Comprehensive Security for Body Area Networks: A Survey

Laura Victoria Morales, David Delgado-Ruiz, and Sandra Julieta Rueda
(Corresponding author: Laura Victoria Morales)

Systems and Computing Engineering Department, Universidad de los Andes
Cra 1 Este No 19A - 40, Mario Laserna Building, Bogotá, Colombia
(Email: l.morales825@uniandes.edu.co)
(Received Sept. 5, 2017; revised and accepted Apr. 13, 2018)

Abstract

Body Area Networks (BANs) are composed of multiple devices that measure, collect, forward and analyze physiological and medical data that may be used for different purposes like activity tracking, health monitoring or medical treatments. Given the type of data BANs manage, several security requirements must be addressed: confidentiality, integrity, privacy, authentication and authorization. This survey studies various proposals that aim to satisfy BAN security requirements, their advances and remaining challenges. We found that the mentioned requirements have not been comprehensively considered; the majority of the studied proposals do not address the entire BAN architecture, they focus on specific components. Although supporting security of individual BAN components is relevant, a comprehensive security view of an entire BAN environment is needed.

Keywords: BAN Security; Body Area Networks; eHealth

1 Introduction

Body Area Networks (BANs) enable wired and wireless communications among different types of devices, such as wearable and implantable sensors, smartphones, tablets and external servers, to collect physiological data for different purposes, particularly to support medical decisions and improve medical care. Data collected by BANs is considered sensitive, thus several security requirements must be addressed. If unauthorized entities gain access to this kind of data, patients may suffer diverse consequences, like job or insurance losses. Modified data may lead to wrong medical decisions; for example, an insulin pump may inject a wrong insulin dose [32, 38].

This survey studies different proposals that address security in BAN environments. We classified these proposals using two criteria: addressed security requirements and considered BAN components. The former aspect includes confidentiality, authentication, authorization, integrity and availability. The latter aspect considers BAN components including devices that measure physiological data (sensors and actuators), forward data (personal servers, smartphones or tablets), and store data (external servers and cloud).

We found that the studied projects only secure one or two components of a BAN architecture, sensors and actuators in particular. Although some BAN components are being secured, there is not a comprehensive security proposal for an entire BAN architecture. In order to build this comprehensive view, we must consider other devices like external servers, cloud services that store collected data, and even auxiliary devices, like gateways and access points.

Having a comprehensive view of the entire BAN architecture enables analysts to see security issues that may be hidden otherwise. For instance, some security solutions that work on external servers and cloud services, may not work on sensors and actuators because of their processing restrictions. Key management is particularly challenging, as it must consider different aspects for sensors and actuators, and for external servers. For example, some proposals generate keys using data collected by the sensors; however, a personal or external server cannot automatically compute these keys.

The rest of the paper is organized as follows: Section 2 presents an overview of BAN components and their interactions, Section 3 summarizes BAN security requirements and classifies the studied proposals according to addressed security requirements and BAN components, and Section 5 presents open issues. Section 6 concludes.

2 Body Area Network (BAN) Architecture

This section presents the main BAN components and types of communications. Later, we will use these characteristics to classify the studied security proposals.

2.1 Components

We identified the following categories of BAN components: Sensors and actuators, personal servers, auxiliary network devices, channels, external servers, and cloud services. Figure 1 illustrates BAN components and their interactions.

Sensors and Actuators: Sensors are implanted or wearable devices [10] that measure human physiological functions and environmental features. Actuators are devices that perform specific tasks; for example, the actuator in an insulin pump injects an insulin dose to a patient. Sensors and actuators may be part of a single device; Implantable Medical Devices (IMD) for instance, have sensors, actuators, and even a CPU [46]. Figure 1 shows several sensors: electroencephalography (EEG), electrocardiography (ECG), blood pressure and motion sensors.

Personal servers: These computing devices collect data from the sensors, temporarily store them, and forward them to interested parties, like a patient's medical team or family [8]. Different devices can be used as personal servers depending on a patient's movement restrictions; personal computers or laptops may work for users with mobility restrictions while tablets or smartphones are more adequate for physically active users. Figure 1 shows two devices that may work as personal servers: a tablet and a laptop.

Auxiliary Network Devices and Channels: We consider access points, gateways and cellular towers as auxiliary network devices, as these devices enable communications among components. Most communications are wireless, since the majority of possible personal servers have Wi-Fi antennas or use cellular networks, like smartphones and tablets. A BAN may also have wired communications; for example, when it includes a server deployed in a hospital. Figure 1 shows the following auxiliary devices: an access point, a gateway and a cellular tower.

External servers: External servers are medium and big-sized computing devices that gather and store information sent by several personal servers that belong to different patients. External servers may keep records for a high number of patients and records may have different types of data, like documents, diagnostic images or videos. Therefore, it is desirable to have servers with high storage and processing capacities.

Cloud: Cloud computing services provide additional storage and computing resources that may be needed in several contexts. For example, hospitals that have a high number of patients can use cloud storage. Cloud services may be used to analyze data for different purposes, like studying diseases and their behavior or creating predictive models.

2.2 Communication Types

We organized communication types in tiers, based on distance between communicating devices and the human body: Intra-BAN for close range, Inter-BAN for medium and Beyond-BAN for long range communications [10]. Figure 1 illustrates this classification.

Intra-BAN Communications: This tier covers communications happening within a two-meter radio from the human body, meaning that this tier comprehends sensor-to-sensor and sensor-to-personal server communications. In this tier, communications are typically wireless, using technologies such as Bluetooth and ZigBee, however wired communications are also possible.

Inter-BAN Communications: This tier covers communications between personal servers or sensors and an auxiliary network device to reach external servers. Internet or cellular networks can be used to establish this kind of communications. There are two types of architecture for Inter-BAN: infrastructure-based or ad hoc-based. The first one is used when a patient is confined within a limited space, like a room. In contrast, the ad hoc-based architecture allows a wider coverage, since it uses multiple access points to connect several networks [10].

Beyond-BAN Communications: The third tier covers communications between an access point, external servers and cloud resources, possibly covering metropolitan areas. In most cases a BAN needs a gateway to enable a connection between Inter-BAN and beyond-BAN devices [10].

3 Security Requirements and Solutions in a BAN Architecture

Different governments have different regulations to control management and address security concerns of health related information.

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) provides legislation and security provisions for safeguarding medical information [31, 32, 62]. The European Union published, in 2016, a new regulation to protect personal data. This regulation 'provides more rights to citizens to be better informed about the use of their personal data, and gives clearer responsibilities to people and entities using personal data. [15]. Australia's Personally Controlled Electronic Health Records and Canada's Health Information Legislation also protect patient's data. Other countries are also working on legislation to protect medical data of their citizens.

Some international standards also address these security concerns. The European Committee for Standardization (CEN/TC 251 - CEN Technical Committee 251) has

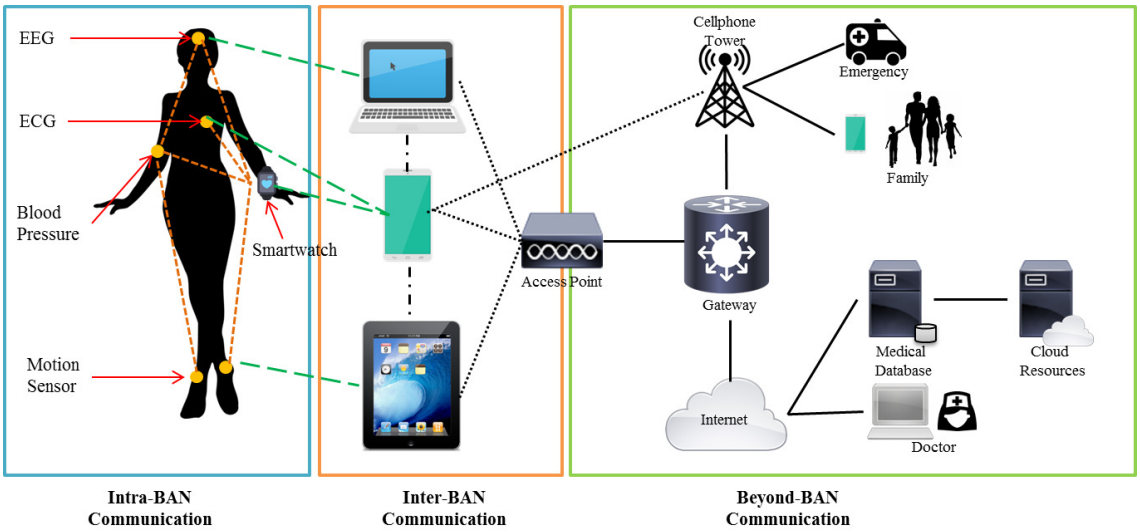

Figure 1: This figure illustrates components and communication types in a BAN architecture. Dashed thin lines show sensor-to-sensor communications and dashed thick lines show sensor-to-personal server communications. A smart watch is used as a sensor and also as a gateway, to send data from sensors to a smartphone, tablet or laptop that serves as the personal server. An access point and a gateway enable communication between personal and external servers. Beyond-BAN communications include communications with elements beyond the access point. Cellphones may use internet or a cellphone network to send data, while laptops and tablets usually do not have access to cellular networks and send data via internet. Extended from [10].

worked to define a standard for data management in the fields of Health Information and Communications Technology in the European Union. The standard establishes requirements for data compatibility and interoperability between systems, as well as data security requirements. The Technical Committee on health informatics of the International Organization for Standardization (ISO/TC 215) has already delivered several standards regarding security of medical records [1].

The IEEE 802.15.6 standard [28] identifies three security levels for BANs.

Level 0. Unsecured communication: No authentication or encryption techniques are used while sending messages.

Level 1. Authentication but not encryption: Authentication and some integrity validation are implemented.

Level 2. Authentication and encryption: Messages are transmitted in authenticated and encrypted frames. The standard also considers integrity, confidentiality and privacy.

Authorization, data freshness and software correctness are security requirement that also appear in a BAN context. In addition, different BAN components, with different features, interact to collect, process and forward data. These components may use different protocols to send sensitive data and may belong to different owners generating a large attack surface and several security concerns.

In this survey we looked for advances and remaining challenges in BAN security. To do so, we selected extended /full papers published in international conferences or journals between 2008 and 2016, that had BAN and security, or variations of these, as keywords. The variations of BAN included Body Area Networks and Body Sensor Networks, and the variations of security included confidentiality, integrity, authentication, authorization, availability and software correctness. We also looked for the first appearances of body sensors security and included one paper from 2003.

3.1 Confidentiality

The goal of this requirement is to guarantee that unauthorized people cannot read protected data. Since sensors generate physiological information that may reveal a disease or disability, data confidentiality is a relevant security requirement in BAN systems [38]. It is important to protect patient's data during transmission between devices, as well as in storage. In addition to medical data, BANs must also protect their device's information such as identification numbers, location, function, configuration and type [47].

3.1.1 Data Encryption and Key Generation

In our set of papers, cryptography is the most studied mechanism to offer confidentiality. However, implementing encryption algorithms for a BAN can be challenging due to power, memory and processing limitations, and low communication ranges of sensors and actu-

Table 1: Papers addressing BAN security requirements per year

	2003	2008	2009	2010	2011	2012	2013	2014	2015	2016	**Total**	**Percentage**
Confidentiality												
Data Encryption												
Secret	0	1	0	0	1	0	1	2	2	0	7	14.8 %
Elliptic Curves	0	0	0	1	1	2	0	1	1	1	7	14.8 %
Total	0	1	0	1	2	2	1	3	3	1	14	29.7 %
Key Generation												
Physiological Signals	1	2	2	3	2	2	3	1	0	1	17	36.1 %
Channel Characterization	0	0	0	0	2	2	3	0	0	0	7	14.8 %
Total	1	2	2	3	4	4	6	1	0	1	24	51%
Key Distribution												
Fuzzy vault	1	1	1	1	0	2	2	0	0	1	9	19.1 %
Diffie-Hellman	0	0	0	1	1	1	1	1	0	1	6	12.7 %
Other	0	2	0	0	1	1	1	2	3	1	11	23.4 %
Total	1	3	1	2	2	4	4	3	3	3	26	55.3%
Access Control												
Authentication	1	3	2	4	6	6	8	3	3	3	39	82.9 %
Authorization	0	0	1	1	1	0	3	0	1	1	8	17 %
Integrity												
Hash Functions	1	0	0	1	2	1	5	1	1	0	12	25.5 %
Session Management	0	1	0	2	3	0	4	1	1	1	13	27.6 %
Availability												
DoS Attack Protection	0	0	1	1	0	2	0	0	0	0	4	8.5 %
Total number of studied papers												**47**

ators [11, 12, 31, 38]. There is another challenge, in some scenarios data must be easily accessed; for example, in a medical emergency. If patient's data is encrypted and the key is not available, then a patient may not receive proper attention [17].

Considering restrictions of sensors and actuators, most of the solutions (38 out of 47 papers, see Table 2) look for efficient encryption methods. The most studied algorithms are secret key encryption and elliptic curve cryptography. Also, physiological values and channel characteristics are used as seeds to generate encryption keys.

Data encryption: Half of the papers that address data encryption use secret key cryptography [6, 18–20, 34, 35, 49], while the other half use Elliptic Curve Cryptography [25, 30, 33, 36, 37, 45, 52].

1) Secret Key Cryptography: Secret key algorithms are more suitable for BAN architectures than asymmetric key algorithms, because they use shorter key lengths, thus requiring shorter random numbers and less computational and energy resources [37]. In addition, symmetric encryption and decryption procedures are faster, making this algorithm better for emergency cases, where doctors will need to retrieve data as fast as possible. On the other hand, secret key algorithms must resolve the problem of key-distribution.

2) Elliptic Curves Cryptography (ECC): Since 2010 ECC has gained research interest (see Table 1). ECC is suitable for BAN architectures because it uses small keys; a 160-bit ECC key is as strong as a 1024-bit RSA key [33]. According to the NIST [9], a 2048 RSA key is equivalent to a 224 ECC key [37]. ECC keys can be distributed using protocols such as Diffie-Hellman. Furthermore, these keys can be used to create digital signatures for authentication purposes [25, 30, 33, 36, 37, 45, 52]. However, ECC implementations still must handle unsolved problems, including the creation of a random number generator for private keys, and the distribution of initial parameters [54].

Key Generation:

1) Physiological Values (PVs): PVs are used by around a third of the studied proposals, to generate encryption keys [11, 26, 40, 42, 44, 46, 50, 59–61, 64, 66, 67, 69]. Some PVs are used as seed for key generation because

   a. They are universal, as the majority of population have them;
   b. Two people do not share the same PVs;
   c. They are easy to collect and to measure;
   d. They are adequate for low computational power devices;
   e. They are difficult to reproduce;
   f. They are random [43, 62].

The Heart Rate Variability (HRV) is the most used PV. Several sensors, such as electrocardiograms (ECG or EKG) and photoplethysmograms (PPG), can measure it. An alternative PV is body acceleration where motion sensors measure body movements [41]. Not all PVs are good seeds for key generation because their possible values are

not as variable as the HRV [62]. For example, blood glucose, blood pressure and temperature values are expected to be within a predefined small range. Some advantages of using PVs are:

1) Sensors do not need to generate random numbers reducing processing and power consumption;
2) Key security is improved; keys do not have to be distributed as all sensors for the same patient will be able to use the same PV to generate a shared encryption key.

Although PVs have several advantages there are several issues that must be solved before they are more widely accepted:

1) Some PVs can be remotely measured [3, 14], giving unauthorized devices the possibility of generating the shared key;
2) BAN architectures with diverse sensors, measuring different PVs, cannot have a single shared key for all the devices;
3) Personal servers would need access to a given PV to be able to create a key shared with the sensors.

Channel characteristics: A different approach, less used, is to handle channel characteristics for key generation.

One of the used characteristics is the received signal strength indicator (RSSI), a wireless channel feature [4, 5, 56, 58, 70]. However, body movements can affect the strength of the signals produced by implanted sensors as the waves are diffracted and trapped along the skin surface. The environment and involuntary movements such as respiration and heartbeat also affect signal strength, setting the variance of the RSSI values [56, 70]. There is one important advantage, since devices measure RSSI by default, there is no need to use computational resources for key generation.

A different approach, the Body-Coupled Communication (BCC), uses the human body as the communication channel [7]. Some researchers state that BCC may prevent several attacks because attackers would need to be very close to their target to be able to communicate [34]. This approach however, does not consider how to protect communications between sensors or actuators and a personal server.

3.1.2 Key Distribution

More than half of the studied research projects choose an available key-distribution algorithm to deliver secret keys in BAN environments. The most used algorithms are Diffie-Hellman and Fuzzy Vaults (see Table 2) .

1) Diffie-Hellman: A quarter of the papers that address key distribution use Diffie-Hellman for key exchange [25, 30, 33, 35–37]. In particular, 5 of these 6 papers adapt the algorithm to use it with ECC to create a shared secret key using public information derived from the keys generated using an elliptic curve. To use Diffie-Hellman with ECC, two devices need to agree about the curve parameters. With these parameters, each device
   a. Calculates a random number that will work as the private key;
   b. Calculates a point in the curve. This point, multiplied by the private key, will be the public key. The shared key will be a device's private key multiplied by the other device's public key.
2) Fuzzy Vault: Around a fifth of the studied papers use this method for key distribution. In this scheme, a user A hides a secret key (K_a) using a set of values $Set_a = \{a_1, a_2, a_3...a_n\}$. A different user, B, has another set of values $Set_b = \{b_1, b_2, b_3...b_n\}$. User B can obtain the secret key K_a if enough values in Set_b correspond to the values in Set_a [29].

   In BANs, fuzzy vaults are used to distribute secret keys generated with PVs and channel characteristics. In particular, some proposals use PVs to create the fuzzy vault that protects a secret key [11, 40–42, 60, 61, 69]. In [70] and [58], the authors use channel characteristics to create the sets for the fuzzy vault. Additionally, in [27] an enhanced fuzzy vault scheme is used to achieve access control. Fuzzy vaults are adequate because they can handle small errors in the measurements of PVs and channel features; users need to provide some of the values, but not necessarily all of them.
3) Other algorithms: The remaining proposals use other key-distribution algorithms. Among them, Distribution centers, with one node in charge of delivering keys to other devices, is the most used protocol [6, 23, 33, 36, 45]. Some proprietary protocols are also used [52, 59].

   The Internet Security Association and Key Management Protocol (ISAKMP) is also used to implement key exchange procedures and create encrypted connections between two endpoints [39]. Although ISAKMP may be used as a security framework in BAN scenarios, a previous study (where personal servers, in a patient's home, forward medical data, measured by sensors, to a hospital), showed that implementing this protocol increases bandwidth and energy consumption [13].
4) Key Agreement: Some proposals [26, 61] use physiological values and channel features to run a predefined algorithm and generate a shared secret key. Keys are generated, they do not need to be distributed. Some solutions for key agreement also include notifying a patient when a key agreement procedure is occurring in the network; for example, generating a brief vibration [19].

3.2 Access Control

Access control must guarantee that only authorized entities; users, processes or devices; will have access to data collected, forwarded and stored by BAN devices. To guarantee access control, two requirements must be addressed: authentication and authorization.

3.2.1 Authentication

Authentication allows a BAN to establish the identity of a given component, stopping devices that do not belong to a BAN from gaining access to private data. Attackers may pose as a legitimate device, like a sensor or a personal server, to eavesdrop, steal, or send erroneous information, possibly affecting sensors and actuators functionality [12, 32, 38, 48].

Most of the studied proposals (around 83%) present authentication protocols. These protocols may work in conjunction with a key-agreement protocol or may work independently. For example, some authors propose using PVs, channel characteristics or devices' identifications to achieve authentication; if a particular sensor can measure a defined PV, that sensor must be implanted or have physical contact with a patient and should be authenticated as a component of a given BAN [11, 26, 40–44, 46, 50, 59–62, 64, 66, 67, 69].

However, new techniques for measuring a PV without physical contact with the user are emerging. In one example authors implemented two methods for retrieving HRV from videos of human faces [3]. Another example implemented a microwave Doppler for non-contact through-clothing measurement of chest wall movements to obtain heart and respiration rates [14]. Although currently these techniques are not widely used, they suggest that authentication based on proximity may not be enough in the future.

Proposals that use channel characteristics for authentication also assume proximity; only legitimate sensors would be attached to a user and could share the same communication channel in order to have similar RSSI values [5, 34, 55, 56, 58, 63, 70].

Other proposals use a device's identification number for authentication; during an installation phase the id number is registered as part of a group. Later, that device sends its identification and a BAN node, in charge of the authentication, checks if that ID belongs to the group [5, 6, 17, 19, 33, 35, 36, 45, 49, 52]. These approaches may not be enough because identifiers may be faked.

Ho [25] evaluates three authenticated key agreement protocols for Intra-BAN communication: out-of-ban public key exchange, where the devices send their public keys over a secured separate channel. A password to alter the shared key, so only entities with the password can access the key. A numerical display, where a hash is used to guarantee that the other party has the necessary key to obtain the same hash. The implementations of these protocols are found to be resistant against impersonation and man-in-the-middle attacks; additionally, the use of the password protocol is strong to offline dictionary attacks. The author claims that these protocols have been adopted into the IEEE standard on BAN [28].

Previous protocols do not explicitly consider movement. If a person can move, authentication and authorization may be more difficult as sensors and communications would need to switch from one access point to another. In this case the authentication protocol should be able to manage re-authentication to provide the same set of established services at the second access point [65].

3.2.2 Authorization

Authorization requirements restrict access to a patient's medical information according to predefined access rules. For instance, a hospital may have several BANs to monitor several patients storing all data in the same server. However, not all doctors and nurses should have access to information of all patients, only medical personal directly involved with a patient should have access to his or her information. A BAN must implement authorization mechanisms to present data only to authorized entities, like a patient's medical team. In addition, an authorized entity should have access exclusively to needed information; for example, doctors should have access to all the information about the patient, but a pharmacist should only have access to drug prescriptions. A role-based access control is, therefore, necessary in a BAN architecture with multiple users [32].

An approach suggests the creation of behavioral profiles based on access patterns to and from devices in a BAN. Only access requests that are consistent with the profiles are allowed. An authorization mechanism may perform mitigation strategies to control inconsistent requests including passive actions like generating alerts or active actions like jamming the signal to deny access to data [68]. An alternative approach builds behavioral profiles based on places and times. Users, including doctors and nurses, only are allowed to access information from particular locations, such as consulting rooms and hospitals, at specific hours [24].

A different approach uses access policies based on attributes. Every user is assigned a set of attributes (n) and a minimum threshold for authorization (d) is established. If a user has (d) out of (n) attributes, then he or she is authorized to access a piece of information from the BAN personal server [27, 49].

Finally, some proposals use additional devices to perform authentication tasks; an additional device may be used as a proxy for communications among sensors and personal servers, and it allows or denies access requests [66].

Regarding intra-BAN components and communications, one approach is to authenticate and authorize sensors and actuators using proximity. Only devices in close proximity or with physical contact to the human body are authorized to obtain information from sensors [44, 46].

We found that only a few of the studied proposals ad-

Table 2: Security requirements addressed by the studied projects. Encryption, Key Distribution and Authentication are the most studied requirements. (Conventions. Sum: Summary, ECC: Elliptic Curve Cryptography, PV: Physiological Values, CC: Channel Characteristics, Sec: Secret Keys)

Papers	Security Requirements													
	Confidentiality									Access Control		Integrity		Availability
	Encryption					Key Distribution								
	Sum	ECC	PV	CC	Sec	**Sum**	Fuzzy Vault	Diffie-Hellman	Other	Authentication	Authorization	Hash Functions	Session Management	DoS Attack Protection
[43]	●	-	●	-	-	-	-	-	-	●	-	●	-	-
[52]	●	●	-	-	-	●	-	-	●	●	-	-	●	-
[20]	●	-	-	-	●	-	-	-	-	-	-	-	-	-
[25]	●	●	-	-	-	●	-	●	-	●	-	-	-	-
[42]	●	-	●	-	-	●	●	-	-	●	-	-	-	-
[64]	●	-	●	-	-	-	-	-	-	●	-	●	-	-
[22]	-	-	-	-	-	-	-	-	-	●	-	-	●	-
[45]	●	●	-	-	-	●	-	-	●	●	-	-	-	-
[27]	-	-	-	-	-	●	●	-	-	-	●	●	●	-
[23]	-	-	-	-	-	●	-	-	●	-	-	●	-	-
[70]	●	-	-	●	-	●	●	-	-	●	-	●	●	-
[69]	●	-	●	-	-	●	●	-	-	●	-	●	-	-
[13]	-	-	-	-	-	●	-	-	●	●	-	-	-	-
[30]	●	●	-	-	-	●	-	●	-	●	-	-	●	-
[37]	●	●	-	-	-	●	-	●	-	-	-	-	-	-
[63]	●	-	-	●	-	-	-	-	-	●	-	-	-	-
[6]	●	-	-	-	●	●	-	-	●	●	-	-	●	-
[49]	●	-	-	-	●	-	-	-	-	●	●	-	-	-
[36]	●	●	-	-	-	●	-	●	●	●	●	-	-	-
[50]	●	-	●	-	-	-	-	-	-	●	-	-	-	-
[18]	●	-	-	-	●	-	-	-	-	-	-	-	-	-
[58]	●	-	-	●	-	●	-	-	●	●	-	-	-	-
[2]	-	-	-	-	-	-	-	-	-	-	-	-	-	●
[33]	●	●	-	-	-	●	-	●	●	●	-	●	-	-
[5]	●	-	-	●	-	-	-	-	-	●	-	●	●	-
[53]	-	-	-	-	-	-	-	-	-	-	-	-	-	●
[41]	●	-	●	-	-	●	●	-	-	●	-	-	-	-
[4]	●	-	-	●	-	-	-	-	-	-	-	-	-	-
[19]	●	-	-	-	●	●	-	-	●	●	-	-	-	-
[34]	●	-	-	●	●	-	-	-	-	●	-	●	●	-
[46]	●	-	●	-	-	-	-	-	-	●	●	-	-	-
[26]	●	-	●	-	-	●	-	-	●	●	-	-	-	-
[56]	●	-	-	●	-	-	-	-	-	●	-	-	-	-
[68]	-	-	-	-	-	-	-	-	-	●	●	-	●	-
[55]	-	-	-	-	-	-	-	-	-	●	-	-	-	-
[61]	●	-	●	-	-	●	●	-	-	●	-	-	●	-
[17]	●	-	-	-	-	-	-	-	-	●	-	-	-	-
[62]	●	-	●	-	-	-	-	-	-	●	-	●	●	-
[66]	●	-	●	-	-	-	-	-	-	●	●	-	●	-
[60]	●	-	●	-	-	●	●	-	-	●	-	-	●	-
[44]	●	-	●	-	-	-	-	-	-	●	●	-	-	●
[59]	●	-	●	-	-	●	-	-	●	●	-	-	-	-
[11]	●	-	●	-	-	●	●	-	-	●	-	●	-	-
[35]	●	-	-	-	●	●	-	●	-	●	-	●	-	-
[40]	●	-	●	-	-	●	●	-	-	●	-	-	-	-
[67]	●	-	●	-	-	-	-	-	-	●	-	-	-	-
[24]	-	-	-	-	-	-	-	-	-	●	●	-	-	●
Total	38	7	17	7	7	24	9	6	11	39	8	12	13	4

dress authorization requirements (see Tables 1 and 2). However, as previously mentioned, not every agent in a BAN should have access to all data.

3.3 Integrity

Attackers may use several methods to modify a packet; they may capture and edit a packet, and then forward it to a server, or create radio interference to alter bits before a packet reaches a destination [38]. Interference by natural reasons is also possible. There are various consequences; an actuator that receives modified commands will not act according to the actual situation, and an application that receives erroneous data will generate false alarms. In any case, a secure BAN architecture should guarantee that data have not been modified during transmission or storage [12, 32, 38, 48, 51].

In addition to unauthorized modifications detection, a BAN also needs to avoid Replay Attacks. In replay attacks adversaries resend/replay old packets trying to make servers believe those packets are valid, possibly generating false alarms or failing to generate warnings. To prevent replay attacks, personal and external servers should evaluate data freshness, a property that indicates if the received information is recent and arrives when expected [32, 38, 48, 51]. To support integrity and avoid replay attacks, the studied proposals use hash functions and session identifiers.

Hash functions. Hash functions are used to verify integrity of a message or stored data by calculating a fixed-size number for a data stream.

Around a quarter of the studied proposals (see Table 2) use hash values to protect messages with medical data. Almost half of these proposals use one of the following hash algorithms: SHA-1, SHA-256, MD5, cyclic redundancy check (CRC) and digests, while the other half use Message Authentication Codes (MAC) [5, 27, 33–35, 69].

A different approach is to use external resources to support integrity checks of stored data. One option is to delegate integrity evaluation, of information stored in external servers, to cloud computing services [23].

Session Management: Replay attacks can be prevented by using session identifiers, such as random numbers [17, 30, 60, 66, 70] and timestamps [6, 22, 27], or by attaching a device ID and a data counter to every message to keep track of arrived messages and avoid repeated ones [5]. It is worth mentioning that only using a device ID and a counter is a technique that may be vulnerable to some attacks, as these values can be guessed.

One of the studied proposals [52] uses databases to store hash values of every received message. If the hash value of an arriving message already is in the database then the message is discarded. Alternatively, in [68], a sequence number is added to every message to track repeated or missing packets in a communication session. Channel characteristics may also be evaluated to find anomalies. If an anomaly is detected, then suspicious packets are jammed.

3.4 Availability

This security requirement, in a BAN, aims to guarantee that data and devices are available whenever they are needed. Physiological and medical information must be available when needed and during emergencies for doctors, nurses and paramedics [31, 32, 47, 48]. Each and every component must be available; if a network does not have enough capacity to transfer all packets, then servers cannot receive data on time [38, 47]. If other components, like sensors or servers, are compromised then information cannot be generated or received and warnings cannot be generated.

This requirement is the least studied; only a few of the considered works use protocols to avoid attacks on availability, like Denial-of-Service (DoS) attacks. Two methods were proposed to detect and mitigate these attacks. In the first one, Adaptive Network Profiles, authors create profiles of normal behavior based on different network characteristics like QoS (Quality of Service), traffic patterns and power consumption [2, 53]. To detect abnormal behavior, the network is constantly monitored, if an atypical behavior is detected, such as a decrease on QoS or increase in energy consumption, then corrective actions are performed.

The second method works by controlling high energy consumption tasks [24, 44]. DoS attacks tend to rapidly drain sensor's resources; data transmission tasks are particularly expensive in energy consumption [44]. To avoid DoS attacks that send high amounts of data, authors created procedures based on proximity; sensors will share information only with devices that are close to the human body. Data transmission only occurs in specific scenarios at controlled environments, thus reducing energy consumption.

While the first approach is designed to protect components and communications in the beyond part of a BAN, the second one is designed to protect the intra-BAN part. Both approaches should be managed within a single framework to guarantee consistency and protect a BAN as a whole.

Authentication procedures also consume more power than other tasks. To avoid battery draining in this case, an approach suggests using profiles; devices only accept communication from predefined devices at specific locations and times [24].

3.5 Software correctness

Sensors and implantable medical devices are controlled by software, and there is always a probability of having software bugs [47]. The Medical Device Recall Report, written by the US Food and Drug Administration (FDA) [16],

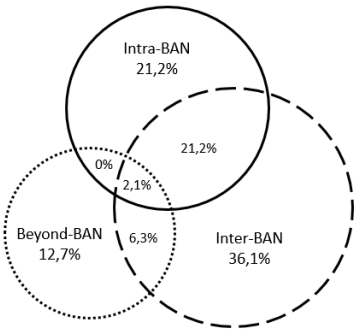

Figure 2: Distribution of works according to addressed BAN communications (Intra-BAN, Inter-BAN and Beyond-BAN communications)

Table 3: Works that secure specific BAN components; Most of the available works focus on sensors and personal servers

Secured BAN Component	***# of Works***	***%***
Sensors	13	27.65%
Sensors and Personal Server	25	53.19%
Personal Server	0	0%
Personal and External Server	4	8.51%
External Server	1	2.12%
External Server and Cloud	1	2.12%
Cloud	2	4.25%
Sensors, Personal and External Server	1	2.12%
Total	47	

states that software design flaws due to lack of proper testing procedures caused the recall of 429 devices. Software design flaws is the main reason to recall devices.

Furthermore, the entire lifecycle of these programs should be managed, not only their design and testing phases. Firmware and software updates must have adequate procedures to prevent the deployment of external firmware or software that may harm or allow unauthorized access to sensors and medical devices [21]. However, we found that none of the studied references consider this aspect.

4 Architecture Analysis

As already mentioned, we classified the studied proposals according to the BAN components they consider and the communications they protect. Table 3 classifies the works based on protected components, while Figure 2 classifies them based on protected communications. Around half of the studied proposals protect two BAN components: sensors and personal servers and their communications.

The interest in Intra-BAN and Inter-BAN communications may be explained because the devices that perform these communications (sensors and actuators) have processing and storage restrictions that have been addressed but are not completely solved. Additionally, these devices use recent technology, presenting new security issues that need to be considered.

In some BAN implementations, sensors may communicate among themselves, not only with the personal server. Around a fifth of the proposals (21.2%) address security of this kind of communications (Intra-BAN communication).

None of the proposals exclusively addressed security of personal servers. This situation may be explained as personal servers are not used for information-gathering or storage tasks, but as gateways between sensors and external servers. However, communications need to be secured and Figure 2 shows that half of the proposals (53.1%) secure communications that involve personal servers.

Few proposals address external servers. This is expected as personal servers usually have good processing and storage capacity. Consequently, traditional security solutions could be used. However, a comprehensive BAN solution must be able to integrate traditional solutions and solutions for devices with restricted resources like sensors and actuators.

We also examined if the proposals considered single or multi-user environments. The proposals that secure a single BAN, one that only involves one patient, are considered as single-user environments. 83% of the authors consider this configuration. On the other hand, a multi-user environment involves multiple patients, their sensors and personal servers send information to a centralized server, typically, a hospital's server. Only 17% of the proposals considered this scenario.

Multi-user BAN environments are relevant because they correspond to real health-care scenarios, like hospitals. Some security issues that have not been explicitly considered emerge in these environments; for instance, a server will need to manage key-generation and key-distribution for different patients.

5 Open Issues

Cloud Computing as a BAN Component: Considering that BANs handle medical information and there are privacy protection standards like The Health Insurance Portability and Accountability Act (HIPAA), BANs must support the requirements standards and legislation have defined. Due to these requirements, the use of cloud computing might be controversial in health related services, as protection and storage of medical information partially depends upon third-party infrastructures and policies.

Currently, cloud computing solutions are not commonly included as part of BANs but are starting to appear. A few of the studied projects considered cloud computing to support medical studies. The focus of these projects is protecting the communication channel between external and cloud servers, and protecting the information stored in the cloud.

Table 4: Percentage of proposals that consider single-user and multi-user environments.

Environment	*# of Works*	*Percentage*
Single-user	39	82.9%
Multi-user	8	17.1%

The proposals presented in [23] and [36] use cloud as a supporting tool to check integrity of a patient's medical information. Other authors secure the communication channel between a BAN and the cloud; for example, in [20] the authors propose a Multi-valued and Ambiguous Scheme to create a cryptographic system, based on secret keys, in order to perform this task.

One proposal addresses the need to support authorization in the cloud; different users should have access to different data according to their particular roles [57]. However, we need more works that study how to support authorization and authentication to grant access to medical records stored in the cloud.

Sensors are the focus of the majority of proposals: As Table 3 shows, most of the projects address security of sensors and personal servers, these are the main topic because the addition of software to control sensors and their role as part of BANs is relatively new. On the other hand, how to comprehensively secure external servers and cloud services that belong to a BAN and store medical data is not a well explored subject.

Multi-user Environment: Most of the studied works protect a single BAN architecture for one patient. They do not consider multi-user BANs, like in the case of a hospital that collects and stores medical information from several patients and must provide different types of access for different physicians and nurses. A few of the authors deal with multi-user environments, and only a small part of these (17.1%, see Table 4) use and try to secure cloud resources [20, 23, 36, 65].

Authorization: Few works consider this subject. One work proposes implementing role-based authorization for personal servers [27], while another one proposes using profiles, based on information like proximity, to allow access to sensor data [44].

Software Correctness: None of the studied works proposes mechanisms to check software correctness. As previously mentioned, according to the US Food and Drug Administration (FDA), software is the main cause for medical devices recalling [16]. This situation happens due to poor procedures to handle software design, update and testing. Therefore, it seems necessary to build methodologies and frameworks to support the development of correct and secure software.

Comprehensive Approach: Most of the analyzed proposals address security of one or two BAN components, they however do not consider the remaining components. None of the studied works addresses the entire environment in a comprehensive way, considering features and requirements across all the components. This view is needed as the security requirements of the collected data do not change depending on the component holding them.

6 Conclusions

In this paper, we made a bibliographic review of security requirements and proposals for BAN architectures. We identified the usual security requirements: Confidentiality, integrity and availability, as well as others like authentication, authorization, data freshness and software correctness.

There are various proposals that address these requirements. We classified them according to the BAN components they protect: sensors, actuators, personal servers, external servers and cloud services; and according to the communications they protect: intra-BAN, inter-BAN and Beyond-BAN. We found that most of the studied proposals only consider one or two BAN components.

We found that approximately 80% of the studied proposals exclusively focus on securing sensors and/or personal servers. The remaining proposals, around 20%, secure external servers and cloud services. Only one proposal considered all components. We argue that a comprehensive view is needed for several reasons. First, the security requirements of medical related data do not change according to the part of the BAN that is holding them. Second, deployed solutions must consider the particular aspects of Intra-BAN, Inter-BAN and Beyond-BAN contexts and communications, but they must be consistent; for example, if a sensor (intra-BAN component) needs to communicate with a personal server (Inter-BAN component), they must establish a protected communication channel. Similarly, a personal server must protect its communications with external servers. Third, a BAN must handle the life cycle of all the algorithms its components run. Finally, when considering a multi-user environment, a BAN external server will need to support security guarantees for several patients.

Acknowledgments

This work was partially supported by the Colombian Administrative Department of Science, Technology, and Innovation (Colciencias).

References

[1] CEN/TC 251, "Business Plan 2015-2018. Health Informatics," 2015. (file:///C:/Users/user/Downloads/

N15-019_Business_Plan_2015-2018_final_clean_20150423.pdf)

[2] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *7th International Conference on Body Area Networks*, pp. 269–275, 2012.

[3] K. Alghoul, S. Alharthi, H. A. Osman, and A. E. Saddik, "Heart rate variability extraction from videos signals: ICA vs. EVM Comparison," *IEEE Access*, vol. 5, pp. 4711–4719, 2017.

[4] S. T. Ali, V. Sivaraman, and D. Ostry, "Zero reconciliation secret key generation for body-worn health monitoring devices," in *Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC'12)*, pp. 39–50, 2012.

[5] S. T. Ali, V. Sivaraman, D. Ostry, and S. Jha, "Securing data provenance in body area networks using lightweight wireless link fingerprints," in *3rd International Workshop on Trustworthy Embedded Devices (TrustED'13)*, pp. 65–72, 2013.

[6] H. Alyami, J. L. Feng, A. Hilal, and O. Basir, "On-demand key distribution for body area networks for emergency case," in *12th ACM International Symposium on Mobility Management and Wireless Access (MobiWac'14)*, pp. 55–58, 2014.

[7] H. Baldus, S. Corroy, A. Fazzi, K. Klabunde, and T. Schenk, "Human-centric connectivity enabled by body-coupled communications," *IEEE Communications Magazine*, vol. 47, pp. 172–178, June 2009.

[8] D. M. Barakah and M. Ammad-uddin, "A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture," in *Third International Conference on Intelligent Systems Modelling and Simulation*, pp. 214–219, Feb. 2012.

[9] E. B. Barker, A. L. Roginsky, "Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths," *National Intitute of Standards and Technology (NIST'15)*, Nov. 2015.

[10] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: A survey," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 171–193, 2011.

[11] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *International Conference on Parallel Processing Workshops*, pp. 432–439, Oct. 2003.

[12] J. Chukwunonyerem, A. M. Aibinu, and E. N. Onwuka, "Review on security of wireless body area sensor network," in *11th International Conference on Electronics, Computer and Computation (ICECCO'14)*, pp. 1–10, Sep. 2014.

[13] R. Divya, T. V. P. Sundararajan, and K. Deepak, "Effect of wormhole attack in hierarchical body area network and need for strict security measures," in *6th International Conference on Computing, Communication and Networking Technologies (ICCCNT'15)*, pp. 1–7, July 2015.

[14] A. D. Droitcour, *Non-Contact Measurement of heart and Respiration Rates with a Single-chip Microwave Doppler Radar*, PhD thesis, Stanford University, 2006.

[15] European Patients' Forum, "The new EU Regulation on the protection of personal data: What does it mean for patients?," (http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf)

[16] A. Ferriter, *Medical Device Recall Report FY 2003 to FY 2012*, US Food and Drug Administration, Technical Report, 2012.

[17] S. Gollakota, H. Hassanieh, B. Ransford, and K. Katabi, D.and Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Computer Communication Review*, vol. 41, pp. 2–13, Aug. 2011.

[18] R. M. Gomathi, A. S. Sangari, J. M. L. Manickam, "RC6 based security in wireless body area network," *Journal of Theoretical and Applied Information Technology*, vol. 74, no. 1, Apr. 2015.

[19] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy (SP'08)*, pp. 129–142, May 2008.

[20] N. D. Han, L. Han, D. M. Tuan, H. Peter In, and M. Jo, "A scheme for data confidentiality in cloud-assisted wireless body area networks," *Information Sciences*, vol. 284, pp. 157 – 166, 2014.

[21] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song, "Take two software updates and see me in the morning: The case for software security evaluations of medical devices," in *2nd USENIX Conference on Health Security and Privacy (HealthSec'11)*, pp. 6, 2011.

[22] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area nNetworks with provable security," *IEEE Systems Journal*, vol. 11, pp. 2590–2601, Dec. 2017.

[23] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Systems Journal*, vol. 12, no. 1, pp. 64–73, 2018.

[24] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *IEEE Global Telecommunications Conference (GLOBECOM'10)*, pp. 1–5, Dec. 2010.

[25] J. M. Ho, "A versatile suite of strong authenticated key agreement protocols for body area networks," in *8th International Wireless Communications and Mobile Computing Conference (IWCMC'12)*, pp. 683–688, Aug. 2012.

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

[27] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 37–46, Sep. 2013.

[28] IEEE, "IEEE standard for local and metropolitan area networks," *Wireless Body Area Networks*, Feb. 2012.

[29] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[30] S. L. Keoh, "Efficient group key management and authentication for body sensor networks," in *IEEE International Conference on Communications (ICC)*, pp. 1–6, June 2011.

[31] M. Kumar, "Security issues and privacy concerns in the implementation of wireless body area network," in *International Conference on Information Technology*, pp. 58–62, Dec. 2014.

[32] P. Kumar and H. J. Lee, "Review security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, Dec. 2011.

[33] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," in *The International Conference on Information Networking (ICOIN'14)*, pp. 453–457, Feb. 2014.

[34] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *IEEE 13th International Conference on e-Health Networking, Applications and Services*, pp. 150–156, June 2011.

[35] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure Ad Hoc trust initialization and key management in wireless body area networks," *ACM Transactions on Sensor Networks*, vol. 9, pp. 18:1–18:35, Apr. 2013.

[36] S. Li, Z. Hong, and C. Jie, "Public auditing scheme for cloud-based wireless body area network," in *IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC)*, pp. 375–381, Dec. 2016.

[37] J. Liu and K. S. Kwak, "Hybrid security mechanisms for wireless body area networks," in *Second International Conference on Ubiquitous and Future Networks (ICUFN'10)*, pp. 98–103, June 2010.

[38] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "A survey on wireless body area network: Security technology and its design methodology issue," in *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS'15)*, pp. 1–5, Mar. 2015.

[39] D. Maughan, M. Schertler, M. Schneider, and J. Turner, *Internet Security Association and Key Management Protocol*, RFC 2408 (Proposed Standard), Nov. 1998.

[40] F. Miao, L. Jiang, Y. Li, and Y. T. Zhang, "Biometrics based novel key distribution solution for body sensor networks," in *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2458–2461, Sep. 2009.

[41] D. Oberoi, W. Y. Sou, Y. Y. Lui, R. Fisher, L. Dinca, and G. P. Hancke, "Wearable security: Key derivation for body area sensor networks based on host movement," in *IEEE 25th International Symposium on Industrial Electronics (ISIE'16)*, pp. 1116–1121, June 2016.

[42] R. T. Rajasekaran, V. Manjula, V. Kishore, T. M. Sridhar, and C. Jayakumar, "An efficient and secure key agreement scheme using physiological signals in body area networks," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI'12)*, pp. 1143–1147, 2012.

[43] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in wireless body area network (WBAN)," in *15th International Conference on Advanced Communications Technology (ICACT'13)*, pp. 998–1001, Jan. 2013.

[44] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *16th ACM Conference on Computer and Communications Security (CCS'09)*, pp. 410–419, 2009.

[45] C. Rong and H. Cheng, "Authenticated health monitoring scheme for wireless body sensor networks," in *7th International Conference on Body Area Networks (BodyNets'12)*, pp. 31–35, 2012.

[46] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *ACM SIGSAC Conference on Computer and Communications Security (CCS'13)*, pp. 1099–1112, 2013.

[47] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *IEEE Symposium on Security and Privacy*, pp. 524–539, May 2014.

[48] S. Saleem, S. Ullah, and K. S. Kwak, "Towards security issues and solutions in wireless body area networks," in *6th International Conference on Networked Computing (INC'10)*, pp. 1–4, May 2010.

[49] A. S. Sangari and J. M. Leo, "Polynomial based light weight security in wireless body area network," in *IEEE 9th International Conference on Intelligent Systems and Control (ISCO'15)*, pp. 1–5, Jan. 2015.

[50] A. S. Sangari and J. M. L. Manickam, "Public key cryptosystem based security in wireless body area network," in *International Conference on Circuits, Power and Computing Technologies (ICCPCT'14)*, pp. 1609–1612, Mar. 2014.

[51] S. Sangari and M. Manickam, "Security and privacy in wireless body area network," *Indian Streams Research Journal*, vol. 4, no. 8, 2014.

[52] M. Sarvabhatla, M. C. M. Reddy, and C. S. Vorugunti, "A robust biometric-based authentication scheme for wireless body area network using elliptic curve cryptosystem," in *Third International Symposium on Women in Computing and Informatics (WCI'15)*, pp. 582–587, 2015.

[53] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-Health IoT applications," in *7th International Conference on Body Area Networks (BodyNets'12)*, pp. 276–281, 2012.

[54] P. G. Shah, X. Huang, and D. Sharma, "Analytical study of implementation issues of elliptical curve cryptography for wireless sensor networks," in *IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*, pp. 589–592, Apr. 2010.

[55] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," in *Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC'12)*, pp. 27–38, 2012.

[56] L. Shi, J. Yuan, S. Yu, and M. Li, "ASK-BAN: Authenticated secret key extraction utilizing channel characteristics for body area networks," in *Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC'13)*, pp. 155–166, 2013.

[57] Y. Tian, Y. Peng, G. Gao, and X. Peng, "Role-based access control for body area networks using attribute-based encryption in cloud storage," *International Journal of Network Security*, vol. 19, 2017.

[58] G. R. Tsouri and J. Wilczewski, "Reliable symmetric key generation for body area networks using wireless physical layer security in the presence of an On-body eavesdropper," in *4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL'11)*, pp. 153:1–153:6, 2011.

[59] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Ekg-based key agreement in body sensor networks," in *IEEE INFOCOM Workshops*, pp. 1–6, Apr. 2008.

[60] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *IEEE Military Communications Conference (MILCOM'08)*, pp. 1–7, Nov. 2008.

[61] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, pp. 60–68, Jan. 2010.

[62] K. K. Venkatasubramanian and S. K. S. Gupta, "Physiological value-based efficient usable security solutions for body sensor networks," *ACM Translations on Sensor Network*, vol. 6, pp. 31:1–36, 2010.

[63] S. Venkatasubramanian and V. Jothi, "Integrated authentication and security check with CDMA modulation technique in physical layer of wireless body area network," in *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1–6, Dec. 2012.

[64] H. Wang, H. Fang, L. Xing, and M. Chen, "An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN)," in *IEEE International Conference on Communications (ICC'11)*, pp. 1–5, June 2011.

[65] Q. Q. Xie, S. R. Jiang, L. M. Wang, and C. C. Chang, "Composable secure roaming authentication protocol for cloud-assisted body sensor networks," *International Journal of Network Security*, vol. 18, pp. 816–831, Sep. 2016.

[66] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *IEEE INFOCOM*, pp. 1862–1870, Apr. 2011.

[67] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A fast key generation method based on dynamic biometrics to secure wireless body sensor networks for p-health," in *Annual International Conference of the IEEE Engineering in Medicine and Biology*, pp. 2034–2036, Aug. 2010.

[68] M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 7, pp. 871–881, Dec. 2013.

[69] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "Ecg-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, pp. 1070–1078, 2012.

[70] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "Channel information based cryptography and authentication in wireless body area networks," in *8th International Conference on Body Area Networks (BodyNets'13)*,, pp. 132–135, 2013.

Biography

Laura Victoria Morales is a doctoral student at Universidad de los Andes. Bogotá, Colombia. She holds an M.S. degree on Information Security from Universidad de los Andes. Her research interests include security in IoT devices, Body Area Networks and computer forensics.

David Delgado-Ruiz is a Computing and Systems Engineering student at Universidad de los Andes. Bogotá, Colombia. His research interests include IoT security.

Sandra Julieta Rueda is an Assistant professor at Universidad de los Andes. Bogotá, Colombia. She holds an M.S. degree from Universidad de los Andes and a Ph.D. from The Pennsylvania State University, USA. Her research interests include systems security, access control and policy analysis.