master key in addition to all nodes' identities.
5. *Physical Unclonable Function schemes:* Physical Unclonable Function (PUF) is the fingerprint of the node's hardware. This property occurs because of the unavoidable manufacturing difference between nodes. This uniqueness and randomness hardware feature is very attractive to researchers to build and design security solutions based on it. The authors in [120] take advantage of the Integrated Circuits (ICs) variant delay characteristics to introduce PUF to be used for authentication and key generation. In [135] a mutual authentication mechanism between any two WBAN sensor nodes using PUF is introduced; however, the authentication process can not be achieved without the help of the coordinator, which according to the authors' assumption, can not be compromised. The authors in [137] present authentication and key establishment scheme, not only between sensor nodes and the coordinator but also between any two nodes with the assistance of the coordinator. Therefore, sensor nodes are afterward able to communicate directly with each other. This proposed shared secret establishment aims at authenticity verification without considering confidentiality. A simplified authentication solution has also been proposed

in [148], which is resilient to some known attacks, such as impersonation attack, replay attack and tampering attack. However, some of the security requirements like anonymity, mutual authentication and unlinkability are not considered. Another PUF-based scheme is proposed in [123] for multi-hop body area network. It is a hierarchical authentication scheme to allow nodes that are not in the direct communication range of the sink to authenticate themselves in an efficient way. Moreover, a cloud TTP has been used in this scheme to store the Challenge-Response Pairs (CRPs) with a view to reducing the storage overhead.

The surveyed authentication and key establishment schemes are summarized in Table 1, stating the solution approach, the stated requirements it fulfills, and the potential improvements to fulfill additional requirements.

5.1.3. Integrity Validation

Message integrity is the process of verifying that the received message is intact and is exactly as sent. This ensures that the transmitted message from the sender to the receiver is not altered by any type of manipulation such as changing content, adding fragments, removing fragments or content transposition. This also includes any type of transmission errors. A secret key is required to ensure the message authenticity; however, confidentiality by itself is not enough to protect data from being modified by an adversary during the transmission phase. For instance, an external adversary may intercept the message and modify it before re-transmitting it again to the receiver. Although applying a message integrity scheme can be a simple task to implement when coupled with a durable cryptographic scheme [32], applying an efficient message integrity mechanism in WBAN can still be a challenging requirement due to the unique characteristics of WBAN[80].

IEEE 802.15.6 provides a mechanism to verify the message authenticity in both security levels one and two [51]. The WBAN Media Access Control (MAC) frame body is formatted, as illustrated in Fig. 6. The MAC frame body length is variable and can scale up to a maximum value defined in the parameter "pMaxFrameBodyLength", which is set in the standard to 255 octets. IEEE 802.15.6 supports two types of frames, secured frames and unsecured frames. The security level is chosen by the two communication parties during the association process according to their security requirements. The Message Integrity Code (MIC) and "Low-Order Security Sequence Number" fields only exist in the secured frames. The "Low-Order Security Sequence Number" field assists in achieving message freshness by using it in both replay detection and nonce construction [51], while the MIC field is used to achieve message integrity by setting it to the Message Authentication Code (MAC) [51].

The Message Authenticating Code (MAC) process is achieved using the Advanced Encryption Standard (AES-128) as an underlying block cipher algorithm with CCM mode (CCM stands for **C**ounter with **C**ipher Block Chaining **M**essage Authentication Code), which is provided in the standard defined by the National Institute of Standards and Technology (NIST) Special Publication SP-800-38C [34]. In security level 1, where no encryption mechanism is provided, the Message Authentication Code (MAC) is computed directly from the frame being transmitted by the sender and the received frame at the receiver, whereas in the security level 2, the Message Authentication Code (MAC) is computed from the unencrypted version of the frame at the sender and from the decrypted version of the received frame at the receiver. Eq. (1) and Eq. (2) are used to calculate the MIC field as follows,

$$MIC = LMB_n(M) = AES(Ctr_0) \oplus X_m \quad (1)$$

$$X_0 = AES(B0), X_i = AES(B_i \oplus X_{i-1}), i = 1, ..., m \quad (2)$$

where M is the message bit string, $LMB_n(M)$ is to specify the leftmost bits of M, $AES(B0)$ is the forward cipher function output of the AES applied to block B and $\oplus$ is the bitwise XOR. AES uses Pairwise Temporal Key (PTK) in unicast secured communication and Group Temporal Key (GTK) in multicast secured communication. Fig. 7 shows the process of the Message Authentication Code (MAC) calculation and the transmitting order, starting from the first octet on the left to the last one on the right.

5.1.4. Encryption

Monitoring the vital signs of the human body demands exchanging extremely sensitive information. This information is used to diagnose health conditions, and then an action can be taken to provide the required telemedicine, such as injecting an insulin dosage. Therefore, in order to ensure the confidentiality and privacy of patient health information, data must be exchanged and stored in an encrypted form. Many encryption algorithms have been proposed in the literature, such as 1024-bit RSA [98] and 3DES [88]; however, these traditional encryption algorithms are not suitable for sensor nodes with stringent resource limitations. Therefore, a lightweight cryptographic algorithm that is energy and computation efficient and able to provide a robust encryption/decryption mechanism is a must. In this survey, heavy encryption algorithms with long key size, high number of rounds, or large block size have not been considered due to their inapplicability to WBAN.

Due to the importance and potential applications of lightweight cryptography, NIST began in 2015 the process to standardize lightweight cryptographic algorithms that fulfill the requirements of constrained devices such as sensor nodes [83]. In order to fulfill the resource restrictions, the following aspects should be considered when choosing a suitable lightweight cryptographic function [116]:

- Key size: with extremely limited storage, for instance, MICAz has only 4-KB EEPROM storage [26], the key size of the cryptographic algorithms plays a significant role. A cryptographic algorithm, which has a smaller key size and provides the same security level,

Table 1
Authentication and Key Establishment Schemes

Literature	Title	Year	Solution	Stated Fulfilled Requirements	Potential Improvements	Comments
[59]	Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system	2020	Certificateless signature schemes	Mutual authentication, Forward secrecy, Anonymity, Session key establishment, Key escrow resilience, Unlinkability	Security analysis against more attacks	Remote certificateless authentication scheme.
[110]	A lightweight multi-layer authentication protocol for wireless body area networks	2018	Certificateless signature scheme	Lightweight, Non-reputation, Mutual authentication, Session key establishment, Key escrow resilience, Forward secrecy	Anonymity	A Certificateless scheme in the section between the PDA and AP.
[139]	Revocable and Scalable Certificateless Remote Authentication Protocol With Anonymity for Wireless Body Area Networks	2015	Certificateless signature scheme	Non-repudiation, Anonymity, Key escrow resistance, Revocability, Mutual authentication, Forward Secrecy	Non-repudiation, Mutual authentication [114]	Remote certificateless authentication scheme only beyond the intra-BAN. The authors in [114] report that this scheme is vulnerable to type-I adversary; therefore, it does not meet the non-repudiation and mutual authentication requirements.
[74]	Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks	2017	Symmetric based schemes	Anonymity, Mutual authentication, Session key establishment, Lightweight, Unlinkability, Forward secrecy	Unlinkability, Forward secrecy [61]	Although authors state that their scheme meet the unlinkability and forward secrecy requirements, it is not [61]. Security is evaluated using AVISPA and compared to other schemes.
[150]	ECG-cryptography and authentication in body area networks	2012	Biometric based security scheme	Lightweight, Session key establishment, Mutual authentication	Anonymity, Unlinkability, Forward secrecy, Non-repudiation, Revocability	A scope specific solution. It requires all nodes to have the same physiological sign sensor.
[103]	An efficient and secure key agreement scheme using physiological signals in body area networks	2012	Biometric based security scheme	Session key establishment, Mutual authentication	Lightweight, Anonymity, Unlinkability, Forward secrecy, Revocability	A scope specific solution. It requires all nodes to have the same physiological sign sensor.
[48]	OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks	2013	Biometric based security scheme	Lightweight, Resistance against brute force attacks, Session key establishment, Mutual authentication	Anonymity, Unlinkability, Forward secrecy, Revocability	A scope specific solution. It requires all nodes to have the same physiological sign sensor.
[73]	Secure Ad-Hoc Trust Initialization and Key Management in Wireless Body Area Networks	2013	Channel based security scheme	Lightweight, Revocation, Mutual authentication, Forward secrecy	Lightweight requirement may need further enhancements	Patient-aided scheme is not an intuitive schemes. Heavy scheme because of the using of modular exponentiation operations, which is not proper for tough resource constraints.
[113]	MASK-BAN: Movement-Aided Authenticated Secret Key Extraction Utilizing Channel Characteristics in Body Area Networks	2015	Channel based security scheme	Lightweight, Session key establishment, Mutual authentication	Anonymity, Key escrow resilience	Limited to the on-body nodes.
[112]	BANA: Body Area Network Authentication Exploiting Channel Characteristics	2013	Channel based security scheme	Lightweight	Session key establishment, Mutual authentication	It just considers the LOS of the on-body nodes without generating keys (An authentication scheme only) [113].
[82]	Proximate: proximity-based secure pairing using ambient wireless signals	2011	Proximity based security scheme	Lightweight, Session key establishment	Further optimizations are required to improve its functionality and test its operability for WBAN	It is a generic security scheme that could be used for sensor networks as authors state. It requires a tough nodes distribution constraint.
[105]	A new biometrics-based key establishment protocol in WBAN: energy efficiency and security robustness analysis	2020	Biometric based security scheme	Lightweight, Session key establishment, Resilience to some known attacks	Forward Secrecy	A scope specific solution. It requires all nodes to have the same physiological sign sensor.
[54]	A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem	2011	ID-based signature schemes	Anonymity, Mutual authentication, Session key establishment, Revocability, Lightweight	Key escrow resilience	Remote authentication scheme, designed for client server infrastructure.
[146]	An efficient and lightweight certificateless authentication protocol for wireless body area networks	2013	Certificateless signature schemes	Anonymity, Mutual authentication, Non-reputation, Lightweight	Insecure scheme [111]	Adversary is able to trace the user information during the session phase [101]. Remote authentication scheme.
[61]	Highly Efficient Privacy-Preserving Key Agreement for Wireless Body Area Networks	2018	Symmetric based schemes	Anonymity, Mutual authentication, Session key establishment, Lightweight, Unlinkability, Forward secrecy	Key escrow resilience	The authors in this research propose a modification to [74] in order to fulfil the unlinkability and forward secrecy requirements.
[135]	Encryption-free Authentication and Integrity Protection in Body Area Networks through Physical Unclonable Functions	2018	Physical Unclonable Function scheme	Mutual authentication, Lightweight, Resilience to impersonate attack, Revocability	Anonymity	It shares secrets between any nodes pair with the help of the coordinator.
[137]	Lightweight mutual authentication among sensors in body area networks through Physical Unclonable Functions	2017	Physical Unclonable Function scheme	Lightweight, Mutual authentication, Session key establishment, Resilience to impersonate attack, Revocability	Anonymity, Unlinkability	The shared secret in the proposed scheme provides just message authenticity without confidentiality.
[148]	Wireless Body Area Network Identity Authentication Protocol Based on Physical Unclonable Function	2018	Physical Unclonable Function scheme	Lightweight, Resilience to some known attacks	Anonymity, Mutual authentication, Unlinkability, Forward Secrecy	A simple authentication scheme based on PUF that does not fulfil some security requirements.
[123]	A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network	2020	Physical Unclonable Function scheme	Lightweight, Mutual authentication	Anonymity, Unlinkability	TTP-based escrow problem.

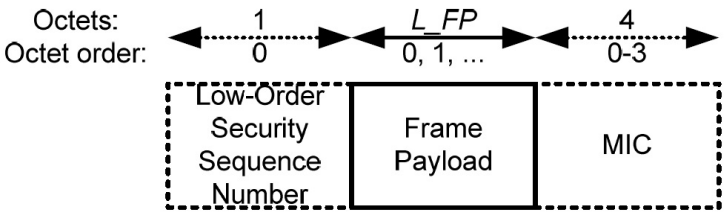

Figure 6: MAC Frame Body Format [51]

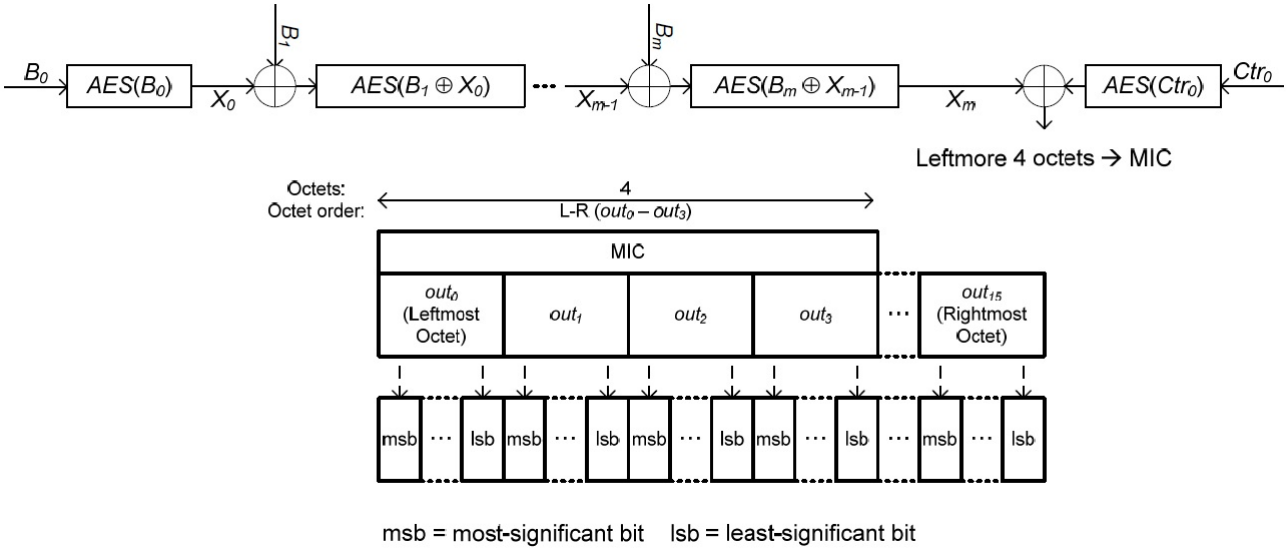

Figure 7: MIC calculation and transmit order [51]

is highly recommended. In [140], authors introduce SIMECK, a block cryptographic algorithm. SIMECK is a hardware-oriented algorithm inspired by the SIMON encryption algorithm's design. With its small key size (64, 96, or 128), it shows a more optimized performance regarding memory and power consumption. mCrypton [76] is a block cipher cryptographic algorithm based on SPN (Substitution Permutation Network) structure. It has three different key sizes, where the smallest one is 64 bits. mCrypton is designed to fit into the low resources environment. Another small key size is TWINE [122], which uses 80 bits key with a Feistel structure.

- Block size: The block size is also another important factor towards a lightweight cryptographic algorithm. Smaller block sizes can decrease the processing time and enhance power consumption. Moreover, medical sensors usually transmit small messages containing vital medical signals; therefore, the smaller block size is more efficient. SPECK [12] is a block cipher based on ARX (Addition-Rotation-XOR) structure. It supports a variety of block sizes ranging between 32 bits and 128 bits. SIMON [12] belongs to the same family as SPECK. However, unlike SPECK, which is designed for software implementation, SIMON is a hardware-oriented algorithm. Another SPN based lightweight cryptographic algorithm is introduced in [147] named RECTANGLE. It uses 64 bits block size with a bit-slice technique in order to achieve rapid execution.

- Number of rounds: Lightweight cryptographic algorithms usually use simple arithmetic, logic and shifting operations to fit into the limited resource restrictions such as ARX structure. Thus, using simple operations leads to increasing the number of rounds. Therefore, the number of rounds is another crucial factor to be considered when adopting a lightweight cryptographic algorithm for WBAN. PRINCE [14] is a block cipher, hardware-oriented cryptographic algorithm that aims to enable encryption in just one clock cycle by using a modest number of rounds (12 rounds), which required a short time to be executed. A 4-round cryptographic algorithm is introduced in [35] called Hummingbird-2. In addition to encrypting, it is able to generate MIC (Message Authentication Code). Another encryption algorithm that uses a low number of rounds is LWE [129]. LWE is a 3-round block cipher algorithm. It has been designed to be light enough in order to meet the resource restrictions of medical sensors and IoT. The key and the block size are 64 bits. The performance of LWE is contrasted with well-known lightweight

Table 2
Lightweight Cryptographic Algorithms

Literature	Algorithm	Year	Block size	Key size	Rounds #	Structure	Possible Attacks
[140]	SIMECK	2015	32/48/64	64/96/128	32/36/44	ARX	Differential attacks [102]
[76]	mCrypton	2005	64	64/96/128	12	SPN	Meet-in-the-Middle Attack [44]
[122]	TWINE	2011	64	80/128	36	GFN	Single-key attack using biclique technique [27]
[12]	SIMON	2013	32/48/64/96/128	64/72/96/128/144/192/256	32/36/42/44/52/54/68/69/72	ARX	23-round linear attack with key guessing technique [24]
[147]	RECTANGLE	2015	64	80/128	25	SPN	Differential attack (18 out of 25 rounds) [147]
[14]	PRINCE	2012	64	128	12	SPN	Key recovery attack (6 rounds version) [119], Sieve-in-the-middle attack (8 rounds) [18]
[35]	Hummingbird-2	2011	16	128	4	SPN	A probabilistic attack (theoretical) [21]
[12]	SPECK	2013	32/48/64/96/128	64/72/96/128/144/192/256	22/23/26/27/28/29/32/33/34	ARX	Sub-cipher attack [31]
[129]	LWE	2020	64	64	3	SPN	No reported attacks yet.

encryption algorithms, such as Rectangle [147] and TWINE [122].
Moreover, in cryptography, when a number of rounds are required to produce the cipher, a round-key is usually used for each round. The algorithm used to produce the round-key from the key is called the key schedule. Consequently, the more complex the key schedule algorithm is, the more memory and computation power it requires. Therefore, a key schedule algorithm could be regarded as another factor to be considered.

The surveyed encryption algorithms are listed in Table 2, stating the block and key sizes, the number of rounds, the algorithm structure and the possible attacks that might compromise the proposed algorithm.

5.2. Intrusion Detection Systems

Securing communication in the intra-BAN and inter-BAN domains is regarded as the first defense line for WBAN security. However, a further security solution that is able to protect WBAN from intruders and monitor the network for suspicious activities can significantly enhance the security of WBAN. IDSs are introduced to form an additional defense layer to protect from malicious activities, inside and outside abuses. Based on the methods of detection, IDS schemes can be grouped as follows:

5.2.1. Signature-based IDSs

By defining a signature for each attack pattern, the IDS can detect malicious activities when an attack pattern matches any defined signature. The main disadvantages of the signature-based IDSs are the need to be updated periodically and the inability to catch unknown attacks. A hybrid, lightweight, multi-level and distributed model that imitates the human immune system with a signature database has been presented in [7]. It takes advantage of the danger model used by our immune system, where a particular type of cell, Dendritic cells, stimulates other cells to form immune responses to any antigens. Copying this alerting mechanism to WSN in addition to the use of predefined features enable the IDS to detect intrusions.

5.2.2. Anomaly-based IDSs

By profiling the normal traffic and operations of the network, anomaly-based IDSs could raise an alert when anomaly behavior is captured. According to [16], the anomaly-based IDSs could be divided into three categories:

5.2.2.1. Statistical-based: It depends on building a statistical reference profile for the network in the optimal conditions without any malicious activities. Afterward, periodic profiles are being generated for the monitored network. The generated profiles are then compared to the reference model to calculate the anomaly probability based on a threshold. A cooperative and a statistical-based IDS has been proposed in [49]. The authors use various types of statistics, such as Forward Percentage (FP) and Local Forward Percentage (LFP), in order to detect anomaly behavior. Owing to using the attack's consequence and technique, the proposed scheme is able to determine the attack type and the attack origin. Although it gives good accuracy in detecting selfish activities, such as DoS attack and sleep deprivation via malicious flooding attack, it shows less accuracy in detecting blackhole and spoofing attacks. However, sharing the responsibility of intrusion detection between nodes with the same resources could be regarded as a good choice to share the computational overhead.

5.2.2.2. Knowledge-based: A previous knowledge for the networks under different circumstances ranging from normal conditions to under attack is used to detect malicious activities. Expert systems and Finite State Machine algorithms are used as a detection engine for a knowledge-based IDS [7, 16].

5.2.2.3. Machine learning based: A more intelligent method to detect any malicious activities in the network, even new ones. Machine learning based IDSs are able to learn from analyzed patterns and update its intrusion detection engine periodically without being explicitly programmed, which gives it the ability to detect not just well-known attacks, but new and unknown attacks as well. Random Forest, Genetic Algorithm (GA), Support Vector Machines (SVMs), Neural Networks and Logistic Regression are all examples of machine learning algorithms used in the literature. iDetect [125] is a distributed IDS that aims to enhance the detection

rate of attacks and choose the most suitable features set that optimize the performance and saves computational power. iDetect IDS is implemented using a multi-objective genetic algorithm to produce the optimal set of features to be used as an input for the intrusion detection engine in order to detect WBAN attacks. The authors in [126] proposed a distributed IDS framework based on mobile agent technology where all nodes inside WBAN participate in the malicious activities detection process by migrating the intrusion detection software form one node to another. The authors state that their framework is able to reduce the communication burden of sending the log in the traditional frameworks, which results in reducing the power consumption. Another hierarchical and distributed IDS based on autonomous mobile agents where the detection software moves from one node to another has been presented by [93]. The proposed IDS framework is evaluated using five different machine learning algorithms (DT, SVM, RF, NBC, KNN). The proposed framework's performance results in around a 6% increase of power consumption; however, results do not show the positive reflection of the proposed framework on the accuracy. The authors in [91] investigated personal medical devices' vulnerabilities by launching different kinds of attacks. Moreover, they proposed HEKA, a passive IDS to monitor and detect malicious activities. The anomaly detection performance of HEKA is evaluated using four machine learning algorithms SVM, KNN, RF and DT, which have been trained using the generated n-grams of the network traffic. The results show an average detection accuracy of around 98% for MITM, Replay, false data injection and DoS attacks. Moreover, the performance of composite attacks of MITM with false data injection and MITM with replay attacks are evaluated and showed an average accuracy of around 95%. Another approach to detect anomaly in the healthcare systems is proposed in [40]. The authors combined two kinds of features, network and biometrics, to enhance the detection performance. The collected dataset is used to train four machine learning algorithms RF, KNN, ANN and SVM. Results show an improvement between 7% and 25%.

5.2.3. Specification-based IDSs

It uses a technique that located in the middle between signature-based IDSs, where predefined rules are used to detect well-known attacks, and anomaly-based IDSs, where normal behavior is defined to detect any abnormal behavior, even unknown ones in contrast to signature-based IDSs [16]. In specification-based IDSs, programmers manually define constraints and features that describe the normal operating behavior in contrast to anomaly-based IDSs, where they are generated automatically. Consequently, the intrusion detection engine can detect suspicious behavior by finding the deviation of the two behaviors.

The IDSs surveyed in this paper are listed in Table 3, stating the used techniques, topology architecture, used simulators, attacks tested for verification and the fulfilled requirements.

5.3. Trust Management Systems

Authentication and key establishment between nodes in WBAN are an imperative task to ensure a high security and privacy level. However, maintaining the successfully established security mechanisms demands a trust relationship between nodes. TMSs assess nodes with an aim to differentiate between trustworthy and untrustworthy nodes. While traditional security mechanisms rely on the nodes' current status, TMSs consider the present behavior of the nodes as well as their behavior history. Thus, deploying TMSs enhances the level of security by continuously monitoring the nodes' behavior and their performance. In light of this, the trust can 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.

Similar to other security aspects of WBAN, deploying a TMS is a challenging task [53], and many factors must be taken into account when proposing a TMS for WBAN. These factors include:

- WBAN architecture.
- Scarcity of resources.
- Communication overhead.
- Resistant to TMSs related attacks.

Taking into account the cooperative manner of nodes within the WBAN, many potential applications emerge for using TMSs ranging from access control and role assignment [84] to trust-based routing protocols [145]. Therefore, TMSs will play a vital role in any interaction and cooperation between nodes inside the WBAN.

The trust estimation engine usually depends on two sources of information in order to produce the trust value:

- Direct trust: Trustor monitors and evaluates the trustee's successful and unsuccessful interactions when both have direct communication and without the help of a third party.
- Indirect trust: When the trustor is not adjacent to the trustee or does not have any historical information to assess the trustee, the trustor depends on the received recommendations from other parties to evaluate the trustee.

TMSs are prone to several internal attacks; therefore, a robust TMS design is sought to defeat this kind of attack. Below is a list of the most common attacks:

- On-off attack: The malicious nodes change their behavior alternately between good and bad manners with a view to remain undetected, and consequently, cause serious damage and degrade the overall performance significantly [68].
- Bad-mouthing attack: One of the dishonest recommendations attacks. This type of internal attack occurs

Table 3
Intrusion Detection Systems Schemes

IDS	Title	Year	Solution	Technique	Architecture	Simulator	Attacks Tested	Fulfillment	Comments
[7]	A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory	2018	Hybrid of anomaly and signature-based IDS	Immune theory technique called Danger Theory	Distributed	Cooja [33]	Blackhole attack, Selective forwarding attack, DDoS attack, Wormhole attack	A lightweight IDS approach that considers power consumption.	This approach is originally proposed for WSN and needs modifications to fit other technologies.
[91]	Heka: A novel intrusion detection system for attacks to personal medical devices	2020	Anomaly-based IDS	Four machine learning algorithms (SVM, KNN, DT, RF)	Distributed	N/A	MITM, replay, false data injection and DoS attacks	A high detection accuracy for single and combined attacks.	The performance of HEKA is evaluated using datasets generated from different real devices.
[49]	A cooperative intrusion detection system for ad hoc networks	2003	Statistical-based IDS	Mobile agent technology	Distributed	ns-2 [29], MobiEmu [149]	Blackhole attack, Spoofing attack, Selfishness attack, DoS attack, Sleep deprivation attack	A good accuracy in detecting some attacks. It shares the overhead between nodes.	It is able to identify the attacker as well as the attack type.
[125]	iDetect: an intelligent intrusion detection system for wireless body area networks	2016	Anomaly-based IDS	Multi-objective genetic algorithm	Distributed	TOSSIM [72]	Jamming attacks, Selective forwarding attack	A good accuracy without breaching the acceptable level of energy consumption.	It reduces the computation complexity by using a reduced set of features for detection.
[93]	Distributed intrusion detection using mobile agents in wireless body area networks	2017	Anomaly-based IDS	Five machine learning algorithms (DT, SVM, RF, NBC, KNN)	Hierarchical and distributed	Castalia [15]	Denial of Service Attacks, Data Falsification, Passive Listening	Accuracy and power consumption are assessed for the following machine learning algorithms DT, SVM, RF, NBC, KNN.	Around 6% rise in power consumption; however, results do not show the positive reflection of the proposed framework on the accuracy metric.
[126]	Autonomous mobile agent based intrusion detection framework in wireless body area networks	2015	Anomaly-based IDS	Mobile agent technology	Distributed	Not used	No attacks are tested for evaluation	Authors state that the proposed framework is able to reduce the communication overhead.	The proposed framework has to be evaluated to find out its feasibility for WBAN.
[121]	A Novel Intrusion Detection System for Wireless Body Area Network in Health Care Monitoring	2010	Anomaly-based IDS	Negative Selection Algorithm	Centralized	QualNet [124]	Denial of Service attacks	A good accuracy in detecting compromised nodes. Minimising the false positives rate.	The performance of the proposed scheme has been evaluated for different routing protocols.
[40]	Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study	2020	Anomaly-based IDS	Four machine learning algorithms (RF, KNN, ANN, SVM)	Distributed	N/A	MITM attacks	A dataset representing two kind of features (network and biometrics).	Further investigation is required to optimize the system overhead.

when a malicious node colludes to destroy some victimized nodes' reputation by giving negative recommendations [45].

- Ballot stuffing attack: Another type of dishonest recommendations attacks. It is the opposite scenario of the bad-mouthing attack. It happens when some nodes give positive recommendations for a malicious node [62].
- Collusion attack: Unlike bad-mouthing and ballot stuffing attacks where just one malicious node provides dishonest recommendations. In the collusion attack, a set of nodes participates in the attack by providing false information, which may mislead the system to take unfair decisions depending on false information received from different sources [43].
- Selective forwarding attack: Discussed in section 4.

Based on the method of estimating the trust value, TMSs could be divided into four groups:

5.3.1. Fuzzy logic based TMSs

In fuzzy-based TMSs, trust value is estimated using fuzzy logic and predefined criteria that have a fuzzy-nature.
DTMS [47] is a fuzzy logic based TMS, which is uniformly distributed amongst the sensor nodes. The authors suggest many different criteria to be taken into account when estimating the direct trust value. Considering all these criteria can increase the computational overhead. DTMS estimates the current trust value by weighting the direct trust value and indirect trust value for each adjacent node. Afterward, the total trust is estimated from the current and previous trust values using the same weighting technique. DTMS shows superior performance compared with earlier trust management models. However, using trust matrices and tables can produce a significant network overhead [60]. FTM-IoMT [8] is another fuzzy-based trust management system proposed for the Internet of Medical Things (IoMT) to prevent Sybil attacks. It is a centralized approach that uses integrity, receptivity and compatibility to evaluate the trust value for the requesting nodes. However, it shows significant processing overhead, which requires further investigation to reduce the

packet delivery latency and the server-side overhead.

5.3.2. Probability based TMSs

Many research projects are put forward using the probability distribution theory in order to estimate the trust value using the inference of former values. Almost all probability-based TMSs use beta probability distribution to evaluate the reputation value; however, other probability distributions such as exponential probability distribution and binomial probability distribution are also used in the literature [37, 151].
To the best of our knowledge, RFSN [39] is the first trust management scheme that uses the beta distribution to evaluate the reputation value for WSN. RFSN uses a watchdog mechanism to collect new observations, which are used to update the posterior reputation value. LTMS [42] is a lightweight TMS for Wireless Medical Sensor Networks (WMSNs). Two methods are proposed in LTMS to evaluate the trust value to fit the resource constraints of in-body, on-body and off-body sensor nodes. LTMS has contrasted with known trust schemes, such as ReTrust [45] and RaRTrust [69], and showed superior performance in terms of detecting attacks and processing overhead. Another probability-based TMS is ETRES [151], which uses the exponential probability distribution in order to represent the reputation value of a node by assuming that the future behavior will have the same mode of the node history. ETRES only considers the indirect recommendations when the certainty of the trust level is not adequate to enhance power consumption. The uncertainty is obtained using the information entropy theory. Both direct reputation value and indirect one are weighted in order to give more significance to the up to date information and the most reputable recommender, respectively. Later, the overall trust value is estimated using the confidence factor technique. Comparing to RFSN [38] and BTMS [36], ETRES shows a bit higher performance.

5.3.3. Weighting based TMSs

A simple way to evaluate the nodes' behavior and generate the trust value for each node based on weighting the nodes' reputation over time. Although this type of TMS is easy to deploy, it lacks a robust math ground [53]. TMR [67] is a weighting based TMS using risk assessment. Considering the risk factor can prompt a fast reaction to misbehaved nodes by making destroying the obtained trust value easier than building it. Evaluating the risk factor enhances the trust management model's reliability by making it more sensitive to any malicious activities. In TMR, both direct trust and indirect recommendations in addition to the risk factor and previous trust value are considered to evaluate the current trust value. RaRTrust [70] is another example of weighting based TMS where authors use the timing window technique for processing the previous trust values. RaRTrust considers the risk assessment technique by adopting a balancing factor that makes acquiring trust is harder than losing it. While RaRTrust shows resiliency to on-off attacks and badmouthing attacks, TMR is just able to defeat on-off attacks.

5.3.4. Other TMSs

There are some TMSs that do not fall within the previous categorization. In [50], a cluster-based with a 3-tier architecture TMS is proposed where tier 1 just focuses on nodes registration. In tier 2, five levels of misbehavior are defined. Although the proposed scheme considers the previous information to find out malicious nodes during the trust process, the used machine learning algorithm is not disclosed. Furthermore, the authors give the same weight for both direct and indirect trust values. To evaluate the overall trust value, a traditional summation technique is used, which may lead to an un-scaled value depending on the number of adjacent nodes. In tier 3, the whole process is about monitoring the consumed power of Cluster Head (CH), and when a threshold is triggered, a new CH is chosen based on the level of trust that nodes have.

The TMSs surveyed in this paper are summarized in Table 4, stating the topology architecture, simulators used, and the proposed contributions.

6. Research Opportunities

WBAN brings new research opportunities to wireless healthcare networks. The ongoing development of WBAN encounters severe resource constraints challenges, in addition to challenges posed by the sensitive nature of WBAN data and the potential catastrophic consequences of compromising network nodes. Therefore, many research opportunities emerge in order to meet these strict restrictions. This section states potential research directions to enhance WBAN technology, including security, communication protocols, and power consumption considerations.

6.1. Upper Stack Protocols

In February 2012, the first and the only WBAN standard were released [51]. IEEE 802.15.6 standardizes the Media Access Control (MAC) layer that supports three different physical layers. WBAN provides low power and short-range wireless communication for devices that operate on, in, or around the human body. Thus, the IEEE standard does not provide a full protocol stack. IEEE 802.15.4/Zigbee is a full protocol stack developed by Zigbee Alliance, an organization working in conjunction with IEEE TG4. IEEE 802.15.4/Zigbee is developed to fulfill the requirements of WSN based on IEEE 802.15.4 [28]. IPv6 over Low Power Personal Area Network (6LoWPAN) is another upper stack introduced by the Internet Engineering Task Force (IETF) to fit into the requirements of WSN. Many research [64, 79, 86, 143] investigate 6LoWPAN and Zigbee protocol stacks as upper stack of IEEE 802.15.4. However, both upper stack protocols have to be fully investigated with IEEE 802.15.6.

6.2. Multi-Hop Communication

WBAN standard adopts a star topology with a maximum of two-hop communication. Theoretically, using a multi-hop approach can potentially provide more reliable communication that may enhance the overall performance; however, this argument has to be proven by experiments taking into account

Table 4
Trust Management Systems Schemes

Literature	Title	Year	Solution	Technology	Architecture	Simulator	Contributions	Comments
[42]	LTMS: A Lightweight Trust Management System for Wireless Medical Sensor Networks	2020	Probability based TMS	Wireless Medical Sensor Networks	Distributed	NS-3 [96]	Two methods to evaluate the trust value for in-body, on-body and off-body SNs.	It is a lightweight trust management scheme that can defend against complicated on-off attacks.
[47]	A fuzzy fully distributed trust management system in wireless sensor networks	2016	Fuzzy logic based TMS	Wireless Sensor Networks	Uniform distributed arcitecture	TRMSim-WSN [87]	DTMS shows superior performance comparing with earlier TM models. It detects compromised, selfish and malicious nodes.	Using trust matrices and tables produces significant overhead [60].
[151]	An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks	2019	Probability based TMS	Wireless Sensor Networks	Distributed	MATLAB	A bit better performance comparing to RFSN [38] and BTMS [36]. Resilience to on-off attack. Resilience to selective forwarding attack. Detecting compromised nodes.	According to the authors, energy consumption will be considered in the future research.
[67]	A reliable trust management scheme in wireless sensor networks	2015	Weighting based TMS	Wireless Sensor Networks	Distributed	MATLAB	It considers the risk factor. Resilience to on-off attack.	The used weighting factors have to be optimized.
[70]	A risk-aware reputation-based trust management in wireless sensor networks	2016	Weighting based TMS	Wireless Sensor Networks	Distributed	MATLAB	It considers the risk factor in addition to a sliding timing window of interactions and local ratings. Resilience to on-off attack.	RaRTrust is able to reduce the effect of bad-mouthing attack.
[50]	A cluster based energy efficient trust management mechanism for medical wireless sensor networks (MWSNs)	2018	Machine learning technique	Medical Wireless Sensor Networks	Cluster based with 3-tier (Hybrid)	ns-2 [15]	Energy efficient by rotating cluster head among the nodes.	The used machine learning algorithm is not disclosed. Unscaled total trust value.
[8]	FTM-IOMT: Fuzzy-based trust management for preventing Sybil attacks in internet of medical things	2020	Fuzzy logic based TMS	Internet of Medical Things	Centralized	Cooja [33]	A centralized approach to evaluate the trustworthiness using integrity, compatibility and receptivity features.	Further work is needed to reduce the server side overhead and the packet delivery latency.

power conservation. In [89], authors find out that using a multi-hop communication enhances the packet delivery ratio. Therefore, further investigation of the multi-hop topology can be rewarding for WBAN.

6.3. Routing

Routing protocols applicable to WBAN is still an open research opportunity. Dedicated protocols need to be considered taking into account the nature of WBAN, where packets have to pass through relaying nodes in order to reach the sink node. There is a wide range of routing protocols proposed for WSN. However, it is not an easy task to choose the most suitable routing protocol for WBAN topology, which conserves power consumption and minimizes communication overhead. Possible consideration could involve QoS-aware, temperature-aware, cross-layered, and postural movement-based routing protocols [9].

6.4. Authentication and Key Establishment

Authentication and key establishment pose a wide range of research opportunities. Most of the literature's proposed schemes are either still vulnerable to some kinds of attack or do not fully address the WBAN security requirements. Moreover, any proposed scheme for key establishment and key revocation, when necessary, must prove its merit in resource conservation.

6.5. Encryption

Data encryption is essential when personal and sensitive data are involved, as the case with WBAN. Encryption should provide data protection in both transmission and storage stages to prevent attacks such as eavesdropping-based attacks. Proposing a lightweight and energy-aware encryption algorithm that satisfies both the security requirements and the stringent resource constraints is still an open area of research with vast contribution opportunities.

6.6. Intrusion Detection Systems

Intrusion detection is another potential area of research. Traditional security schemes aim to keep attackers out; however, they do not have the ability to detect internal attacks and react to them accordingly. Therefore, applying IDS to WBAN can address attacks and vulnerabilities where traditional schemes fail to do so. For instance, DoS attacks affect the network's availability and may not be detectable by traditional security countermeasures. Therefore, further investigation for developing a WBAN specific IDS is necessary to detect different types of attacks.

6.7. Sustainable Power Source

One of the main challenging tasks is maintaining a continuous source of power to nodes implanted inside the body since replacing the battery of implanted devices requires surgery. Therefore, finding other sources of energy is still an open area of research. For instance, according to [57], each cm^2 of the human body is able to produce 20 mW compared with $15mW/cm^2$ produced by solar panels, which makes it a promising alternative source of energy.

6.8. Security Evaluation

Most security countermeasures are evaluated using simulations in order to prove their effectiveness. This is due to the difficulty of getting real testbeds. Therefore, there is a lack of realistic evaluation regarding the effectiveness of the proposed security mechanisms applicable to medical devices. This creates additional research opportunities for realistic evaluation of WBAN security countermeasures.

6.9. Smart Transmission

Transmission is the main contributor to power consumption. Adopting any smart transmission technology such as cognitive radio may enhance power consumption and prolong battery life dramatically. Therefore, the optimized transmission is a significantly challenging task and still has opportunities for further research contributions.

6.10. Data Processing

Data processing is another open research area in the Internet of Things (IoT) field, which WBAN is part of. WBAN nodes generate a massive amount of data that needs to be stored and processed in a secure manner to guarantee patients' security and privacy. On the other hand, different WBAN sensors may register the same physiological signals, which consequently pose a challenge for their data processing. Therefore, effective methods for big data processing and data fusion are possible research opportunities.

6.11. Access Control

Developing an adequate access control mechanism is another possible research direction. Access control allows physicians and technicians to adjust the configuration of the sensor nodes. Two types of access control should be considered, which are attribute-based and role-based, in order to ensure patient safety and privacy.

7. Conclusion

In this survey paper, a review of the current research and future research directions on Wireless Body Area Networks have been presented. First, a concise overview of WBAN architecture, topology and design requirements have been discussed. Furthermore, security requirements and challenges have been investigated, and a wide range of threats and attacks are identified. Moreover, different types of security countermeasures have been discussed throughout the survey to meet the security requirements of WBAN and defeat potential threats. Specifically, secure communication, intrusion detection systems and trust management systems. Finally, potential research opportunities and directions have been proposed.

References

[1] Abdel-Fattah, F., Farhan, K.A., Al-Tarawneh, F.H., AlTamimi, F., 2019. 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), IEEE. pp. 28–33.

[2] Abidi, B., Jilbab, A., Mohamed, E.H., 2020. Wireless body area networks: a comprehensive survey. Journal of Medical Engineering & Technology , 1–11.

[3] Al Ameen, M., Liu, J., Kwak, K., 2012. Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems 36, 93–101.

[4] Al Barazanchi, I., Abdulshaheed, H.R., Safiah, M., Sidek, B., 2020. A survey: Issues and challenges of communication technologies in wban. Sustain. Eng. Innov 1, 84–97.

[5] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., Shamshirband, S., 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal 18, 113–122.

[6] Al-Riyami, S.S., Paterson, K.G., 2003. Certificateless public key cryptography, in: International conference on the theory and application of cryptology and information security, Springer. pp. 452–473.

[7] Alaparthy, V.T., Morgera, S.D., 2018. A multi-level intrusion detection system for wireless sensor networks based on immune theory. IEEE Access 6, 47364–47373.

[8] Almogren, A., Mohiuddin, I., Din, I.U., Al Majed, H., Guizani, N., 2020. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. IEEE Internet of Things Journal .

[9] Bangash, J., Abdullah, A., Anisi, M., Khan, A., 2014. A survey of routing protocols in wireless body sensor networks. sensors 14, 1322–1357.

[10] Barakah, D.M., Ammad-uddin, M., 2012. 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, IEEE. pp. 214–219.

[11] Barbi, M., Sayrafian, K., Alasti, M., 2016. Using rts/cts to enhance the performance of ieee 802.15.6 csma/ca, in: 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE. pp. 1–5.

[12] Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., Wingers, L., 2015. The simon and speck lightweight block ciphers, in: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), IEEE. pp. 1–6.

[13] Bharathi, K.S., Venkateswari, R., 2019. Security challenges and solutions for wireless body area networks, in: Computing, Communication and Signal Processing. Springer, pp. 275–283.

[14] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., et al., 2012. Prince–a low-latency block cipher for pervasive computing applications, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer. pp. 208–225.

[15] Boulis, T., Tselishchev, Y., Pediaditakis, D., . Castalia simulator. URL: https://github.com/boulis/Castalia. accessed: 23-04-2019.

[16] Butun, I., Morgera, S.D., Sankar, R., 2014. A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials 16, 266–282.

[17] Cai, L., Zeng, K., Chen, H., Mohapatra, P., 2011. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas., in: NDSS.

[18] Canteaut, A., Naya-Plasencia, M., Vayssiere, B., 2013. Sieve-in-the-middle: improved mitm attacks, in: Annual Cryptology Conference, Springer. pp. 222–240.

[19] Cao, X., Zeng, X., Kou, W., Hu, L., 2009. Identity-based anonymous remote authentication for value-added services in mobile networks. IEEE Transactions on Vehicular Technology 58, 3508–3517.

[20] Cavallari, R., Martelli, F., Rosini, R., Buratti, C., Verdone, R., 2014. A survey on wireless body area networks: Technologies and design challenges. IEEE Communications Surveys & Tutorials 16, 1635–1657.

[21] Chai, Q., Gong, G., 2012. A cryptanalysis of hummingbird-2: The differential sequence analysis. IACR Cryptology ePrint Archive 2012,

233.

[22] Challa, S., Wazid, M., Das, A.K., Khan, M.K., 2017. Authentication protocols for implantable medical devices: taxonomy, analysis and future directions. IEEE Consumer Electronics Magazine 7, 57–65.

[23] Chaudhary, S., Singh, A., Chatterjee, K., 2019. Wireless body sensor network (wbsn) security and privacy issues: A survey. International Journal of Computational Intelligence & IoT 2.

[24] Chen, H., Wang, X., 2016. Improved linear hull attack on round-reduced simon with dynamic key-guessing techniques, in: International Conference on Fast Software Encryption, Springer. pp. 428–449.

[25] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., Leung, V.C., 2011. Body area networks: A survey. Mobile networks and applications 16, 171–193.

[26] CMT, . Micaz. URL: http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet-t.pdf. accessed: 07-11-2019.

[27] Çoban, M., Karakoç, F., Boztaş, Ö., 2012. Biclique cryptanalysis of twine, in: International Conference on Cryptology and Network Security, Springer. pp. 43–55.

[28] Cunha, A., Koubaa, A., Severino, R., Alves, M., 2007. Open-zb: an open-source implementation of the ieee 802.15. 4/zigbee protocol stack on tinyos, in: 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems, IEEE. pp. 1–12.

[29] DARPA, . ns-2. URL: https://www.isi.edu/nsnam/ns/. accessed: 25-04-2019.

[30] Diaz, A., Sanchez, P., 2016. Simulation of attacks for security in wireless sensor network. Sensors 16, 1932.

[31] Dinur, I., 2014. Improved differential cryptanalysis of round-reduced speck, in: International Conference on Selected Areas in Cryptography, Springer. pp. 147–164.

[32] Djenouri, D., Khelladi, L., Badache, N., 2005. Security issues of mobile ad hoc and sensor networks, in: IEEE Communications Surveys Tutorials, IEEE Communications Society. pp. 2–28.

[33] Dunkels, A., . Cooja. URL: http://www.contiki-os.org. accessed: 25-04-2019.

[34] Dworkin, M.J., 2004. Sp 800-38c. recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality .

[35] Engels, D., Saarinen, M.J.O., Schweitzer, P., Smith, E.M., 2011. The hummingbird-2 lightweight authenticated encryption algorithm, in: International Workshop on Radio Frequency Identification: Security and Privacy Issues, Springer. pp. 19–31.

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

[37] Fang, W., Zhu, C., Chen, W., Zhang, W., Rodrigues, J.J., 2018. Bdtms: Binomial distribution-based trust management scheme for healthcare-oriented wireless sensor network, in: 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), IEEE. pp. 382–387.

[38] Ganeriwal, S., Balzano, L.K., Srivastava, M.B., 2008. Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks (TOSN) 4, 15.

[39] Ganeriwal, S., Srivastava, M.B., 2004. Reputation-based framework for high integrity sensor networks, in: Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM. pp. 66–77.

[40] Hady, A.A., Ghubaish, A., Salman, T., Unal, D., Jain, R., 2020. Intrusion detection system for healthcare systems using medical and network data: A comparison study. IEEE Access 8, 106576–106584.

[41] Hajar, M.S., Al-Kadri, M.O., Kalutarage, H., 2020a. Etaree: An effective trend-aware reputation evaluation engine for wireless medical sensor networks, in: 2020 IEEE Conference on Communications and Network Security (CNS), IEEE. pp. 1–9.

[42] Hajar, M.S., Al-Kadri, M.O., Kalutarage, H., 2020b. Ltms: A lightweight trust management system for wireless medical sensor networks, in: 2020 The 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020), IEEE. pp. 1–8.

[43] Han, G., Jiang, J., Shu, L., Niu, J., Chao, H.C., 2014. Management and applications of trust in wireless sensor networks: A survey. Journal of Computer and System Sciences 80, 602–617.

[44] Hao, Y., Bai, D., Li, L., 2015. A meet-in-the-middle attack on round-reduced mcrypton using the differential enumeration technique, in: International Conference on Network and System Security, Springer. pp. 166–183.

[45] He, D., Chen, C., Chan, S., Bu, J., Vasilakos, A.V., 2012. Retrust: Attack-resistant and lightweight trust management for medical sensor networks. IEEE transactions on information technology in biomedicine 16, 623–632.

[46] He, D., Zeadally, S., 2015. Authentication protocol for an ambient assisted living system. IEEE Communications Magazine 53, 71–77.

[47] Hossein, J., Mohammad, R., et al., 2016. A fuzzy fully distributed trust management system in wireless sensor networks. International Journal of Electronics and Communications 9, 1–10.

[48] Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X., Chen, D., 2013. Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks, in: 2013 Proceedings IEEE INFOCOM, IEEE. pp. 2274–2282.

[49] Huang, Y.a., Lee, W., 2003. A cooperative intrusion detection system for ad hoc networks, in: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, ACM. pp. 135–147.

[50] Hussain, S.A., Raza, I., Mehdi, M.M., 2018. 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), IEEE. pp. 433–439.

[51] IEEE, 2012. Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks. IEEE Std 802.15.6-2012 , 1–271doi:10.1109/IEEESTD.2012.6161600.

[52] IEEE, 2016. Ieee standard for low-rate wireless networks. IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011) , 1–709doi:10.1109/IEEESTD.2016.7460875.

[53] Ishmanov, F., Malik, A.S., Kim, S.W., Begalov, B., 2015. Trust management system in wireless sensor networks: design considerations and research challenges. Transactions on Emerging Telecommunications Technologies 26, 107–130.

[54] Islam, S.H., Biswas, G., 2011. A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Journal of Systems and Software 84, 1892–1898.

[55] Javadi, S.S., Razzaque, M., 2013. Security and privacy in wireless body area networks for health care applications, in: Wireless networks and security. Springer, pp. 165–187.

[56] Jo, M., Han, L., Tan, N.D., In, H.P., 2015. A survey: energy exhausting attacks in mac protocols in wbans. Telecommunication Systems 58, 153–164.

[57] Johny, B., Anpalagan, A., 2014. Body area sensor networks: Requirements, operations, and challenges. IEEE Potentials 33, 21–25.

[58] Kaliski, B., 2006. The mathematics of the rsa public-key cryptosystem. RSA Laboratories .

[59] Kasyoka, P., Kimwele, M., Mbandu Angolo, S., 2020. Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. Journal of Medical Engineering & Technology 44, 12–19.

[60] Kazmi, F., Khan, M.A., Saeed, A., Saqib, N.A., Abbas, M., 2018. Evaluation of trust management approaches in wireless sensor networks, IEEE. pp. 870–875.

[61] Khan, H., Dowling, B., Martin, K.M., 2018. 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), IEEE. pp. 1064–1069.

[62] Khan, T., Singh, K., Abdel-Basset, M., Long, H.V., Singh, S.P., Manjul, M., et al., 2019. A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks.

IEEE Access 7, 58221–58240.
[63] Khernane, N., Potop-Butucaru, M., Chaudet, C., 2016. 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), IEEE. pp. 307–315.
[64] Kohvakka, M., Kuorilehto, M., Hännikäinen, M., Hämäläinen, T.D., 2006. Performance analysis of ieee 802.15. 4 and zigbee for large-scale wireless sensor network applications, in: Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks, ACM. pp. 48–57.
[65] Kompara, M., Hölbl, M., 2018. Survey on security in intra-body area network communication. Ad Hoc Networks 70, 23–43.
[66] Kwak, K.S., Ullah, S., Ullah, N., 2010. An overview of ieee 802.15.6 standard, in: 2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010), IEEE. pp. 1–6.
[67] Labraoui, N., 2015. A reliable trust management scheme in wireless sensor networks, in: 2015 12th International Symposium on Programming and Systems (ISPS), IEEE. pp. 1–6.
[68] Labraoui, N., Gueroui, M., Sekhri, L., 2015. On-off attacks mitigation against trust systems in wireless sensor networks, in: IFIP International Conference on Computer Science and its Applications, Springer. pp. 406–415.
[69] Labraoui, N., Gueroui, M., Sekhri, L., 2016a. A risk-aware reputation-based trust management in wireless sensor networks. Wireless Personal Communications 87, 1037–1055.
[70] Labraoui, N., Gueroui, M., Sekhri, L., 2016b. A risk-aware reputation-based trust management in wireless sensor networks. Wireless Personal Communications 87, 1037–1055.
[71] Latré, B., Braem, B., Moerman, I., Blondia, C., Demeester, P., 2011. A survey on wireless body area networks. Wireless Networks 17, 1–18.
[72] Levis, P., Lee, N., Welsh, M., Culler, D., . Tossim. URL: http://tinyos.stanford.edu/tinyos-wiki/index.php/TOSSIM. accessed: 25-04-2019.
[73] Li, M., Yu, S., Guttman, J.D., Lou, W., Ren, K., 2013. Secure ad hoc trust initialization and key management in wireless body area networks. ACM Transactions on sensor Networks (TOSN) 9, 18.
[74] Li, X., Ibrahim, M.H., Kumari, S., Sangaiah, A.K., Gupta, V., Choo, K.K.R., 2017a. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks 129, 429–443.
[75] Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M., Choo, K.K.R., 2017b. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Computers & Electrical Engineering 61, 238–249.
[76] Lim, C.H., Korkishko, T., 2005. mcrypton–a lightweight block cipher for security of low-cost rfid tags and sensors, in: International Workshop on Information Security Applications, Springer. pp. 243–258.
[77] Liu, A., Ning, P., 2008. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks, in: Proceedings of the 7th international conference on Information processing in sensor networks, IEEE Computer Society. pp. 245–256.
[78] Liu, R., Wang, Y., 2014. A new sybil attack detection for wireless body sensor network, in: 2014 Tenth International Conference on Computational Intelligence and Security, IEEE. pp. 367–370.
[79] Ma, X., Luo, W., 2008. The analysis of 6lowpan technology, in: 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, IEEE. pp. 963–966.
[80] Mainanwal, V., Gupta, M., Upadhayay, S.K., 2015. 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), IEEE. pp. 1–5.
[81] Masdari, M., Ahmadzadeh, S., 2016. Comprehensive analysis of the authentication methods in wireless body area networks. Security and Communication Networks 9, 4777–4803.
[82] Mathur, S., Miller, R., Varshavsky, A., Trappe, W., Mandayam, N., 2011. Proximate: proximity-based secure pairing using ambient wireless signals, in: Proceedings of the 9th international conference on Mobile systems, applications, and services, ACM. pp. 211–224.
[83] McKay, K., Bassham, L., Sönmez Turan, M., Mouha, N., 2016. Report on lightweight cryptography. Technical Report. National Institute of Standards and Technology.
[84] Misra, S., Vaish, A., 2011. Reputation-based role assignment for role-based access control in wireless sensor networks. Computer Communications 34, 281–294.
[85] Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., Jamalipour, A., 2014. Wireless body area networks: A survey. IEEE Communications surveys & tutorials 16, 1658–1686.
[86] Mulligan, G., 2007. The 6lowpan architecture, in: Proceedings of the 4th workshop on Embedded networked sensors, ACM. pp. 78–82.
[87] Mármol, F.G., . Trmsim-wsn. https://sourceforge.net/projects/trmsim-wsn/. Accessed: 2019-05-02.
[88] Nadeem, A., Javed, M.Y., 2005. A performance comparison of data encryption algorithms, in: 2005 international conference on information and communication technologies, IEEE. pp. 84–89.
[89] Natarajan, A., Motani, M., de Silva, B., Yap, K.K., Chua, K.C., 2007. Investigating network architectures for body sensor networks, in: Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, ACM. pp. 19–24.
[90] Ndoye, E., Jacquet, F., Misson, M., Niang, I., 2013. Evaluation of rts/cts with unslotted csma/ca algorithm in linear sensor networks. NICST 2013 .
[91] Newaz, A.I., Sikder, A.K., Babun, L., Uluagac, A.S., 2020. Heka: A novel intrusion detection system for attacks to personal medical devices, in: 2020 IEEE Conference on Communications and Network Security (CNS), IEEE. pp. 1–9.
[92] Niksaz, P., Branch, M., 2015. Wireless body area networks: attacks and countermeasures. International Journal of scientific and engineering research 6, 565–568.
[93] Odesile, A., Thamilarasu, G., 2017. Distributed intrusion detection using mobile agents in wireless body area networks, in: 2017 Seventh International Conference on Emerging Security Technologies (EST), IEEE. pp. 144–149.
[94] Office of National Statistics, 2016. National population projections: 2016-based statistical bulletin. URL: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationprojections/bulletins/nationalpopulationprojections/2016basedstatisticalbulletin/pdf. accessed: 14-05-2019.
[95] Omala, A.A., Kibiwott, K.P., Li, F., 2017. An efficient remote authentication scheme for wireless body area network. Journal of medical systems 41, 25.
[96] Open source, . Ns-3 a discrete-event network simulator for internet systems. URL: https://www.nsnam.org/releases/. accessed: 09-12-2020.
[97] Osanaiye, O.A., Alfa, A.S., Hancke, G.P., 2018. Denial of service defence for resource availability in wireless sensor networks. IEEE Access 6, 6975–7004.
[98] Padmavathi, B., Kumari, S.R., . A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution .
[99] Paul, P.C., Loane, J., Regan, G., McCaffery, F., 2019. Analysis of attacks and security requirements for wireless body area networks-a systematic literature review, in: European Conference on Software Process Improvement, Springer. pp. 439–452.
[100] Paul, S., Chakraborty, A., Banerjee, J.S., 2017. A fuzzy ahp-based relay node selection protocol for wireless body area networks (wban), in: 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), IEEE. pp. 1–6.
[101] Polai, M., Mohanty, S., Sahoo, S.S., 2019. A lightweight mutual authentication protocol for wireless body area network, in: 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), IEEE. pp. 760–765.
[102] Qiao, K., Hu, L., Sun, S., 2015. Differential security evaluation of

simeck with dynamic key-guessing techniques. IACR Cryptology ePrint Archive 2015, 902.

[103] Rajasekaran, R.T., Manjula, V., Kishore, V., Sridhar, T., Jayakumar, C., 2012. An efficient and secure key agreement scheme using physiological signals in body area networks, in: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, ACM. pp. 1143–1147.

[104] Rughiniş, R., Gheorghe, L., 2010. Storm control mechanism in wireless sensor networks, in: 9th RoEduNet IEEE International Conference, pp. 430–435.

[105] Sammoud, A., Chalouf, M.A., Hamdi, O., Montavont, N., Bouallegue, A., 2020. A new biometrics-based key establishment protocol in wban: energy efficiency and security robustness analysis. Computers & Security , 101838.

[106] Segovia, M., Grampín, E., Baliosian, J., 2013. Analysis of the applicability of wireless sensor networks attacks to body area networks, in: Proceedings of the 8th International Conference on Body Area Networks, ICST (Institute for Computer Sciences, Social-Informatics and .... pp. 509–512.

[107] Shakhov, V.V., 2013. Protecting wireless sensor networks from energy exhausting attacks, in: International Conference on Computational Science and Its Applications, Springer. pp. 184–193.

[108] Shamir, A., 1984. Identity-based cryptosystems and signature schemes, in: Workshop on the theory and application of cryptographic techniques, Springer. pp. 47–53.

[109] Sharma, R., Kang, S.S., 2020. Wban for healthcare applications: A survey of current challenges and research opportunities. Journal of Critical Reviews 7, 2444–2453.

[110] Shen, J., Chang, S., Shen, J., Liu, Q., Sun, X., 2018a. A lightweight multi-layer authentication protocol for wireless body area networks. Future Generation Computer Systems 78, 956–963.

[111] Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., Tang, Y., 2018b. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications 106, 117–123.

[112] Shi, L., Li, M., Yu, S., Yuan, J., 2013. Bana: body area network authentication exploiting channel characteristics. IEEE Journal on selected Areas in Communications 31, 1803–1816.

[113] Shi, L., Yuan, J., Yu, S., Li, M., 2015. Mask-ban: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. IEEE Internet of Things Journal 2, 52–62.

[114] Shim, K.A., 2018. Comments on "revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks". IEEE Transactions on Information Forensics and Security .

[115] Singh, R., Sinha, S., Anand, S., Sen, M., 2020. Wireless body area network: An application of iot and its issuses—a survey, in: Computational Intelligence in Pattern Recognition. Springer, pp. 285–293.

[116] Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H., 2017. Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing , 1–18.

[117] Singh, U., Narwal, B., . A novel authentication scheme for wireless body area networks with anonymity, in: Progress in Advanced Computing and Intelligent Engineering. Springer, pp. 295–305.

[118] Smith, D.B., Miniutti, D., Lamahewa, T.A., Hanlen, L.W., 2013. Propagation models for body-area networks: A survey and new outlook. IEEE Antennas and Propagation Magazine 55, 97–117.

[119] Soleimany, H., Blondeau, C., Yu, X., Wu, W., Nyberg, K., Zhang, H., Zhang, L., Wang, Y., 2015. Reflection cryptanalysis of prince-like ciphers. Journal of Cryptology 28, 718–744.

[120] Suh, G.E., Devadas, S., 2007. Physical unclonable functions for device authentication and secret key generation, in: 2007 44th ACM/IEEE Design Automation Conference, IEEE. pp. 9–14.

[121] Sundararajan, T., Shanmugam, A., 2010. A novel intrusion detection system for wireless body area network in health care monitoring. Journal of Computer Science 6, 1355.

[122] Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E., 2011. Twine: A lightweight, versatile block cipher, in: ECRYPT Workshop on Lightweight Cryptography.

[123] Tan, X., Zhang, J., Zhang, Y., Qin, Z., Ding, Y., Wang, X., 2020. A puf-based and cloud-assisted lightweight authentication for multi-hop body area network. Tsinghua Science and Technology 26, 36–47.

[124] Technologies, S.N., . Qualnet. URL: https://www.scalable-networks.com/qualnet-network-simulation. accessed: 25-04-2019.

[125] Thamilarasu, G., 2016. idetect: an intelligent intrusion detection system for wireless body area networks. International Journal of Security and Networks 11, 82–93.

[126] Thamilarasu, G., Ma, Z., 2015. 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), IEEE. pp. 1–3.

[127] Toorani, M., 2015. On vulnerabilities of the security association in the ieee 802.15. 6 standard, in: International conference on financial cryptography and data security, Springer. pp. 245–260.

[128] Toorani, M., 2016. Security analysis of the ieee 802.15. 6 standard. International Journal of Communication Systems 29, 2471–2489.

[129] Toprak, S., Akbulut, A., Aydın, M.A., Zaim, A.H., 2020. Lwe: An energy-efficient lightweight encryption algorithm for medical sensors and iot devices. Electrica 20, 71–81.

[130] Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., Kwak, K.S., 2012. A comprehensive survey of wireless body area networks. Journal of medical systems 36, 1065–1094.

[131] Ullah, S., Mohaisen, M., Alnuem, M.A., 2013. A review of ieee 802.15. 6 mac, phy, and security specifications. International Journal of Distributed Sensor Networks 9, 950704.

[132] Usman, M., Asghar, M.R., Ansari, I.S., Qaraqe, M., 2018. Security in wireless body area networks: From in-body to off-body communications. IEEE Access 6, 58064–58074.

[133] Vadlamani, S., Eksioglu, B., Medal, H., Nandi, A., 2016. Jamming attacks on wireless networks: A taxonomic survey. International Journal of Production Economics 172, 76–94.

[134] Wang, H., Li, Q., 2006. Efficient implementation of public key cryptosystems on mote sensors (short paper), in: International Conference on Information and Communications Security, Springer. pp. 519–528.

[135] Wang, W., Shi, X., Qin, T., 2018. Encryption-free authentication and integrity protection in body area networks through physical unclonable functions. Smart Health .

[136] World Health Organization, 2010. Global status report. URL: https://www.who.int/nmh/publications/ncd_report_full_en.pdf. accessed: 14-05-2019.

[137] Xie, L., Wang, W., Shi, X., Qin, T., 2017. Lightweight mutual authentication among sensors in body area networks through physical unclonable functions, in: 2017 IEEE International Conference on Communications (ICC), IEEE. pp. 1–6.

[138] Xiong, H., 2014. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Transactions on Information Forensics and Security 9, 2327–2339.

[139] Xiong, H., Qin, Z., 2015. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE transactions on information forensics and security 10, 1442–1455.

[140] Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G., 2015. The simeck family of lightweight block ciphers, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer. pp. 307–329.

[141] Yang, J.H., Chang, C.C., 2009. An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Computers & security 28, 138–143.

[142] Yazdandoost, K., Sayrafian-Pour, K., 2010. Tg6 channel model id: 802.15-08-0780-12-0006. IEEE submission, Nov .

[143] Yibo, C., Hou, K.M., Zhou, H., Shi, H.l., Liu, X., Diao, X., Ding, H., Li, J.J., De Vaulx, C., 2011. 6lowpan stacks: A survey, in: 2011 7th International Conference on Wireless Communications, Networking

and Mobile Computing, IEEE. pp. 1–4.
[144] Yoo, H.J., 2013. Wireless body area network and its healthcare applications, in: 2013 Asia-Pacific Microwave Conference Proceedings (APMC), IEEE. pp. 89–91.
[145] Zhan, G., Shi, W., Deng, J., 2012. Design and implementation of tarf: A trust-aware routing framework for wsns. IEEE Transactions on dependable and secure computing 9, 184–197.
[146] Zhang, L., Liu, J., Sun, R., 2013. An efficient and lightweight certificateless authentication protocol for wireless body area networks, in: 2013 5th International Conference on Intelligent Networking and Collaborative Systems, IEEE. pp. 637–639.
[147] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I., 2015. Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences 58, 1–15.
[148] Zhang, W., Qin, T., Mekonen, M., Wang, W., 2018. Wireless body area network identity authentication protocol based on physical unclonable function, in: 2018 International Conference on Sensor Networks and Signal Processing (SNSP), IEEE. pp. 60–64.
[149] Zhang, Y., Li, W., . Mobiemu. URL: http://mobiemu.sourceforge.net/. accessed: 25-04-2019.
[150] Zhang, Z., Wang, H., Vasilakos, A.V., Fang, H., 2012. Ecg-cryptography and authentication in body area networks. IEEE Transactions on Information Technology in Biomedicine 16, 1070–1078.
[151] Zhao, J., Huang, J., Xiong, N., 2019. An effective exponential-based trust and reputation evaluation system in wireless sensor networks. IEEE Access 7, 33859–33869.

Muhammad Shadi Hajar received his B.Eng. in Computer Engineering and Automation in 2008, and M.Sc. in Computer Engineering and Networking in 2013 from Damascus University, Damascus, Syria. He is currently pursuing his Ph.D. degree in Cyber Security at Robert Gordon University in the UK. His current research interests are in Wireless Medical Sensor Networks, Trust Management Systems, IoT security and lightweight authentication schemes.

M. Omar Al-Kadri received his B.Eng. in Computer Engineering from IUST, Syria, in 2010, M.Sc. (with distinction) in Networking and Data communication from Kingston University, UK in 2013, and Ph.D in Telecommunication engineering from King's College London, UK, in 2017. He is now an assistant professor in networking and cyber security at Robert Gordon University, UK. His current research interests include security of wireless communications with application to healthcare, security of vehicular networks, full-duplex communications, HetNets, and MAC/routing protocols.

Harsha Kumara Kalutarage is a lecturer in Cyber Security in the School of Computing at Robert Gordon University in the UK. He has 10+ years of research experience in Cyber Security and has produced 40+ publications in this area. His research interests span AI & Security, the use of AI for security applications and studying the security of AI-enabled systems. Harsha holds a Ph.D. in Computing (Cyber Security), an M.Phil. in Computer Science (NLP) and a B.Sc. Special (Hons) degree in Statistics & Computer Science.