A Technical Aspect of WBAN Security Protocols and Their Challenges: Brief Survey

P. Anitha
Ph.D. Research Scholar,
Department of Computer Science,
Sree Narayana Guru College,
K.G.Chavadi, Coimbatore – 641105, Tamil Nadu, India.

Dr.R. Priya
Associate Professor and Head,
Department of Computer Science,
Sree Narayana Guru College,
K.G.Chavadi, Coimbatore – 641105, Tamil Nadu, India.

Abstract

The "Wireless Body Area Network (WBAN)" has risen to prominence as one of the most promising new health-improving technologies available right now. WBAN's unmanned aspect, conventionality, portability and cost-efficiency are all advantages of using this pervasive computing approach for communications. Those WBANs are especially crucial for patients with life-threatening illnesses. For instance, those with cardiovascular problems, pregnant women and the cognitively ill always need constant monitoring. WBAN, therefore, serves as a real support system for its users on the one side. But on the other side, WBAN uses a wireless medium for its implementation which lacks security. All of the restrictions, particularly those relating to insecurity, were been detailed here. Patients' lives are at risk because of the sensitive nature of their medical information. WBAN's biggest shortcoming is still its inability to keep endpoints and communications upon those networks secure. When it comes to networks transmitting such sensitive information, existing security measures aren't up to the task, which necessitates the development of new ones. The purpose of this review article is to gain insight into WBAN's security issues and to examine current security solutions like "Cryptographic Protocols", "Intrusion Detection Systems" and "Trust Management Systems" in depth. It is very apparent from our observations that current security measures have serious drawbacks. As part of this effort, we also present prospective insights and solutions for resolving the various WBAN security threats.

Keywords: *Wireless Body Area Network, Cryptographic Protocols, Intrusion Detection, Trust Management Systems*

DOINumber:10.14704/nq.2022.20.8.NQ44923 **NeuroQuantology 2022; 20(8): 9029-9040**

1. Introduction

E-health has benefited greatly from the recent development of advanced innovations and information technology. The WBAN development is a specific example of this. The WBAN is used in a wide range of applications. For long-term observation of physiological signals including temperatures, hypertension and respiratory rate, these devices are most often utilized. Hyperglycemia, Alzheimer's, Seizures, Cardiac Arrhythmia Problems, Asthmatic and Infertile are just a few of the medical conditions in which these devices are used.

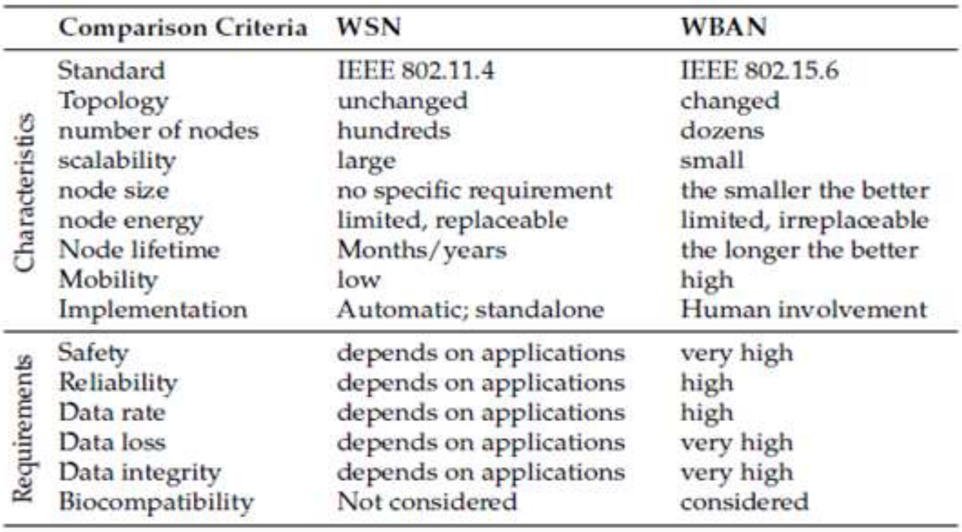
Patients' health may be monitored continuously by WBANs, which can respond as quickly as feasible in the event of an emergency [1]. During a cardiac arrest, for instance, the patient's bodily monitoring system is overloaded with readings from several medical devices. An extremely minimal period must be used to communicate the vast amounts of data that have been gathered.

These requirements include clarity and dependability, moderate price and minimal energy usage along with minimal End-to-End latency because of their real-time characteristics and also high levels of confidentiality and trustworthiness. WBAN hence needs these requirements.

Additionally, the WBAN could be deployed in sporting activities to monitor the physiological parameters of a sportsman while they are engaged in an activity, such as running. To keep track of the healthiness of crops, WBAN may be placed in the natural atmosphere. They may also be used to protect and promote the health of endangered animals. Eventually, they might be used in infotainment, lifestyles and ecological analytics, cognitive computation, defense, or surveillance applications [2].

WBAN differ from conventional "Wireless Sensor Networks (WSN)" in that they incorporate people, are movable, smaller in size and have a much higher rate of data transmission. On the other hand, WSNs are self-contained, have a huge scale and are dependent on the dependability of the application to determine their system throughput. Table 1 shows the differences and similarities between the two.

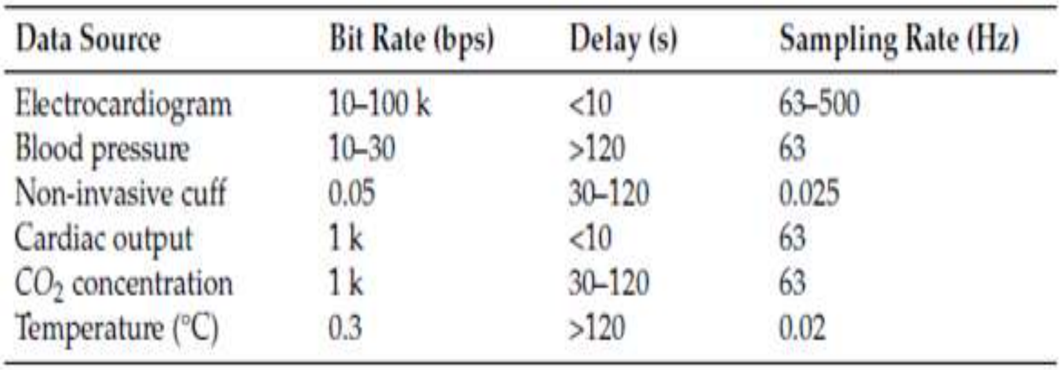
Table 1. Comparison of WSN and WBAN



	Comparison Criteria	WSN	WBAN
Characteristics	Standard	IEEE 802.11.4	IEEE 802.15.6
	Topology	unchanged	changed
	number of nodes	hundreds	dozens
	scalability	large	small
	node size	no specific requirement	the smaller the better
	node energy	limited, replaceable	limited, irreplaceable
	Node lifetime	Months/years	the longer the better
	Mobility	low	high
	Implementation	Automatic; standalone	Human involvement
Requirements	Safety	depends on applications	very high
	Reliability	depends on applications	high
	Data rate	depends on applications	high
	Data loss	depends on applications	very high
	Data integrity	depends on applications	very high
	Biocompatibility	Not considered	considered

Sensor nodes in WBAN, as opposed to WSN, have varying criteria for data rate and delay. Certain regularly preferred sensors in the e-health area have a wide range of requirements, as shown in Table 2. The WBAN is used in a medical environment to manage and store sensitive information about the health of the patient. The "Quality of Service (QoS)" and even system security of these users are quite high. In terms of meeting WBAN system restrictions, several studies [3] have concentrated on the QoS only. Security procedures for WBAN nodes must also take into consideration their unique features in terms of ensuring their safety. WBAN applications' QoS will suffer if the security methods used for confidential records are complex.

Table 2. Bit Rate, Delay and Sampling Rate Requirements for Health Sector Applications



Data Source	Bit Rate (bps)	Delay (s)	Sampling Rate (Hz)
Electrocardiogram	10–100 k	<10	63–500
Blood pressure	10–30	>120	63
Non-invasive cuff	0.05	30–120	0.025
Cardiac output	1 k	<10	63
CO_2 concentration	1 k	30–120	63
Temperature (°C)	0.3	>120	0.02

The employment of smart technologies like "TeleHealth Response Watch," "Remote Patient Monitoring (RPM)" monitors and "Comprehensive Assessment Cameras", which are beneficial for physiology information gathering, makes the implementation of the WBAN functionally practicable. Those gadgets may be used on, within and around the human body. A "Local Processing Unit (LPU)" connects them to specialized applications for analyzing and displaying the collected data. The LPU acts as a bridge between both the "AccessPoints (APs)" and the biophysical sensor systems that are installed on the body. Sensors in the patient's surroundings, such as medical and non-medical sensors, may also interface well with WBAN sensors [4].

WBAN makes use of two different methods for communicating information:

(i) Intra-WBAN:

It solely takes into account the transmission within a cluster of sensing devices as a whole. The WBAN's primary unit, LPU, will connect with each of those nodes. When it comes to the LPU, it's designated the Cluster-Head (CH).

(ii) Inter-WBAN:

This method takes into account communications between several LPU entities, which represent the core entities of various communicating WBANs. WBAN's different communication methods are shown in Figure 1.

Four primary situations for WBAN implementation are identified by these two communication methods:

On-body: It has to do with the transmission of information from one portion of the human body to another.

In-body: It has to do with the transmission of information from inside of the body to the skin.

Off-body: Communications between the individual body surface and any device positioned within 3 meters of the body are the focus of this method.

Body-to-body: It characterizes the inter-WBAN connections between two bodies.

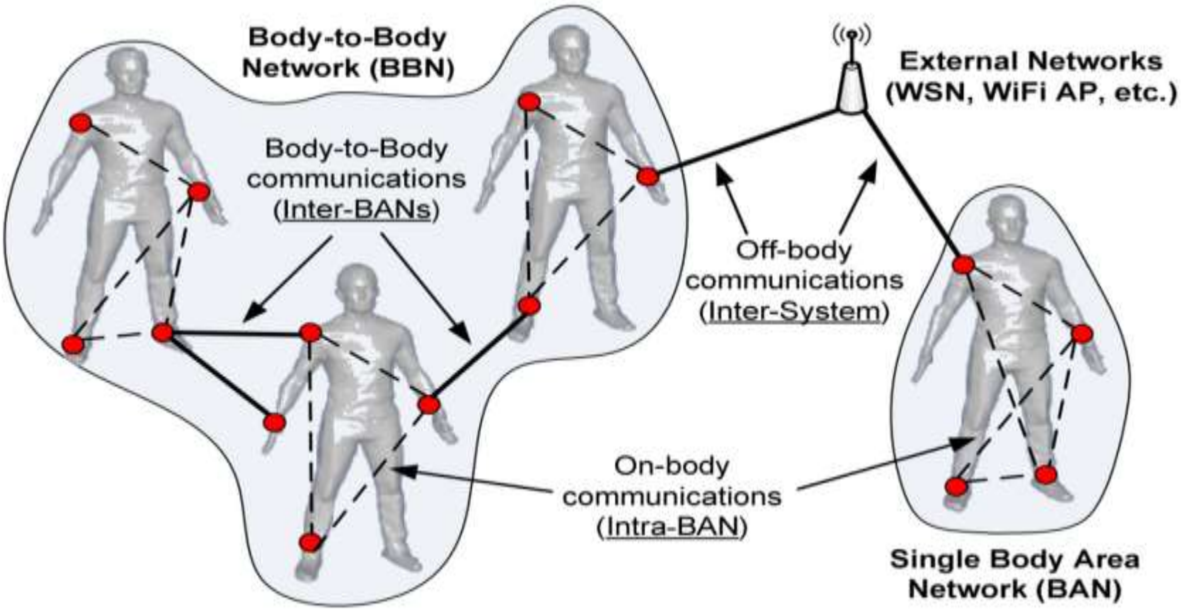

Body-to-Body Network (BBN)
Body-to-Body communications (Inter-BANs)
External Networks (WSN, WiFi AP, etc.)
Off-body communications (Inter-System)
On-body communications (Intra-BAN)
Single Body Area Network (BAN)

Figure 1. Different WBAN communication methods

Those possibilities may be established using a 3 or 4 layered architecture, which includes autonomous medical equipment and interfaces with resource constraints which include a battery, storage, processing and signal strength. In [5] provides a comparative analysis of the techniques that may be employed in this kind of architecture. A WBAN design uses the LPU to preprocess gathered data before sending it to the clouds or a distant server, depending on whether the architecture has 4 or 3 layers. The 3-tiered architecture is shown in Figure 2.

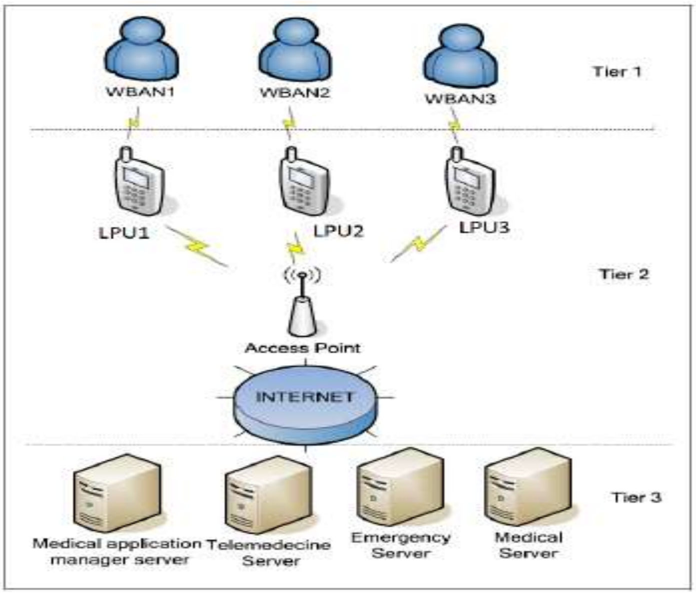


Figure 2. Architecture for 3-Tier WBAN

Research's Problem Statement:

Patients' vital signs are monitored by WBAN, which has access to highly confidential information. In addition, the power usage and privacy demands from these networks are quite high. As a result of its usage of wireless connectivity, the WBAN is vulnerable to a wide range of hypothetical cyberattacks that might have a direct impact on the patient's health. Confidentiality of sensitive information conveyed and privacy of their collection and processing are critical issues. Illegal parties engaged in a destructive activity are attempting to conduct attacks on patients' confidential information. As a result, unauthorized access must be restricted and communications must be encrypted. Reliability, Confidentially, Validity, Consistency and Information Integrity are the most important security characteristics to protect. Various methods may be used to meet the security needs. WBAN security has been the subject of several studies. One thing that none of these proposals have done is address WBAN's robust security measures. In addition, there is a multitude of studies available on WSN's approach to reputation management. The "Mobile Adhoc Networks (MANETs)", "Internet of Things (IoT)", or WSN is the focus of those studies. Neither of them would have taken into account WBAN as a potential application area.

Research Contributions:

The WBAN security problem is investigated in this research. As a consequence, we concentrate on "Cryptographic Protocols", "Intrusion Detection Systems" and "Trust Management Systems" in WBAN, which are all important aspects of WBAN security. As a part of WBAN, we examine and categorize the obstacles and attacks linked to the aforesaid methods. A thorough review of the fundamental and current contributions of this research highlights the aforementioned methods presented. With WBAN as a framework, we can identify the most promising future avenues for tackling security issues.

Paper Organization:

The remainder of the article is structured as follows: Section 2 presents the recent WBAN works proposed by different authors in terms of security, Section 3 briefs about the "Cryptographic Protocols", "Intrusion Detection Systems," and "Trust Management Systems" methodologies with its related approaches by various authors, Section 4 provides the merits and demerits about the surveyed approaches and provide the insights and solutions and Section 5 Concludes this survey article.

2. Related Works

According to [6] in 2017, researchers focused on WBAN connectivity design, privacy and security concerns, vulnerabilities and also the most pressing difficulties those systems confront. Safety procedures and investigations in WBANs are also included in this research. As the last step in this investigation process, they look at prospective extensive exploration and advancement ideas.

There is a concise summary available for WBAN security provided by the researchers in 2018 [7]. Health care services may be categorized using a basic classification proposed by the researchers. It has been determined that all WBAN tiers are vulnerable to security threats. Potential conflicts and wider access have also been identified by the researchers.

A comprehensive review of WBANs including their features and also a categorization of different authenticating methods and processes were provided by the researchers in 2019 [8]. In particular, it examines the pros and cons of different authentication methods, along with their ability to withstand different security threats. Furthermore, the researchers discuss possible prospects.

Researchers in 2020 [9] conducted a complete review of WBAN and WSN privacy and security issues. Comparison has been made after a thorough examination of the features, structure, operational measurements and usage of each. Furthermore, researchers are allowed to participate in research projects that are accessible to the public.

Researchers in 2021 [10] provide a comprehensive review of WBANs innovation, emphasizing privacy and security challenges, solutions, suggestions for further studies and problematic areas. They also offer future research paths for WBAN technology.

Merely methods seem to be of interest to the researchers, who were only concerned with evaluating them. These aforementioned studies didn't include many analyses of the method employed in authenticating WBAN methods about their choice, effectiveness, the preferred modeling techniques and justifications. As a consequence, we've compiled this survey article with a number of the most commonly deployed cryptographic protocols, together with their justifications and the unresolved concerns that remain.

3. Methodologies

To ensure the safety of any network, it is necessary to include both preventive and detection measures. WBAN solutions are described in this section using traditional methods.

3.1. Protocols Based on Cryptography

Confidentiality, Authentication and Data Integrity may all be achieved via the application of cryptographic security. The medical data sent through WBAN may be protected using Asymmetric or Symmetric Encryption/Decryption methods and their variants. Data integrity may be ensured by the use of "Hashing" techniques. To ensure the authenticity of treatment feedback devices, authentication techniques may be deployed. There are three levels of security provided by the 802.15.6 standard relying on cryptographic techniques at the WBAN network layer.

- Level-0: There is no inherent security in an unprotected profile.
- Level-1: There is no confidentiality but provides authentication.
- Level-2: Confidentiality and Authentication are both provided.

However, since cryptography is being used in several effective security contexts, the particular resource and network limitations of WBAN present architecture errors and complexity associated with cryptographic protocols [11].

In WBANs, IEEE 802.15.6 standardized the basic privacy characteristics for confidentiality and authentication. The CH introduces a unique master key or utilizes a pre-shared variant (optional) to construct a secured channel across both terminals if a node chooses to enhance from a non-secure to a secure account. For every conversation between both the node and CH, paired temporal keys are created. During multicast interactions, a group temporal key is utilized.

In WBAN, the following important cryptographic protocols already exist:

The authors of [12] offer endpoint protection for WBANs. Rather than exchanging private information, they employ referencing frames. The "Independent and Adaptive Management of Keys (IAMKeys)" and "Key Management and Encryption for Securing Inter-Sensor Communication (KEMESIS)" techniques were deployed on two levels of hierarchy. To secure communications between both the CHs and BS, the former protocol is employed while the latter has been utilized for a node to CH data transfer. Because of the use of stacked "XOR" techniques, the encryption/decryption processes are simple. In comparison to the IAMKeys protocol, the main distinction between KEMESIS although it is that only one of both when encrypting and decrypting data, "Symmetric Keys (SK)" have been utilized, with the index of the key "K1" or "K2" connected to the data frame.

Regarding inter-node connectivity, the researchers in [13] designed an "Elliptic-Curve Diffie-Hellman (ECDH)" based "Public-key Cryptography" protocol. The "Electro Cardio Gram (ECG)" waveforms information from both communication nodes was utilized to create the identical randomized number 'x' for both connected ends. By analyzing certain ECG waveform properties including amplitude and intervals and also digital slopes, using "Noise Filtering" methods, this is achievable. The "Recursive Polynomial Function f(x,s)" creates the identical SK across both sides for encrypting and decrypting using distinct random numbers s at each node.

A new encryption scheme based on ECG was developed by the researchers in [14]. In an attempt to get identical ECG values within a similar time frame, they hypothesized that the connecting nodes were close to one another. The ECG methods employed various polynomial functions to produce the SK for encrypting and decrypting, but they both retrieved similar aspects from the signal waveform. The "Message Authentication Code (MAC)" and "MAC Acknowledgement (MACK)" are also included in their module. After successfully decrypting the received message, the MACK module guarantees that the receiver responds to the sender with an ACK.

The researchers in [15] chose a quite alternative strategy when it came to the distribution of significant traits. The "Photo

Plethysmo Gram (PPG)" was investigated by the researchers as an alternative to the ECG to provide temporally varying feature sets for creating the polynomial function of encryption. The transmitter generates a Randomized SK, which is then used for encrypting the raw information being sent. On top of that, they added the ciphertext and MAC to an output of the "Fuzzy Vault Obfuscation (FVO)" algorithm. Using similar physiological information sets, the receiver may estimate the nearest feasible polynomial to that generated by the FVO function. As a result of "Lagrangian Interpolation," an approximate polynomial may be reconstructed with reasonable accuracy. When the polynomial is successfully reconstructed, the secret SK is retrieved and decrypted.

3.2. Intrusion Detection System (IDS)

A network's preventive security procedures would be incomplete without an IDS to track down and stop potential security threats. Security breaches that go undiscovered might cause irreparable harm to the network. The IDS may be divided into two basic groups depending on how they identify threats:

Determination based on Rules: Predetermined attack signatures and patterns are stored in a database that is used to assess the system and network activity.

Detection based on Anomaly: It establishes a baseline of anticipated behavior and labels anything that deviates from it as an anomaly.

There are many new anomaly and rules based detection methods that WBAN's IDS needs to effectively identify network abnormalities. An IDS solution for WBAN must handle issues such as collecting audit features, constructing a proper network behavior and regular user profile.

In WBAN, the following important IDS systems already exist:

It was one of the first efforts to identify intrusions on WBANs using a "Negative Selection Pattern Matching" technique presented by the researchers in [16]. The technique was modeled on how the body's immune system identifies and eliminates foreign cells when they invade. Nodes' usual behavior is defined by a sequence of feature sets and the second set of features termed detectors, which have no matching in the feature set repository. The method has been built to keep track of modifications in feature sets regularly. In able to do an inter-set comparison, every node's actions are continuously recorded on the server-side. This server then turns the information into encoded string patterns.

Comparative experiments were conducted by the researchers in [17] involving "Snort" and "Kismet", two prominent IDS tools. Nodes have been configured to carry out "Signal Jamming" and "Packet Flooding" attacks in their research. To capture traffic on a network, "WireShark" with "PPPSniffer" were utilized as an intermediate transcoder and the recorded information was analyzed offline using the IDS tools. WBAN IDS approaches for "802.15.4 Zigbee" towards the working team 6 draft standards were missing inside this research, probably owing to uncertainty over feature revisions. A fresh batch of solutions relying on the 802.15.6 standard started to appear after its approval in 2012.

Incorporating "Support Vector Machine (SVM)" for activity categorization and "Linear Regression" to examine anomalies, the researchers in [18] created a centralized "Machine Learning (ML)" based IDS. Their approach was based on the CH's ability to recognize anomalies in the sensor data. Regression, Classification and Training are all carried out by the CH.

The researchers of [19] suggested an IDS scheme that involves "Multi-Objective Genetic Algorithm (GA)" methods. They used "Detection Rate (R)", "False Positive Rate (P)" and "Total Energy Usage (E)" to solve the trade-off between security and resource utilization. It was decided that the GA's fitness function should aim to increase R while minimizing both P and E. This technique has been employed to choose, recombine, mutations and substitution feature sets to identify the best possible permutation for the training stage. Many adversarial approaches were used to evaluate the system's effectiveness.

As a solution to the problem of sensors broadcasting network records in contrast to their detected information, the researchers in [20] suggested a "Mobile Agent (MA) based IDS". Training MAs relied on localized data sources, whereas network-wide correlation calculations were carried out on the CHs. As a result, the CH sends independent MA programs to monitor sensor nodes for intrusions and conduct localized assessment and detection. As a result of the noticeably modest size of MAs when compared to real-time network activity records, their technique considerably lowered network resource consumption.

3.3. Systems Based on Trust Management (TM)

Against nodes that have been hacked from inside a network, the cryptographic methods are worthless.Insider assaults are frequently countered using trust-based security measures.In terms of determining how trustworthy a node is, the TM systems take into account a multitude of elements, including its historical behavior, the results of its attack detection and the views of its neighbors.Nodes in a reputation-based TM system are rewarded for positive conduct and condemned for negative ones.Reputation statistics are determined, allocated and disseminated in different ways in each of the two systems.Traditional WSNs often employ TM methods as lightweight encryption options.

In WBAN, the following important TM systems already exist:

Sybil/clone threats may be detected in a WBAN with numerous patients in an ICU, for instance, using a distributed TM system developed by the researchers in [21].When they developed their protocol, they decided to extend the RED methodology for WSN.Nodes that are authentic work together to assess their neighbors and exclude clones under the auspices of SRED withan effective andself-healing mechanism.Each node broadcasts a signed packet with its ID and position to its neighbors after broadcasting a complete network seeding for randomly chosen at set intervals.The seed would then be used to generate a random selection of network nodes to test the veracity of the broadcasted data. Almost every node delivers its acquired geolocation packet to the observers for assessment when one of those witness nodes is selected.If 2 packets having various locations and a similar ID are identified, revocation procedures for the nodes with that ID will be initiated.

Alternative compact TM depending on "Self-Correlation" methods was suggested in the article [22] by the researchers.Each node within the network has a vector of its trust values and this vector is maintained by the protocol.As the size of the network in WBANs is very minimal, this is deemed possible.After querying its neighbors for their perspectives on their intended receiver, a transmitter node tries to determine how much weight each of their comments should be given, depending on how close their trust vectors are to one other.The standardized partial derivative including both trust vectors yields the similarity measure.Finally, the trustworthiness of the recipient is computed as a composite index of the individual views of the neighbors of the transmitting node.

The researchers of [23] suggested a TM interface between both the WBAN and the BS users.The research reflects on using inexpensive trust certificates to manage access to a cloud-based WBAN data bank.Every characteristic that may be associated with a user is included in a certificate.A TM server and a user database server must be contacted separately by the user to get the values of trust and role.Two servers reply by transmitting the data to an authorization server that creates a trusted certificate based on both sources of evidence and sends it back to the client.In able to authenticate and authorize the cloud-based WBAN BS, the certificate serves as a token for the user.

4. Discussion of the Study

4.1. Survey Findings

The WBAN security solutions investigated in this research is an attempt to expose both their advantages and disadvantages, dependent on the assessment of existing methods.

(i) Protocols based on Cryptography:

Protocol Structure: It's generally based on a Decentralized structure.

Methodologies:

- Preliminary key creation with five fake frames.
- The minimum and maximum order in which polynomial-keys may be generated.
- A polynomial-key concealment function has a minimum and maximum order.

Computation Over-Head: Heavy

Advantages:

- Ensuring security and integrity of data with an eminently practical and secure key agreement

Disadvantages:

- Buffering is required for every communication node pair, which makes it harder to identify a hacked node in the system.
- Confined to node monitoring ECG phenomena, key generating is very vulnerable to interference, the difficulty of computing is quite large, impossible to pinpoint a corrupted node.
- Detection of a hacked node is difficult owing to the continual notification of successful decryption, which is confined to ECG measuring nodes.
- Several nodes monitoring the same phenomena may communicate, which makes it challenging to identify a hacked node. This makes it vulnerable to noise.

(ii) Intrusion Detection System:

System Structure: It's generally based on a Centralized or Semicentralized structure.

Methodologies:

- Training and signature set represented in strings.
- Setting up a training program.
- Training sets that are genetically encoded.
- Information on mobile agents' operations and training sets.

Computation Over-Head: Moderately Low

Advantages:

- The compromised nodes that are simpler and more accurate are finally separated.
- False positives are less likely with a two-stage assessment and vulnerable nodes may be more readily detected.
- The vulnerable nodes may be quickly identified owing to a careful balance of resource consumption and accuracy trade-offs.
- Because of the tiny size of the agent code, there is minimal communication overhead, which makes it easier to isolate hacked nodes.

Disadvantages:

- Logs are sent through the network at a large communication cost, limiting redundancy and scalability and are only available for a limited range of attack signatures.
- Analyzes only data gathered via the usage of sensors.
- The time complexity may be too long in certain cases.
- The MA may be tampered with and hijacked by an attacker.

(iii) Systems based on Trust Management:

System Structure: It's generally based on Distributed structure.

Methodologies:

- The interval between seed broadcasts.
- Instances of vectors with pre-set opinion values.

Computation Over-Head: Medium

Advantages:

- Compromises are quickly identified owing to the randomness of witnesses and the strong redundancy and resilience of the system.
- Compromised nodes are segregated with a high likelihood owing to the system's strong scalability and redundancy.

Disadvantages:

- The probability that not every witness at a given point in time is malevolent is based on the overhead that comes from the continual broadcast of information.
- Easily manipulated by harmful feedback.

Overall Findings:

According to the finding of the survey, cryptography-based security solutions are the most common and have a relatively large overhead. A hacked node with cryptographic keys might severely restrict these solutions' ability to protect the network. In addition, the results of this survey show that these networks lack innovative IDS methods. From the results of this study, we could conclude that a safe WBAN requires both TM and IDS mechanisms to safeguard systems from threats and powerful cryptography-based security methods to enable protection measures.

4.2. WBAN Research Importance and Insights of the Survey

The WBAN technology transmits both patient based information and medicinal instructions that are very important. As a result, WBAN seems to be more vulnerable. The "Body Control Unit (BCU)" and also the distant healthcare workers may be eavesdropped on by malicious users, who can then insert communications, repeat previous communications, counterfeit and eventually damage the device's integrity. When an attack succeeded, those activities will not only compromise a patient's confidentiality and also suppress valid data or introduce fraudulent data through the network, resulting in undesired activities such as medication distribution or blocking lawful actions such as alerting a doctor in an emergency.

Recently hackers gained access to a Texas healthcare system's network, exposing the personal medical data of 405,000 people in one of the worst HIPAA security vulnerabilities ever revealed. The worst part is that low-tech security interface weaknesses allowed implanted cardiac devices to be hacked, along with cordless insulin infusion systems.

All of the aforementioned factors might be harmful to patients' health and limit the adoption of WBAN based clinical applications. As a result, the "Food and Drug Administration (FDA)" in the United States believes that medical equipment and healthcare networks have to pay more attention to security in particular to limit public risk.

4.3. Solutions

When it comes to creating a secure network for WBAN, it might be more difficult than for other kinds of networks. The following suggestion plans for improvement must be met by a WBAN security infrastructure.

(i) Efficiency:

Because of their small size, WBAN nodes often lack appropriate energy, compute, storage and transmission range. Complicated cryptographic processes, requiring large amounts of energy, cannot be performed by them. To reduce connectivity overheads and power consumption, the network infrastructure must be built to be as lightweight and quick as feasible.

(ii) Scalability:

It's an acronym for "plug and play". Sharing any similar cryptographic information across various devices is problematic because of device compatibility considerations. However, nodes may depart or connect to the network at any moment due to the human body's constant movement. WBAN cannot benefit from a time-consuming security procedure. As a result, while creating WBAN security infrastructure, designers must prohibit depending on too much past security knowledge. Scalability is not about increasing in size; shrinking is also sometimes overlooked.

(iii) Usability:

Because most patients lack the requisite technical expertise to operate the device, the system design must be basic and easy to implement. Skilled procedures may result in improper device configurations and a crappy user experience if they are too complicated.

5. Conclusion

We looked at the security issues and vulnerabilities in the framework of WBAN throughout this review. Based on our research, we've identified many types of security measures already in use. We conducted a thorough evaluation of those solutions to determine their advantages and disadvantages. Viable protection mechanisms and design considerations for WBANs were examined, covering potential solutions to various threats. Future research combining cryptography, IDS and TM approaches will be significant in furthering information security in these networks.

Micro-sensor equipment, embedding engineering and low-power radio telecommunication technologies are all expected to lead to lighter and better medical sensors in the future. The resource constraints may be more difficult to manage for nodes at the nanoscale or those implanted. Our vision also includes the ability for individuals to purchase and wear sensors as part of their clothing, as well as the ability to 3D print their sensors. Security methods for these devices may need to be more adaptable and compatible. Many obstacles remain to developing a secure, non-intrusive and user-pleasant WBAN system. This survey work might serve as a guide for researchers who want to create a secure WBAN and promote the widespread usage of WBAN medical applications in everyday life.

References

[1]. Narwal, B.; Mohapatra, A.K. A Survey on security and authentication in Wireless Body Area Networks. J. Syst. Archit. 2021, 113,101883.

[2]. Ullah, F.; Khan, M.Z.; Mehmood, G.; Qureshi, M.S.; Fayaz, M. Energy Efficiency and Reliability Considerations in Wireless Body Area Networks: A Survey. Comput. Math. Methods Med. 2022, 2022, 1090131

[3]. Jabeen, T.; Ashraf, H.; Ullah, A. A survey on healthcare data security in wireless body area networks. J. Ambient Intell. Humaniz. Comput. 2021, 12, 1–14.

[4]. Vignesh, M.R.; Sivakumar, S. Healthcare Sensors Issues, Challenges & Security Threats in Wireless Body Area Network: A Comprehensive Survey. Int. J. Trend Sci. Res. Dev. 2021, 5, 989–997.

[5]. Sharma, R.; Kang, S.S. Wban for healthcare applications: A survey of current challenges and research opportunities. J. Crit. Rev. 2020, 7, 2444–2453.

[6]. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt. Inform. J. 2017, 18, 113–122.

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

[8]. Hussain, M.; Mehmood, A.; Khan, S.; Khan, M.A.; Iqbal, Z. A Survey on Authentication Techniques for Wireless Body Area Networks. J. Syst. Archit. 2019, 101, 101655

[9]. Roy, M.; Chowdhury, C.; Aslam, N. Security and Privacy Issues in Wireless Sensor and Body Area Networks. In Handbook of Computer Networks and Cyber Security; Springer: Cham, Switzerland, 2020; pp. 173–200.

[10]. Hajar, M.S.; Al-Kadri, M.O.; Kalutarage, H.K. A survey on wireless body area networks: Architecture, security challenges and research opportunities. Comput. Secur. 2021, 104, 102211

[11]. M. Toorani, “On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard,” arXiv:1501.02601 [cs], vol. 8976, pp. 245–260, 2015, arXiv: 1501.02601. [Online]. Available: http://arxiv.org/abs/1501.02601

[12]. R. V. Sampangi, S. Dey, S. R. Urs and S. Sampalli, “A security suite for wireless body area networks,” arXiv:1202.2171 [cs], Feb. 2012, arXiv: 1202.2171.

[13]. A. S. Sangari and J. M. L. Manickam, “Public key cryptosystem based security in wireless body area network,” in 2014 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Mar. 2014, pp. 1609–1612.

[14]. 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, no. 6, Nov. 2012.

[15]. 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, no. 1, Jan.2009.

[16]. T. Sundararajan and A. Shanmugam, “A Novel Intrusion Detection System for Wireless Body Area Network in Health Care Monitoring,” Journal of Computer Science, vol. 6, no. 11, 2010.

[17]. S. Maharjan, “Development of a Lab Experiment for Intrusion Detection System in Wireless Body Area Networks,” 2013. [Online]. Available: https://www.duo.uio.no/handle/10852/37443

[18]. O. Salem, A. Guerassimov and A. Mehaoua, “Anomaly Detection in Medical Wireless Sensor Networks using SVM and Linear Regression Models,” LIPADE Laboratory, University of Paris Descartes, France, Jun. 2014.

[19]. G. Thamilarasu, “iDetect: an intelligent intrusion detection system for wireless body area networks,” International Journal of Security and Networks, vol. 11, no. 1/2, p. 82, 2016. [Online]. Available: http://www.inderscience.com/link.php?id=75074

[20]. G. Thamilarasu and Z. Ma, “Autonomous mobile agent based intrusion detection framework in wireless body area networks.” IEEE, Jun. 2015, pp. 1–3. [Online]. Available:http://ieeexplore.ieee.org/document/7158178/

[21]. M. Anandkumar, C. Jayakumar, A. Kumar, M. Sushma and R. Vikraman, “Intrusion Detection And Prevention Of Node Replication Attacks in Wireless Body Area Sensor Network,” International Journal of UbiComp, vol. 3, Jul. 2012.

[22]. W. Li and X. Zhu, “Recommendation-Based Trust Management in Body Area Networks for Mobile Healthcare,” in 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems, Oct. 2014, pp. 515–516.

[23]. X. Wu, “A Lightweight Trust-based Access Control Model in Cloud-Assisted Wireless Body Area Networks,” International Journal of Securityand Its Applications, vol. 8, no. 5, pp. 131–138, 2014.