IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Security Issues in Wireless Body Area Networks - Review

G. Sridevi Devasena[1*], S. Kanmani[2]

[1]Indian Maritime University, Chennai, India
[2]Department of Information Technology, Pondicherry Engineering College, Institute, Puducherry, India

[*]*Corresponding Author: sridevigphd@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 06/Jul/2018, Published: 31/Jul/2018

***Abstract*—**Recently, Wireless Body Area Sensor Networks (WBANs) becoming more attractive and have revealed a great prospective in real-time monitoring of the human body. WBANs have attracted an extensive variety of monitoring applications such as sport activity, healthcare and psychoanalysis systems. These wearable sensor systems plays significant role since it monitors and controls the patient life. Security Issues in Wireless Body Area Networks – Review reports the overview of WBAN architecture, various security requirements, WBAN routing protocols. Secure WBAN is essential to develop strong security system in order to protect the life critical applications. However providing security and privacy for wireless sensor network and WBAN is a critical and challenging one. Here a common outlook for secured WBAN is given along with the reviews of various protocols using security and privacy issues.

***Keywords*—**Wireless Body Area Network, Security Issues, Security Requirements, WBAN Routing protocols.

I. INTRODUCTION

Introduction WBAN's are a special kind of Wireless Sensor Networks (WSN) designed particularly for monitoring the human body and communicate the vital signs such as blood pressure, temperature, heart beat rate, etc., WBAN is a network where sensor nodes are fixed in and around of the human body [1]. The monitored signals are collected by using sensors and control unit. Communication protocol among the sensor nodes is selected based upon the application requirements. The monitored signal or data passes over many devices to reach the destination. Hence the data should be delivered confidentially to the receiver side.

Typically, the vital physiological signals of patient or group of patient are captured by using BAN technology, still facing many issues. It includes capturing the signals and delivering it in a timely fashion, data loss during aggregation, unauthorized access, modifying original message by the adversaries, etc., since wireless or remote technology is open to everyone. Therefore security and privacy is an enormous issue in the network [7].

Recent research area of wireless network security involves many technical concerns. Many security requirements are in need of protecting a network and that should be considered in the design of a security protocol. It includes factors like confidentiality, integrity, and authenticity. An effective security protocol should make available of those services to meet the requirements. A common security service for WSNs includes authenticity, non-repudiation, freshness, availability, intrusion detection, and key management.

The contributions of this survey paper are as follows. The system architecture described the structure of WBAN. The major security and authentication requirements to ensure the safety of a WBAN are explained. Various traditional WBAN secure routing protocols are described and tabulated its advantage and disadvantages.

The Rest of the paper is organized as follows, Section I contains the introduction of WBAN, Section II presents WBAN system architecture, Section III presents WBAN system architecture, Section IV presents WBAN routing protocols, section V concludes the survey.

II. WBAN SYSTEM ARCHITECTURE

Wireless communication among the sensor nodes reduces the physical constraints and simplifies the network structure. Several WBAN applications were developed and deployed with appropriate verification. The application areas are widely increasing day by day. It includes mobile health care, biometric monitoring, and sporting areas to sense and send acceleration data during the course. WBAN system architecture is shown in figure 1 consists of group of nodes includes sensors, actuators and control units. Wireless channels are used to communicate from one node to other node. The sensed data are sent to the data processing node using remote channel.

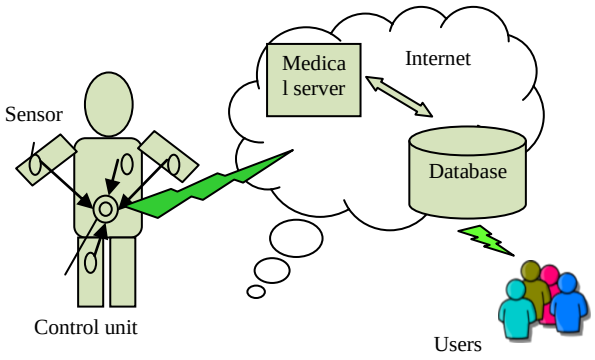

Figure 1. WBAN System Architecture

The sensors communicate with local control unit placed at accessible distance then this control unit communicate with destination to exchange data in order to investigative and therapeutic purpose.

A. Information Security and Privacy in WBAN

WBAN has several security measures and plays a very major role in the field of patient health monitoring. Establishing secure communication between the sensors and the users is a very big challenge. Patient's Health Record (PHR) is maintained using a set of attributes and the treatment is given based on the collected information which is obtained using sensors. The attributes of PHR should get verified for its authenticity. The data composed in WBANs are very perceptive and imperative because these are the basis of clinical diagnostics.

Information security is that the information is securely stored and transmitted over the communication channel. Information privacy is that the information can only use and access by the authorised persons. Data confidentiality in WBAN is the most important issue. Data confidential prevents the information from disclosure of information to others i.e., it does not reveals the information. Eavesdropping attack easily breaks data confidential sometimes since the protocol data unit uses the source and destination information headers and passes the information through intermediate nodes.

Encrypting the information using encryption technique provides data security or confidentiality. Security algorithms such as Data Encryption Standard (DES), Advance Data Encryption Standards (ADES), Advanced Encryption Standard (AES), Secured Hash Algorithm (SHA) etc., was proposed in order to provide secured and confidential communication.

Integrity is provided for the data prevention reasons since integrating data prevents the data modification during data transmission. To support confidentiality and integrity for the generated information data freshness factor is used. Data freshness factor is applied in terms of delay. Availability of information is must for e-health care system in order to carry required operation at any instance of time. Data privacy is essential to make the collected information secure and the privacy of source location is essential to reduce the attacks. Proper mechanism is carried out for maintaining the privacy among the nodes.

The sensors communicate with local control unit placed at accessible distance then this control unit communicate with destination to exchange data in order to investigative and therapeutic purpose.

B. Achieving Data Authenticity in WBAN

To prevent the revelation of sensitive information to unauthorized users, the statistic information must be transmitted in encrypted structures. Formerly key agreement has been a main focus of many researchers. However, most of them need either pre-share key materials or complicated cryptographic calculation, which shows low efficiency and poor flexibility.

Wireless channels are open and everyone can participate in the communication by configuring the configuring the radio interface at the same frequency band. This gives a simple and better advantageous route for attackers to break into a network. Research in network security includes several technical issues.

Several security requirements should be considered in the design of a security protocol, including confidentiality, integrity and authenticity. An effective security protocol should provide services to meet these requirements. A common security service includes confidentiality, integrity, authenticity, non-repudiation, freshness, availability, intrusion detection, and key management [8].

Cryptographic key is used for secured communication between sender and receiver. The secure key management methodology includes generating keys, improving the level of security by using smaller key size and managing the key among the users. Public key, private key, hash and dynamic key, group key are the types of cryptographic keys. Several security techniques such as are implemented using these keys.

III. MAJOR SECURITY REQUIREMENTS

A. Confidentiality

Patient-related detected information ought to be kept confidential during storage periods. Particularly, its secrecy or confidential rate should be robust against node compromise and user conspiracy.

B. Confidentiality

The sensed information should not be modified illicitly during storage periods, which can be recognized by a node dynamically.

C. Dependability

Patient related information must be promptly retrievable when node failure or information eradication happens.

D. Access Control (Privacy)

To avoid unauthorized access a fine-grained data access policy should be approved in order to protect the patient related information generated by the WBAN.

E. Accountability

When a user of the WBAN mishandles the privilege to carry out illicit actions on patient-related data, then the corresponding user should be identified and held responsible.

F. Revocability

The privileges of WBAN users or nodes should be withdrawn from them in time at once they are identified as compromised or behave maliciously.

G. Authentication

The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented.

H. Ease of Use

The patient-related data should be accessible even under denial-of-service (DoS) attacks.

IV. WBAN ROUTING PROTOCOLS

It should include important findings discussed briefly. Wherever necessary, elaborate on the tables and figures without repeating their contents. Interpret the findings in view of the results obtained in this and in past studies on this topic. State the conclusions in a few sentences at the end of the paper. However, valid colored photographs can also be published.

A. Security Key Management

Highest priority is given to secured communications in order to prevent the network degradation and to deduce the criticalness of the system. Security Key Management (SKM) is helpful in generating keys for secure data communication. In the earlier period numerous SKM methodologies were proposed and named as symmetric and asymmetric key management, deterministic key material distribution management, random key material distribution management, location-based key material distribution management, key agreement model, wireless body area network uses group key management [9].

B. Physiological-Signal-Based Key Agreement (PSKA) Scheme

This technique is used to secure the inter-sensor communication within the range of body area network in a plug and play manner. Here authenticated symmetric (pair-wise) cryptographic key using physiological signals [2] are used to provide secure communication among neighbor nodes. A random symmetric key is generated by one of the two sensors using a feature obtained from physiological signal. The fuzzy vault scheme is used to hide the keys generated using a set of values 'A' and can be unlocked by another set of values 'B'. Message Authentication Code (MAC) such as Hash MAC - Secure Hash Algorithm 1 (HMAC-SHA1)] is the key locked in the vault.

C. Certificate-less Remote Anonymous Authentication WBAN

An efficient and light-weight authentication protocols was proposed to facilitate remote WBAN users to anonymously enjoy the healthcare services. Authority mechanism called certification authority (CA) that can create and verify cryptographic keys for different purposes. Therefore healthcare service providers and patients contacts CA for key distribution. This security enhanced anonymous authentication includes three phases such as initialization, registration and authentication. The legitimate client chooses the partial private key using the algorithm Partial Private-Key-Extract then proper verification is done [3].

D. Secure Key management Scheme based on ECC algorithm

In order to protect patient's sensitive information and to establish secure communication between users and sensors fixed in or around patient's body. Elliptic Curve Cryptography (ECC) algorithm [4] based secure and proficient key management method was proposed to protect patient's medical information in healthcare system. This method consists of four phases such as setup, registration, verification and key exchange. Patient's smart phone SIM card number is the Identification code used with a private key generated by legal use and it also helps to prevent replay attack using counter number at every process of exchanging authenticated message.

ECC is a one of the public key cryptography. ECC is one of the better security solutions for wireless networks because of its small key size and low computational overhead. For example, in RSA 1024-bit key is considered to be as secured but in ECC only 160-bit key is enough to provide secured communication.

E. Hybrid Security Mechanism for WBAN

To meet the security requirements of WBANs with strict source constraints a feasible hybrid security mechanism [5] was proposed. For providing link level security an ID-based Elliptic Curve Diffie-Hellman (ECDH) Key Exchange protocol and Master Key establishment is developed which distributes a single symmetric key. Symmetric cryptosystems are essential to enlarge the link level security mechanism as well as to guaranty the MAC layer security of WBAN. By selecting appropriate parameters the cryptographic operation time can be extremely fast. A feasible hybrid security structure is finely developed by combining symmetric and asymmetric cryptographic algorithm in order to provide all these security requirements with resource constrains.

F. Enhanced secure sensor association and key management

Based on ECC and hash chains an enhanced protected sensor association and key management [6] was proposed to carry out authentication mechanism. Wireless communications are mostly vulnerable to several attacks like reflexive eavesdropping and message interception hence it is mandate to provide security for the information passed over this channels. This sensor protocol includes initialization phase then sensor association phase; the public keys generated are forwarded to achieve higher secrecy.

The static public key is bound to the entity for a certain period of time, typically through the use of certificates. The PC computes number of secret keys {k1, k2, k3...,kn} for each node equipped with the patient body by using n number of random numbers{ r1, r2, ..., rn}, then hash operation is computed for generating the strong secret key h2 = (kx||kx). Mutual authentication should be provided between all the nodes, PC distributes the group key for all the nodes embedded to the patient body. The entity user k should compute the secret key MACK (2, I Dd, I Dc, Rd, Rc) therefore explicit key authentication can be provided by preventing the node from malicious attackers.

G. Coercion faced in WBAN

WBAN works in diverse atmospheres with open access therefore attackers can easily accommodate the network and injects false information. Hence data base or data storing system is one of the challenging tasks from preventing data thefts. Because of open access the data is liable to be altered, eavesdropped due to wireless medium, injected with false information etc. Information brakes occur due to false message injected in the node and this leads to network failure by frequent changes occurred in the node. The wireless channels are configured at similar frequency bands are often suffers from the attackers since the same frequency configuration the nodes in the network can able to communicate at every time and leads to network failures. Therefore it is necessary for applying strong security mechanisms in order to protect the network from different types of attacks. The essential key factors for providing security are data integrity, data freshness secure management and data authenticity. Table 1 describes some security and privacy protocols discovered for WBAN.

Table 1. WBAN- security and privacy protocols

Security Protocols	Cryptographic Techniques	Advantages	Disadvantages
Hardware encryption	Chip con2420	Restrained power utilization	Depends on definite sensor set of connections
Secure discovery protocol	Public key	Mitigate Dos attacks	Constrained computation Takes long time
BioSec: A Biometric Based Securing Communication	Biometric Public key	Secure communication Error. Fraud, Mistake does not exist. Distinctive Universal Collectable Effective and Well secure compared to other.	Randomness: difficult to guess. Cannot be used everywhere, Small size. Physically fraud present
Public key cryptographic based method	Elliptic curve cryptography Public key	Communication efficient	Computational inefficient
GDP protocol	Group key	Reduces total time and complexity Efficient in computation and communication	Error and mistakes
Symmetric cryptosystems	Biometric Public key	Low computational cost	Used to measure the similar type of physiological parameters

V. CONCLUSION

Nowadays, people regularly have fixed sensor in their body to extend their life. This work reviewed the deployment of WBANs in terms of security and privacy. An outlook for WBAN and some of the protocols discovered for security and privacy were discussed. A small outline for the conventional security protocols review has been made with respect to safety measures concern carried out by this technology. The WBAN current security measures and recent WBAN routing protocol regards security and privacy along with issues have been explained. This survey will encourage to design and built a novel, dependable, reliable as well as secure and privacy in WBAN.

REFERENCES

[1] I.A. Sawaneh, I. Sankoh, D.K. Koroma, "*A survey on security issues and wearable sensors in wireless body area network for healthcare system*", 14th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 304-308, 2017.

[2] K.K. Venkatasubramanian, A.Banerjee, S.K.S. Gupta, "*PSKA: Usable and secure key agreement scheme for body area networks*", IEEE Transactions on Information Technology in Biomedicine, Vol.14, Issue.1, pp. 60-68, 2010.

[3] J. Liu, Z. Zhang, X. Chen, K.S. Kwak, "*Certificateless remote anonymous authentication schemes for wirelessbody area networks*", IEEE Transactions on Parallel and Distributed Systems, Vol.25, Issue.2, pp.332-342, 2014.

[4] Y.S. Lee, E. Alasaarela, H. Lee, "*Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system*", IEEE International Conference on Information Networking, pp. 453-457, 2014.

[5] L. Jingwei, K.S Kwak. "*Hybrid security mechanisms for wireless body area networks*", Second International Conference on Ubiquitous and Future Networks, pp. 98-103, 2010.

[6] J.Shen, H.Tan, S.Moh, I.Chung, Q. Liu, Q., X. Sun, X. "*Enhanced secure sensor association and key management in wireless body area networks*, Journal of Communications and Networks, Vol.17, Issue.5, pp.453-462, 2015.

[7] M.R.K. Naik, P. Samundiswary, "*Wireless body area network security issues—Survey*", IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies pp. 190-194, 2016.

[8] D.He, S. Zeadally, N. Kumar, J.H. Lee, "*Anonymous authentication for wireless body area networks with provable security*", IEEE Systems Journal, 2016.

[9] M.Gowtham, S.S. Ahila, "*Privacy enhanced data communication protocol for wireless body area network*", 4th International Conference on Advanced Computing and Communication Systems, pp. 1-5, 2017.

