Security Challenges for Healthcare Applications Regarding Body Area Network: A Comprehensive Survey

Arsalan Barolia
Biomedical Engineering Masters Student
Department of Engineering, Ryerson University
Toronto, Canada
arsalan.barolia@ryerson.ca

***Abstract*—Body area network (BAN) are commonly used in healthcare environments such as hospitals, surgical centers, clinics, etc. to aid in the monitoring for chronic diseases like asthma and heart attacks. BAN enables sensors and actuators to connect to the human body and collect the patients' readings which can then be viewed by the physician. Wireless body area network (WBAN) offers more flexibility in terms of transferring the patient's recordings as it uses a greater range of communication methods that BAN is not capable of. Like any biomedical instrumentation, BAN is essential for healthcare monitoring, healthcare systems, sport medics, and multimedia communication. However, since these networks are small and they utilize sensors and actuators, high levels of energy are consumed to ensure that no data loss occurs during the transmitting of information. In this comprehensive survey, the methodological approaches of BAN regarding the safety, reliability, effectiveness of transmitting data, and security will be thoroughly discussed.**

Keywords—Body area network (BAN), security limitations, healthcare monitoring, key distribution, public key distribution, symmetric key distribution.

I. INTRODUCTION

The wireless sensor network (WSN) is comprised of sensor nodes that detect acoustic changes/factors in an individual's body like temperature, pressure, sound, pulse rate, ECG, blood pressure, and heart rate in real-time. The WSN in healthcare is referred to as wireless body area network (WBAN). It should be noted that since BAN and WBAN follow the same goal and were built of each other, these terms will be used interchangeably in this survey paper as common challenges and security issues apply to both networks.

BAN devices connect a wearable device, on a human body, to the internet through gateway devices. These devices are very flexible in terms of how they can be embedded and their applications for an individual. For instance, common BAN devices can be embedded in one's body, like implants, surface mounted at a fixed location on the body, and/or simply a wearable device like watches or gloves. Surface mounted BAN devices are extremely beneficial for patients with conditions that are hard to detect due to internal factors. A prime example of this would be a patient who is diabetic. A surface mount BAN device, mainly a pump, would be attached to the patient allowing insulin to be auto injected into the patient's blood stream when a decline in insulin level is detected [1].

To be specific, sensor nodes can communicate with the BAN device in two possible ways [2]. The first is by enabling sensors to communicate with Personal Device Assistants (PDA) like Bluetooth or Zigbee. Although Bluetooth is common to most, Zigbee is also very beneficial for BAN technologies that rely on secure

networking and long-lasting battery life. It was developed to express low-cost and low-power wireless Internet of Things (IoT) networks. In simple words, IoT networks can transfer data over a network without human-to-human or human-to-computer interaction [3]. The second way for sensor nodes to communicate with BAN devices is through the usage of radio interface signals connecting PDAs to the base station. Nowadays, with the advancement of more reliable and secure networks, these two methods have been merged to allow sharing of collected information via internet. In Figure 1, the BAN architecture can be seen where the wearable device on the human is monitoring EEG, ECG, temperature, respiration, blood oxygen levels, blood pressure, and heart rate. These recordings are then transferred to a PDA device via Bluetooth, or other means, that is later sent to base station. Depending on the respective user application, the base station can transfer the data to ambulances, doctors, care takers/family members, or cloud databases via the internet [2, 4].

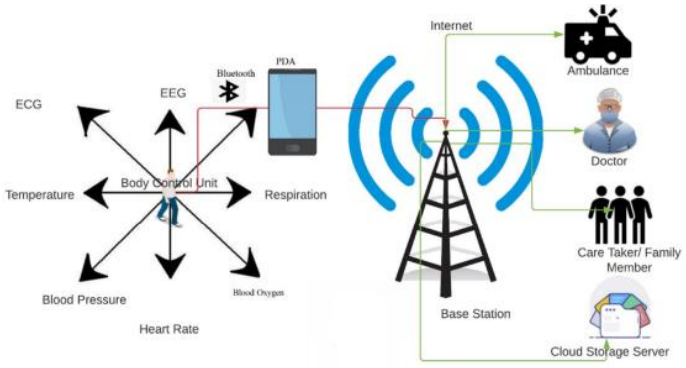

Figure 1: Body area network architecture

More specifically, each node/electrode that is connected to the human body sends a signal to a relay node that sends all those messages to the base station. The base station then transfers the collected data to the internet which can then be viewed by a doctor or caregiver. For example, a caregiver puts 5 sensor nodes (SN1–SN5) around the patient's chest to observe his/her heart rate. The sensor nodes detect the movement and sends the data they collected to the relay node. The relay node collects the data from all 5 sensors and transfers the data to the base station. The base station allows the caregiver to view the collected data via the internet. Figure 2 helps visualize the example mentioned.

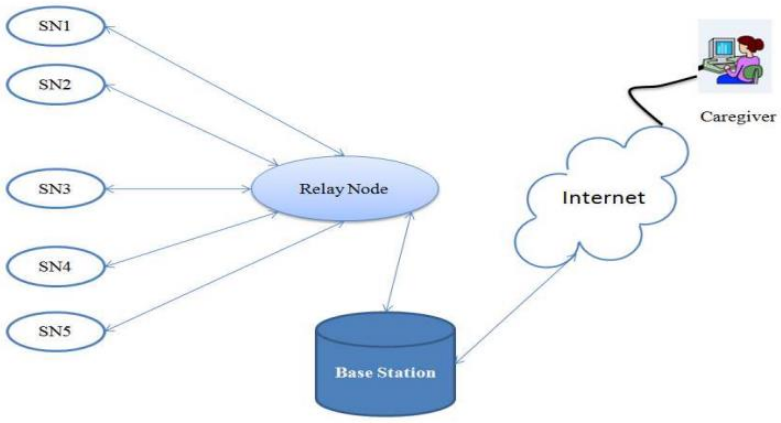

Figure 2: Using sensor nodes and relay nodes to collect information for the caregiver to interpret

In 1995, WBAN technology was becoming more discovered trying to recreate the idea of using wireless personal area network (WPAN) [5]. This type of network is commonly used when connecting one's personal device to the internet and transferring data between the user's connected devices. For instance, a computer can wirelessly send a message to the printer indicating the document it needs to print via the WPAN network. In Figure 3, a visualization of this example is shown along with the other various networks that are used in today's world.

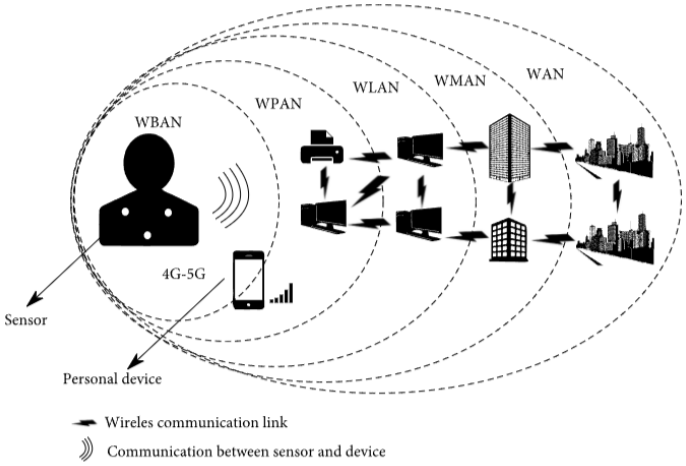

Figure 3: WPAN networks in comparison to other networks.

From Figure 3, it can also be noted that at the time when BAN was not discovered, WPAN was the most personalized network to exist. However, when BAN technology was developed, it became the most personalized network system, compared to the others, as it was physically dealing with data that was collected, on a human being, and transmitted to the device. Due to this more condensed and personalized network, security issues need to be addressed to ensure the system is safe, secure, and dependable. This will be discussed later in this survey paper.

BAN is a network that uses the integration of sensors, nodes, and actuators and is designed to function with a human body and its surroundings. A typical BAN kit consists of sensors, a processor, a transceiver, and power source. Since these BAN devices are being attached to a human body, it is crucial that the device exhibits the following elements [6]:

- Reliability
- Output low consumption
- Resilient to interference
- Operational at high ranges (Max: 5 m)

In the 90s, Massachusetts Institute of Technology tried connecting an electrical device to the human body for monitoring applications. Common monitoring applications we see WBAN devices used for are muscle activity, brain electrical activity, trunk position using a tilt sensor, respiration, heart activity, blood pressure, and estimate a user's activity with the help of movement sensors [7].

Like mentioned previously, since BAN is a more condensed and personalized network that connects a device to a human being, security threats and issues arise which will now be discussed in the next section.

II. SECURITY THREATS AND ISSUES

The purpose of network security is to protect the patient's data from threats during data transmission. There are two types of network attacks that can occur when breaching network security – active and passive attacks. Although both attacks steal patient data, the way it affects a system's operation differs. For instance, in a passive attack, the attack does not degrade the information resources but instead damages and modifies the data whereas the active attack's goal is to get a patient's data while also significantly impacting the operation of the system. [2].

When dealing with any security threats and system vulnerabilities confidentiality, authorization, authentication, integrity, availability of the network, and non-repudiation should be addressed. Since BANs are used for health applications and monitoring devices, the nodes that collect and record an individual's data must be protected from imposters and unwanted sources. These aspects of security will be discussed in detail and summarized, in Table 1, regarding the existing security methods used today.

A. Confidentiality

Confidentiality is a key aspect that must be always protected. This helps prevent the attacker from seeing the patient's personal health information and thus, the sensors that are collecting the data on the patient should have some form of encryption algorithm when sending data within a BAN instead of plain text. There are numerous encryption methods that have been developed to consume low energy such as DES, 3DES, AES, Blowfish, SIT, RSA, DSA, ECC, Diffie-Hellman key Exchange, etc. A study shows that the Blowfish Feistel algorithm is the best algorithm for securing data as it used 4-large S-tables, requiring embedded RAM, key length ranging from 32-488 bits, and a recursive key length schedule that enables this algorithm to be fast, compact, simple, and secure with the help of key expansion and data encryption [8].

B. Authorization

After the data has been transmitted to the base station and forwarded to the healthcare professional, it is important to verify that the professional is authorized to analyze the patients' readings and that the data is only available to people that are allowed to view it. Having an authorization mechanism that grants access once the identity is confirmed prevents intruders from accessing the data and creates additional constraints to secure and protect the patient's health and personal information.

C. Authentication

When an individual uses the monitoring device or BAN-reliant application, entity authentication and data authentication must be discussed. It is important for BANs to ensure that the person who he/she claims to be is indeed them. In addition, data authentication helps verify that the data that is being transmitted is being sent to the right sender and not an intruder. This is achieved using public key cryptography (PKC) whose integrity is verified by a Certificate Authority (CA).

D. Integrity

Since we are dealing with an individual's health and well-being, it is important to verify that the data being transmitted from the device to the health professional has not been altered, modified, deleted, or replaced in any manner by an intruder. Modified readings can cause for inaccurate readings and result in life threatening consequences for the patient. Any altercation to readings and records should be immediately detected using

communication entities [9]. The readings are verified using the message integrity code (MIC) and PKC. However, the authentication of PKC requires out-of-band channels to verify the public keys.

E. Availability of the Network

Since BANs are primarily used for healthcare applications and often carry sensitive and personal information of a patient, it is essential that the network is constantly available regardless of where the practitioner is located [10]. Due to this, secure wireless transfers are required to prevent intruders from eavesdropping and stealing privileged information.

F. Non-repudiation

Non-repudiation determines that every data being transmitted has been received, and vice versa, in BANs. This means that every interaction and data being sent and received is monitored ultimately tracking the attacker if any non-repudiation evidence is found. This is enforced using digital signature and digital certificates for all transmission process in healthcare – including BANs.

III. EXISTING SECURITY METHODS USED FOR COMMUNICATION PROTOCOLS

Security and privacy protocols that are used for communication security issues can be used and applied to BAN networks as well. The four common communication protocols that are currently in place for BANs are Bluetooth, ultra-wideband (UWB), Zigbee, and Task Group 6 (TG6) [9].

A. Bluetooth [IEEE 802.15.1]

When discussing security related to networks, it is important to have a strong foundational understanding of the Open Systems Interconnection Model) OSI Model. The OSI model helps visualize and describe the functions of each category in a networking system. It helps gain a better insight of the universal rules and computing functions in play. Figure 4 illustrates the 7 sections in the OSI model along with a brief explanation of its purpose.

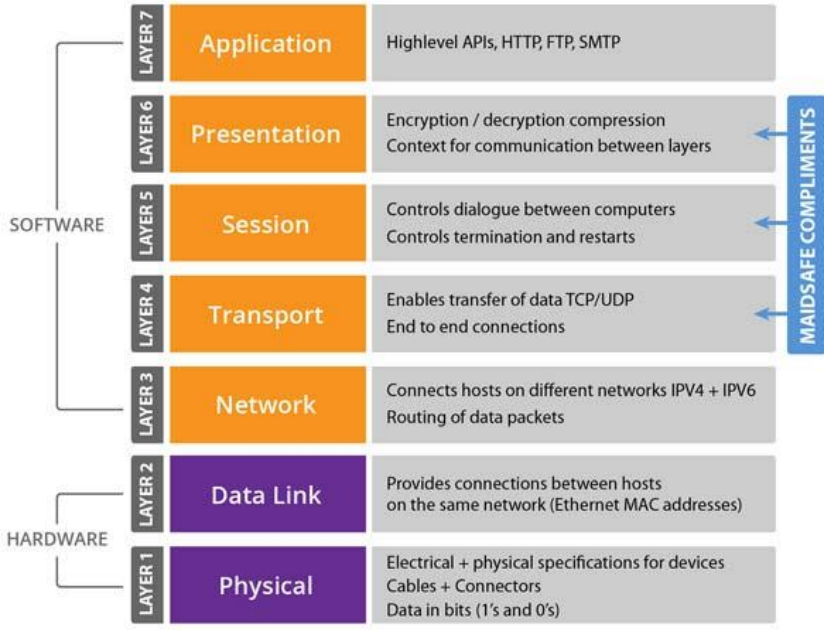

Figure 4: The 7 layers that make up the OSI Model

As seen in Figure 4, the first two layers deal with hardware and the other 5 layers are implemented using software. In Bluetooth, there are four different entities that are used to enforce and maintain security [9, 11]. This occurs in the data link, Layer 2. The four entities in the data link related to security are as follows:

- A public address → Ensuring every user's address is unique to them.
- Two secret keys → Enforces confidentiality and integrity.
- Random number → A random number that is generated for every new transaction.

In the data link layer, the initialization key, when no combination of keys has been identified or exchanged, is used to protect the transfer of initialization parameters. This key derived one of 3 ways – a personal identification number (PIN) code, public address, or random number. Often we see a fixed PIN that is set to 0000 when pairing new devices together via Bluetooth. However, this PIN can be changed by the user and entered in units with the man-machine interface (MMI) [13]. This interface allows the user to interact with the control system of the device [14].

Using PIN code is not the most secure way of protecting BANs as it can be easily deciphered using brute force attacking or exhaustive iterations. In addition, using PIN codes become impractical when dealing with implantable devices and majority of biosensors, in BAN, as they do not have an MMI. Thus, Bluetooth becomes an undesirable option for BANs.

Some Bluetooth security protocols that are put in place are LMP and L2CAP – *Baseband, Link Manager Protocol* and *Logical Link Control and Adaptation*, respectively. With the help of baseband, data can be transferred in forms of packets where the LMP is responsible encryption, authentication, and the exchange of encryption keys. Furthermore, L2CAP aids in providing a higher quality of communication service but is often used for multi-level complex network designs [10].

B. Ultra-wideband, UWB [IEEE 802.15.3]

UWB was developed to help improve the security issues Bluetooth faced. UWB operates at high frequencies using radio waves. It was tested that the UWB technology outperforms Bluetooth in terms of accuracy, wireless connectivity, robustness, and security [15].

UWB is viable for communication systems that have either no security or strong cryptography. When a communication system has no security protocols, the system is unable to perform any operations regarding cryptography on the medium access control (MAC) frames. In other words, a device cannot have encryption and decryption capabilities if no security protocols are embedded into the system. On the other hand, if strong cryptography is implemented into a device that uses UWB, then symmetric key cryptography is used to protect frames using encryption and integrity [16]. It supports 128-bit advanced encryption standard (AES) security suite and key management. If an intruder is present during the communication, a beacon is put in place to record time stamps of messages to prevent playback communication. This beacon rejects playback communication if the if the time stamp/token on a previous message is less than the current time stamp/token [9, 15, 16].

Although UWB surpasses Bluetooth communication in terms of security, UWB is limited as it has no way to enforce authentication, authorization, and non-repudiation.

C. Zigbee [IEEE 802.15.4]

This security mechanism uses symmetric-key cryptography and was designed to address some security issues that were not addressed by Bluetooth and UWB such as data confidentiality, data authentication, and

replay detection. Despite Zigbee's eight level encryption algorithm, it still lacks key generation and key distribution which are both vital for symmetric-key cryptography. Hence, although the overall security performance provided by Zigbee is superior to Bluetooth and UWB, it is heavily dependent on ensuring that the distribution of keys is secure before beginning a communication session. If these keys are intercepted by an intruder, then no security is offered, and the patients' health and personal information is compromised [17]. Due to this, Zigbee's security method does not validate authorization, non-repudiation, and integrity control.

D. ***Task Group 6, TG6 [802.15.6]***

Even though Bluetooth, UWB, and Zigbee are the most common communication protocols used for BANs today, it was discussed that they do not encompass and enforce all the security policies. For this reason, TG6 was developed to help solve these issues however, it is currently being developed and tested. This communication protocol was designed to optimize low-power devices that operate on, in, and/or around the human body. Although this protocol was not specifically designed for human bodies, it helps with enforcing some security protocols that Bluetooth, UWB, and Zigbee do not [18]. TG6 uses the Diffie-Hellman key exchange method to generate and distribute keys, MIC to authenticate the message, and advanced encryption standard (AES) for ciphering. In Table 1, a summary of all the different communication methods – Bluetooth, UWB, and Zigbee, and its security protocols it enforces are shown below.

Table 1: Summarized communication methods and their security protocols [9]

Protocols	**Bluetooth**	**UWB**	**Zigbee**	**TG6**
Confidentiality	Yes	Yes	Yes	Yes
Authorization	No	No	No	No
Authentication	Yes	No	Yes	Yes
Non-repudiation	No	No	No	No
Integrity	No	Yes	No	Yes

A list of current and existing security threats along with possible solutions that are present with discussing BANs have been tabulated in Table 2.

Table 2: Security threats and actions for BAN [10]

Security threats	Security requirements	Possible security solutions
Unauthorized access	Key establishment and trust setup	Random key distribution and Public key cryptography
Message disclosure	Confidentiality and privacy	Link/network layer encryption and Access control
Message modification	Integrity and authenticity	Keyed secure hash function and Digital signature
Denial of Service (DOS)	Availability	Intrusion detection systems and redundancy
Compromised node	Resilience to node compromise	Inconsistency detection and node revocation and Tamper – proofing
Routing attacks	Secure routing	Secure routing protocols
Intrusions and malicious activities	Secure group management, Intrusion detection Systems and secure data aggregation	Secure group communication Intrusion detection systems

IV. SYMMETRIC AND PUBLIC KEY CRYPTOGRAPHY IN BANS

When dealing with BANs and WBANs, data encryption and security must be addressed. A device that is on, in, or around a patient and actively monitoring them means that sensitive and personal information needs to stay within the group that is authorized to view these readings and excludes the intruders. Many encryption methods have been developed and used based on the application. However, it was found that using public key and symmetric key cryptography (SKC) was most beneficial in BANs.

It was found that when public key cryptography (PKC) is paired with elliptic curve cryptography (ECC) in BAN, it yielded accurate results. This was due to the two cryptographic methods to have a small key-size, compact signature, and high computational capabilities [10]. However, like any security mechanism, it has its advantages and disadvantages.

A. Public Key Cryptography in BANs

PKC's ability to easily generate a public key from the private key using mathematical operations allows for the less demanding computational resources. Although the public key can be easily generated using the private key, the reverse computation is significantly harder. In other words, going from a public key to a private key is computationally complex. For this case, PKC's most advantageous features it has to offer is that it does not require a secured channel when distributing the initial keys [9]. In PKC, the public and private key play different roles. A person's public key is available to everyone where the private key is unique and only known by the owner. In PKC, the sender uses the recipients public key to encrypt a message and the recipients will use his/her private key to decipher the message. Figure 5 illustrates the encryption and decryption process in PKC.

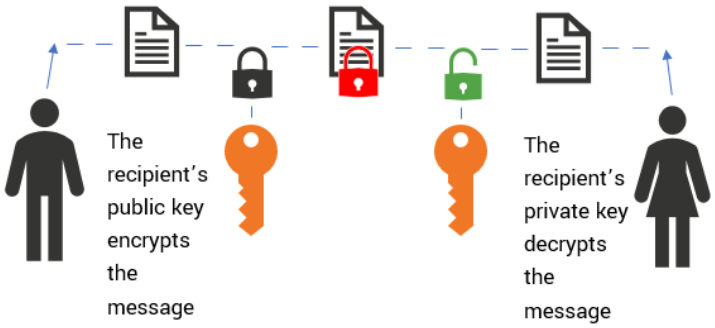

Figure 5: Encryption and Decryption in public key cryptography

RSA and ECC are common cryptosystems that are paired with PKC for network security. However, due to their nature of being computationally intense, power demanding, lengthy processing time, and large data size these were believed to be impractical in WSN. More research and optimizations were preformed to improve these cryptosystems so that they could be used in WSNs. The multiplication, reduction, and exponential calculations were optimized such that required less memory occupation, energy consumption, and processing time [9, 11, 12]. From these optimizations, RSA and ECC paired with PKC became feasible for WSNs like BANs and WBANs.

These optimizations were tested by implementing ECC and RSA using an Atmel ATmegal128 microprocessor. This microprocessor has a two-bit microcontroller operating at 8MHz that can do rapid and precise calculations without hardware calculation. After optimizing the algorithms Gura et al. saved memory, Malan et al. were able to generate public and private keys within 34.2 seconds and 0.23 seconds, respectively, and Wander et al. conserved energy by reducing the amount of data that was exchanged in the secure sockets layer (SSL) [19, 20, 21]. SSL operates from Layer 6, Presentation Layer, in the OSI Model – Figure 4.

Although these researchers, and many others have optimized algorithms and explored ways to reduce the speed for generating public and private keys along with signature/verification generation, the memory and energy consumption still demands a lot for biosensors. Moreover, RSA and ECC were found to be good when dealing with selected amounts of data, but when huge data sets are introduced, the encryption and decryption becomes slow making it dependent on the healthcare application.

B. *Symmetric Key Cryptography in BANs*

SKC is preferred when dealing with BANs as it demands less memory and computational resources. The reason for this is because PKC required 2 separate keys for encryption and decryption. The public key was used for encryption whereas the private key would be used for decryption. On the contrary, SKC uses the same key when encrypting and decrypting. Figure 6 depicts how a ciphered data is encrypted and decrypted using SKC.

Figure 6: Encryption and Decryption in symmetric key cryptography

In BANs, SKC is often used with Rivest Cipher 4 (RC4), Rivest Cipher 5 (RC5), AES, HIGHT, and KATAN. One of the main differences between RC4 and RC5 is that one uses stream cipher and the other uses block cipher, respectively. RC4 uses a stream of bits that are generated pseudo-randomly and combines it with the plain text. RC5 is more secure than RC4 but lacks in speed, simplicity, and efficiency. The AES encryption standard was developed to replaced DES, the previous encryption standard, because DES used a small cipher key which could be deciphered by a determined intruder. DES was first broken in 1997 for the first time and by 1998, DES could be broken in 56 hours. In 2021, DES is broken in 5 minutes which means that it is no longer a viable and proven to be an inadequate cryptographic method to implement [22]. A more in-dept comparison between AES and DES can be found in Table 3.

Table 3: Differences between AES and DES [9, 23]

	DES	**AES**
Date	1976	1999
Block Size	64	128
Key Length	56	128, 192, 256
Number of Rounds	16	10, 12, 14
Design	Open	Open
Design Rationale	Closed	Open
Viable	No	Yes

Biosensors are small sensors that cannot be equipped with the best computational hardware thus, minimalistic yet effective encryption and decryption methods should be considered. For this reason, RC5 cannot be used as it was not designed for sensor networks that need to do 8-bit sensor computation. After, HIGHT was a new algorithm that was proposed as it used a 64-bit block length with a 128-bit key. Having these block and key lengths are suitable in biosensors they are low-cost, low-power, and compatible with ultralight implementation. It was concluded that when HIGHT and RC5 ran at the same speed, HIGHT was superior in terms of being power efficient and consuming less memory [9]. Shortly after, a new algorithm was introduced called KATAN. This piece of hardware was known to be efficient using block ciphers of 3 block sizes of 32-, 64-, and 128-bit. The performance of KATAN surpassed RC4 and RC5 however, the security concerns still needed to be addressed. It was found that KATAN was prone to break if the meet-in-the-middle and/or key attack techniques were used [9, 24]. In Table 4, a summary of the different cryptographic algorithms discussed can be seen.

Table 4: Summary of the cryptographic algorithms tested on BANs [9]

Algorithms	Description
RC4	Stream cipher, simple
RC5	Block cipher, a variable block size (32, 64, or 128 bits), more secure than RC4.
AES	Block cipher, a 128-bit block size, the encryption standard adopted by the USA
HIGHT	Block cipher, block size (64 or 128 bits)
KATAN	Block cipher, block size (32, 48, or 64 bits)

It should be noted that hashing algorithms were used as well to test their effectiveness for BANs. Secure hashing algorithms (SHA) when used with other encryption methods was found to transmit data more securely and powerfully. However, since hashing generates digital signatures and used Asymmetric key generation, a public and private key, ultimately making the computation slower and more complex [25].

In conclusion, it was found that to use digital signature and securely transport the patients' data, symmetric keys would need to be used instead of asymmetric/public keys to reduce the amount of mathematical computation that is required.

V. KEY MANAGEMENT IN BANS

From the previous section, the advantages, and disadvantages that PKC and SKC have on one another were explored. It was found that although PKC used an asymmetric key generation method, a second secure channel was not needed to generate and distribute the keys. However, because of its highly computational demands, it consumes more memory, power, effects speed, and requires expensive hardware. When SKC was explored, it was found that PKC did not have this issue as it used symmetric keys and required less computational hardware. Moreover, since the two keys generated are the same, a secure channel must be established to share the keys without an invader or eavesdropper intercepting it. Thus, in this section the 3 types of key management for symmetric key cryptography will be explored.

A. *General and Biometric-Based Symmetric Key Generation*

This process uses random binary sequences (BSs) to encrypt data. The number of random numbers that can be generated are limited by the physical hardware of the system and can only be random to some degree. Thus, these random algorithm generators need to be further randomized into BSs but will take a toll on speed and increase complexity. For this reason, two methods used to generate random and pseudorandom sequences are by converting random source signals and by calculating mathematical algorithms like a linear congruential generator (LCG) [9, 26]. A study was done where Latif et al. were able to generate random sequences by using the discrete signal received from the sensors. The signal was converted using the digitally received signal strength indicator (RSSI). This method promotes low-costing operating hardware as no additional hardware is needed for this computation. The quality and frequency of the randomly generated bits are created based on the error of bits that are received. Since RSSI is taking the digital signal received from the sensor nodes, it is important to ensure that the nodes are cycling occasionally so that a pattern cannot be discovered. Different sensors will have different errors causing the random numbers to vary and not follow any specific pattern. It should be noted that this method is not suitable for BANs as the randomness of numbers cannot be determined and the position of nodes are usually at a fixed location [9, 26, 27].

B. *Symmtric Key Distribution*

Symmetric key distribution in BANs can be pre-distributed. The secrecy of this distribution method must be protected such that an intruder cannot view find it. For BAN related applications, a deterministic pairwise key pre-distribution scheme (DPKPS) was implemented on a sensor platform so that the energy, memory, and computational RAM can be measured. It was found that when using a MICAz sensor platform with the DPKPS, little energy, flash memory, and RAM were used at 17.23μ/Ah, 2KB, and 69 bytes, respectively [27]. This method becomes viable only if additional sensors are not added to the system. This is because since the keys must be pre-distributed and the sensors should have the keys in advance, adding additional biosensors becomes difficult to account for [9, 27]. This method partially becomes unsuitable for BAN because a patient's health is constantly changing, and additional sensors may need to be added. An encryption method needs to be both secure and adaptive to the situation. Using DPKPS although has benefits in terms of saving energy, memory, and RAM, it lacks the ability to be flexible and adapt if needed.

C. *Key Distribution via Bio-channels*

Bio-channels, in this case, refer to the linkage between the human body and BAN through nodes. In the human body, the cell membrane to be specific, bio-channels exist that allow ions to be exchanged using a voltage-gated channel. In BANs, bio-channels are the term used to enable the transfer of exogenous or endogenous information. This method of key distribution is still being tested but the theory proposed with this method is that a sensor will generate a symmetric key and use bio-channels to relay them to the other nodes/sensors. However, since this method is still in development and testing, it was discovered that more research needs to be done to develop a low-cost and reliable method of key distribution using bio-channels.

VI. CONCLUSION

In conclusion, although security algorithms and cryptographical methods have advanced, one method cannot protect against all attacks from security. It was discussed that security in BAN must address confidentiality, authorization, authentication, integrity, availability of the network, and non-repudiation. However, Table 1 displayed that even with the common communication methods we have today, such as Bluetooth, UWB, Zigbee, and TG6, these methods cannot protect one's information completely. Thus, handling an information as sensitive as a patient's health and incorporating these methods in BANs were undesirable. Next, the two main forms of key distributions were discussed where PKC and SKC were

compared. PKC was found to be more secure but, in turn, demanded more energy, memory, and RAM – as it uses asymmetric keys. The public and private needs to be mathematically computed which ultimately increases the computational time and complexity of security system. Biosensors are relatively small and are not suitable to handle large and complex computations that PKC requires. Although SKC is not as secure as PKC, it uses a symmetric key which reduces the computational stress on a biosensor. However, unlike PKC, SKC needs a second secure channel to enable the distribution of keys. SKC is preferable than PKC, yet the distribution of keys have not yet been perfected. A patient's information is very sensitive and must be always protected from the encryption to the transferring of data.

REFERENCES

[1] N. Security, "Body area network," *BAN*. [Online]. Available: https://www.networxsecurity.org/members-area/glossary/b/ban.html. [Accessed: 06-Dec-2021].

[2] J. Vijitha Ananthi and · P. Subha Hency Jose, "A perspective review of security ... - link.springer.com," *International Journal of Wireless Information Networks (2021)*. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s10776-021-00538-3.pdf. [Accessed: 06-Dec-2021].

[3] A. S. Gillis, "What is IOT (internet of things) and how does it work?" *IoT Agenda*, 13-Aug-2021. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#:~:text=The%20internet%20of%20things%2C%20or,human%2Dto%2Dcomputer%20interaction. [Accessed: 06-Dec-2021].

[4] M. Fotouhi, M. Bayat, A. K. Das, and H. A. N. Far, "A lightweight and secure Two-factor authentication scheme ...," *A lightweight and secure two-factor authentication scheme for wireless body area networks in healthcare IoT*. [Online]. Available: https://www.researchgate.net/publication/341634618_A_lightweight_and_secure_two-factor_authentication_scheme_for_wireless_body_area_networks_in_health-care_IoT. [Accessed: 09-Dec-2021].

[5] Techopedia, "What is a Wireless Personal Area Network (WPAN)? - definition from Techopedia," *Techopedia.com*, 12-Jan-2017. [Online]. Available: https://www.techopedia.com/definition/5109/wireless-personal-area-network-wpan. [Accessed: 09-Dec-2021].

[6] C. A. Tavera, J. H. Ortiz, O. I. Khalaf, D. F. Saavedra, and T. H. H. Aldhyani, "Wearable Wireless Body Area Networks for medical applications," *Computational and Mathematical Methods in Medicine*, 26-Apr-2021. [Online]. Available: https://www.hindawi.com/journals/cmmm/2021/5574376/. [Accessed: 09-Dec-2021].

[7] A. A. Ltd, "History of the Body Area Networks," *UK Essays*, 12-Aug-2021. [Online]. Available: https://www.ukessays.com/essays/information-technology/history-of-the-body-area-networks-information-technology-essay.php. [Accessed: 13-Dec-2021].

[8] A. Z. Alshamsi, M. A. Serhani, and E. S. Barka, "Lightweight encryption algorithm in wireless body area network for e-health Monitoring," *Lightweight encryption algorithm in wireless body area network for e-health monitoring*. [Online]. Available: https://ieeexplore.ieee.org/document/7880042. [Accessed: 13-Dec-2021].

[9] I. Science, "A review on security and privacy issues in wireless body area networks for Healthcare Applications," *Smart Moves*, 18-Feb-2020. [Online]. Available: https://www.academia.edu/42006669/A_Review_on_Security_and_Privacy_Issues_in_Wireless_Body_Area_Networks_for_Healthcare_Applications. [Accessed: 13-Dec-2021].

[10] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for Healthcare Applications,” *Egyptian Informatics Journal*, 16-Nov-2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110866516300482. [Accessed: 14-Dec-2021].

[11] “What is the OSI model?” *Forcepoint*, 06-May-2021. [Online]. Available: https://www.forcepoint.com/cyber-edu/osi-model. [Accessed: 15-Dec-2021].

[12] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, “A review on body area networks security for Healthcare,” *ISRN Communications and Networking*, 30-Jun-2011. [Online]. Available: https://www.hindawi.com/journals/isrn/2011/692592/. [Accessed: 15-Dec-2021].

[13] J. Valenzuela-Valdes, M. A. Lopez, and P. Padilla, “Human neuro-activity for securing body area networks: Application of brain-computer interfaces to people-centric internet of things,” *IEEE Xplore*. [Online]. Available: https://ieeexplore.ieee.org/document/7841473. [Accessed: 15-Dec-2021].

[14] N. B.N. Ibn Minar and M. Tarique, “(PDF) Bluetooth Security Threats and solutions: A survey,” *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/267200901_Bluetooth_Security_Threats_And_Solutions_A_Survey. [Accessed: 15-Dec-2021].

[15] D. Spitler, “Applying ultra-wideband wireless technology for Security and Automation,” *Security Industry Association*, 17-Nov-2020. [Online]. Available: https://www.securityindustry.org/2020/11/17/applying-ultra-wideband-wireless-technology-for-security-and-automation/. [Accessed: 17-Dec-2021].

[16] Y. Zhang, W. Liu, Y. Fang, and D. Wu, “Secure localization and authentication in ultra-wideband Sensor Networks,” *IEEE Xplore*. [Online]. Available: https://ieeexplore.ieee.org/document/1618808. [Accessed: 17-Dec-2021].

[17] S. Khanji, F. Iqbal, and P. C. K. Hung, “(PDF) zigbee security vulnerabilities: Exploration and evaluating,” *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/334762096_ZigBee_Security_Vulnerabilities_Exploration_and_Evaluating. [Accessed: 17-Dec-2021].

[18] B. Hoon Jung, R. U. Akbar, and D. K. Sung, “Throughput, energy consumption, and energy efficiency of IEEE 802.15.6 Body Area Network (BAN) mac protocol,” *IEEE Xplore*. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6362852. [Accessed: 17-Dec-2021].

[19] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, “Comparing elliptic curve cryptography ... - home - springer,” *SpringerLink*. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-3-540-28632-5_9. [Accessed: 18-Dec-2021].

[20] D. Malan, M. Welsh, and M. Smith, “A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography: Semantic scholar,” *undefined*, 01-Jan-1970. [Online]. Available: https://www.semanticscholar.org/paper/A-public-key-infrastructure-for-key-distribution-in-Malan-Welsh/77f8cf7e431942ac81d64d1d82bde9ae55bd222d. [Accessed: 18-Dec-2021].

[21] A.S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C. Shantz, “Energy analysis of public-key cryptography for Wireless Sensor Networks,” *IEEE Xplore*. [Online]. Available: https://ieeexplore.ieee.org/document/1392772?reload=true. [Accessed: 18-Dec-2021].

[22] Simplilearn, “What is AES encryption and how does it work? - simplilearn,” *Simplilearn.com*, 18-Sep-2021. [Online]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption. [Accessed: 18-Dec-2021].

[23] “What is DES and AES?” *IBM*. [Online]. Available: https://www.ibm.com/docs/en/zos/2.1.0?topic=encryption-what-is-des-aes. [Accessed: 18-Dec-2021].

[24] “Fault analysis of the KTANTAN family of block ciphers: A ...” [Online]. Available: https://eprint.iacr.org/2018/258.pdf. [Accessed: 18-Dec-2021].

[25] T. Jabeen, H. Ashraf, and A. Ullah, “A survey on healthcare data security in Wireless Body Area Networks,” *Journal of ambient intelligence and humanized computing*, 02-Jan-2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7778405/. [Accessed: 19-Dec-2021].

[26] Z. Mahmood, J. L. Rana, and A. Khare, “Symmetric key cryptography using dynamic key and linear ...,” *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/258651762_Symmetric_Key_Cryptography_using_Dynamic_Key_and_Linear_Congruential_Generator_LCG. [Accessed: 19-Dec-2021].

[27] R. Latif and M. Hussain, “Hardware-based random number generation in wireless sensor ...,” *SpringerLink*. [Online]. Available: https://www.researchgate.net/publication/220850010_Hardware-Based_Random_Number_Generation_in_Wireless_Sensor_NetworksWSNs. [Accessed: 19-Dec-2021].