Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wireless Body Area Network Security

Jyoti S. Kamble, Amarsinh V. Vidhate
Ramrao Adik Institute of Technology, Mumbai University,
Maharashtra, India

Abstract— The WBANs (Wireless Body Area Networks) becoming interesting research domain for many researchers due to its increasing use in different real time environments such as healthcare systems, medical systems etc. WBAN is made of wireless sensor networks by consisting of small tiny sensor devices and remote devices for remote person body monitoring activities and related environment. Therefore WBAN is becoming the interesting method for real time wireless monitoring of physiological human body signals in order to support healthcare system related applications. WBAN is having two main issues or challenges to handle for researchers such as energy efficient and security. In this paper we review different security techniques in WBAN. We presented the literature survey on methods of security like biometric based security, elliptical curve based security, TinySec based security and hardware encryption based methods. In WBAN, security is required to ensure the reliable and trustworthy patients personal health information collections.

Keywords— WBAN, Biometric, Elliptical curve, ECC, TinySec, ECG, SPINS

I. INTRODUCTION

Since from last 15 years, use of wireless sensor networks (WSN) is rapidly growing for different applications and domain. Wireless biomedical sensor network is one of widely used WSN deployment for measuring the different patient's physiological signals. Such a network is Body Area Network or Wireless Body Area Network (WBAN) or BAN. WBAN is nothing but the radio network which is used for performing the communication between sensor nodes which are working around person body that continuously monitors body movements and parameters [1] [2]. Such monitored signals are further collected by personal end user devices such as smartphones or PDA. These personal devices are treated as sink for data that is collected by sensor nodes for transmitting it to the allocated healthcare system persons in order to track the current health status of patient. Figure 1 shows WBAN in medical application [1]. In this, human biological data such as ECG (electrocardiogram), BP (blood pressure), SpO2 (oxygen level), body movements etc. is collected by sensor nodes. It is then transmitted to controller like PDA or Smartphone [1].

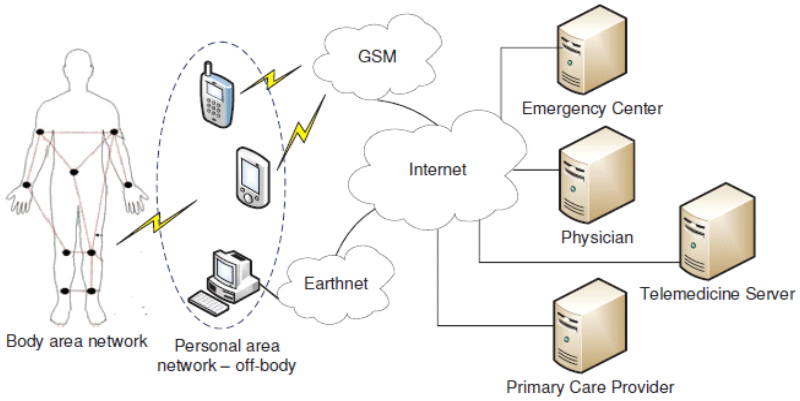

Fig 1: Healthcare System Example of WBAN

As WBAN is composed of wireless sensor nodes, there are two major challenges of WBAN such as energy and data security. As sensor nodes are having limited power, there should be efficient technique for data collection and communication with goal of extending the network lifetime of sensor nodes. There are wide ranges of energy efficient methods already proposed by various authors. Energy efficiency is out of scope of this paper and our main focus is on literature survey over different WBAN security methods [3].

Security is unaddressed research problem which is yet to be resolved completely for WBAN networks. The growth of WBAN is important in health applications like m-health as well as modern telemedicine, but having lack of security to person's critical health information. There are many methods introduced to address the security issues in WBAN. In earlier stage, different research teams have contributed the various approaches towards designing the WBAN systems. But these research teams majorly focused on designing the system blocks as well as in network protocols. Apart from this, there is no other parameter such as security is considered; therefore it becomes difficult to find the solutions on providing

the data security in WBAN. Hence for WBAN, security should be separately addressed. In literature, there are different security methods proposed for wireless sensor networks [1] [2] [3]. The SPINS (security protocols for sensor networks) is the set of protocols for wireless sensor network that achieves the security requirements. To perform data encryption and computation of MAC (message authentication code), SPINS uses symmetric keys. But the limitations of SPINS is that it only applied on wireless sensor networks, therefore it is difficult to applied SPINS over the WBAN as it having the environmental parameters such as human body as well as constrained computing resources.

Therefore for WBAN, separate security methods should be proposed. Recently many symmetric key cryptography security methods introduced for WBAN security. These methods dealing with issues of limited resources in WBAN sensors, however suffered from the problems such as delaying symmetric keys disclosure and relatively weak security approach resulted as this method is failed to achieve security of data against the physical attacks. Therefore researchers claiming that symmetric key algorithms are better for WBAN in order to provide the security for data that is sent to control node. In addition to this, random numbers are used in security methods which are generated by biometrics. Such researchers believe that person's biometric parameters are efficient for securing WBAN as they can achieve strong security with less communication overhead. In WBAN, as wireless nodes are required to interconnect among each other, this can build the secure data communication route which is unavailable from all other wireless networks. Therefore in WBAN, it is assumed that if WBAN build properly, then network itself provides the secure information communication in WBAN, as other networks may require software and hardware's to achieve security. Such methods are collectively called as Biometric-based Security methods [1] [3].

Apart from this, recent methods are presented for efficient encryption technique. These methods uses ECC (elliptic curve cryptography) [3] for securing the patients information in WBAN. This technique also uses the symmetric key methods like AES, DES etc. for encrypting and decryption information related patients health. Along with this ECC method is used to execute processes like distribution of keys, updating of keys and revocation keys as and when required. TinySec is another security approach for WBAN which is resulted in efficient communication, less memory overhead, less computation overhead etc. There are two security options provided by TinySec protocol such as Tinysec-AE (authenticated encryption) and TinySec-Auth (authentication only).

There is different network security solutions proposed so far, but those are applicable to specific WBAN applications due to different constraints of WBAN sensor nodes. The goal of this paper is to take survey of such security methods presented for WBAN with its advantages and disadvantages along with its comparative analysis. Reminder of paper is composed of below sections. Section II, discussing the fundamental security requirements in a WBAN which are vital to study for security solutions. Section III, discussing the different methods of security in WBAN. Section IV, will discuss the comparative analysis of recent security methods. Finally conclusion is presented in section V.

II. FUNDAMENTAL SECURITY REQUIREMENT's IN WBAN

Data Confidentiality: This is basic requirement to protect data from damage. In medical applications, the Body node forwards the sensitive information such as health status of the patients. To make it more confidential the data are encoded using the secret key and then shared among Body node and Coordinator.

Data Authentication: For both medical and nonmedical applications, data authentication is important. It is necessary for every Body node and BNC to check whether the sensor nodes sending the data is trusted and not affected by any attacker. The data authentication is acquired using the symmetric techniques in WBANs.

***Data Integrity*:** The medical data of the patient can be changed by an adversary while transmitting through insecure WBAN. The attacker can change the patient information before reaching the coordinator. The data authentication helps in attaining the data integrity.

Data Freshness: This property ensures that data is new. This means ensuring that data frames are well ordered and not used again.

Non repudiation: The root of patient related data cannot be rejected by the source that generated it. It is the sender of a message cannot later reject having sent the message and the recipient also cannot deny having received the message.

Availability: The information about the patients is available to the physician all times. By disabling ECG node, the invader targets the WBAN's availability which results in loss of life.

III. WBAN SECURITY TECHNIQUES

A] Biometric Based Security Methods

The biometric approach is nothing but the process of automatic recognition or detection of human being by using her or his physiological features. This method utilizes the intrinsic parameters of human body for identity authentication in order to secure the cipher key distribution inside of WBAN data communications.

In [4], author Lin yao et al. proposed method for security in WBAN by using biometric key for protecting the integrity and confidentiality of private health data. This method is introduced to solve the privacy and security problems in body area networks. This approach aims for generation and distribution of the session key among the coordinator and biosensor secretly. The proposed approach in this paper is purely based on concepts of biometric encryption. The electrocardiogram (ECG) signal of human body is utilized for performing the task of authentication among the CU and biosensor. Here ECG is used by observing the human body conditions which is flexible and complex. Also physiological conditions of human body are changing over time randomly and not fixed. ECG biometric parameter is most commonly used for in many security methods. ECG information is collected and then used in different types of recognition applications.

In [5], author Sofia.Najwa.Ramli et al. introduced the new security method for transmitting the health information securely based on human body biometric parameters in WBAN. In this method author selected the ECG feature which is utilized as biometric key for the process of data authentication method within the WBAN networks. Hence by this security approach of WBAN, patients information can only be personally detected and derived and not mixing up the information of one patient with another. For successful data authentication, there is requirement of statistical results in order to prove the every ECG signals uniqueness. In addition to this, process of encryption is included by extracting the biometric parameter treated as secrete key for information transmission in WBAN.
In [6], author P.Abina et al. proposed the novel method for biometric based security approach in WBAN by introducing the new scheme for key agreement known as ECG-IJS (Improved Jules Sudan). This method uses the ECG physiological for deriving the cryptographic keys. By using this approach, earlier key distribution is not needed as the implementation of secure sensor nodes communication is done by plug and play manner. Secret keys are generated based on ECG features and used in data communications. The secrete key which is generated from proposed scheme is unique as well as different from each patient in WBAN.
The advantage of this method is that, it needs less computational needs with less time for generated the secrete keys. Compared to other techniques, this approach performs well for FRR (false reject ratio) and FAR (false acceptance rate).
In [7], author Shreyas S.Tote et al. proposed another biometric feature based security method for WBAN communication. The goal of this method is to propose security solution for secure health data communications based on human body biometric features in WBAN. In this method patients ECG signal is used as the biometric key for performing the task of data authentication inside the WBAN. The patient's signals are sensed personally and not mixed with other patient's information for secure communication.

B] Elliptic Curve Cryptography Method

Elliptic Curve Cryptography (ECC) is a public key cryptography technique in which ECC public key is a point on the curve. Random number is treated as private key. The public key is obtained by multiplication of generator point G of the curve and private key. The ECC domain parameter is a generator point G, curve features 'a' and 'b' and few constant values. The benefit of using ECC method is that it needs small key size as compared other security methods like RSA, DSA etc. Due to its small key length, it takes less time, less storage, less computation costs and hence gaining many researchers attention since from last few years for security applications especially in applications where resources are having constraint's like WBAN. In [8], author presented the comparative study between ECC method and RSA method on 8-bit computer system. In this paper, ECC method was outperforming existing RSA method.
In [9], author proposed the SCK (self-certified keys) and ECC based security approach by generating the asymmetric keys for data authentication. In this approach KDC is used for the process of key generation. ECC approach utilizes SNAP protocol to generate the pair wise keys among the gateway and nodes. Every sensor node has biometric device to authenticate the patient in WBAN. The shared secrete key is utilized for secure communication with network base station. However, this approach does not generating any kind of group keys. There are many works done using the ECC and asymmetric key based approach for secure solutions. This approach is best for resource constrained networks.
The next attempts of using ECC method for WBAN network security is presented in [10] by author Young Sil Lee. Author proposed the efficient scheme for encryption using the ECC in order to secure health related information in WBANs. The novelty in this method is that author used ECC with symmetric key cryptography method rather than asymmetric key cryptography. This approach used the symmetric key cryptography algorithm such as DES, AES etc. for secret data communication in the WBAN systems. Due to the use of symmetric key approach, it saves communication costs, memory, storage and time of generating the keys in WBAN.

C] TinySec Method

In [11], author uses the TinySec technique for information security. TinySec approach is used in WBAN for sensitive data security due to its characteristics of providing the authentication, confidentiality and integrity with less memory utilization and less energy consumption. This drawback of this approach of security is that it is heavily depends on network based key distribution technique therefore if single sensor node is compromised then entire WBAN network will compromised.
Basically TinsySec [11] is nothing but the link layer security approach for WSNs and it is part of release of TinyOS. The secure key is generated by encrypting data and uses the group key that is shared among all sensor nodes and then computes the MAC (message authentication code) for entire data. The limitation of this approach is its dependency on single key which is shared among all sensor nodes in network before deployment. This approach is just considered as basic for network security. Hence this method is not generally referred for WBAN security.

D] Hardware Based Encryption

Due to the limitation of TinySec, the alternative approach was introduced by few researchers in which hardware encryption over the ChipCon 2420 ZigBee complaint RF Transceiver chip. This chip is used to perform encryption as it is most widely used radio chip on sensor nodes. Using AES 128-bits based encryption approach; the chip can execute the WBAN security tasks with inclusion of CTR (counter) mode cryptography operations, CBC-MAC authentication as well as CCM encryption with authentication. This approach can also be used to execute the stand along and plain text based encryption using 128-bit blocks.

In [12], the group of WBAN adopted this security solution in their WBAN network systems in which personal server system distribute the encryption key information with all sensor nodes within WBAN while initialization of WBAN session. In [13], such hardware encryption based method if adopted in method called ALARM-NET. The drawback of this technique is that this technique not supporting the AES decryption, therefore the data transmitted by source node is not addressed or accessed by intermediate sensor nodes if it is required for any special purposes. The decryption can only be executed at sink side. Another limitation of this approach is that it is depend on particular platform. Therefore different networks required to design different security solutions.

IV. SUMMARY

In this section we compare all four different approaches of WBAN security as discussed above in this paper with their advantages and disadvantages.

Table 1: **C**omparative Study of Different WBAN Security Schemes

Method Name	FRR and FAR Performance	Advantage	Disadvantage
TinySec Method	Worst	This is basic security method hence easy to deploy and understand	Network dependent key distribution as all sensor nodes sharing single key. Less security
Hardware Encryption Method	Average	This is best alternative to TinySec Method	It is platform dependent. AES decryption is not supported.
ECC Based Method	Good	It requires less memory and energy requirements	There is still scope of improve the network security.
Biometric Based Method	Best	This method requires less memory and energy resources while providing strong network security.	Not identified

Table 2: Comparison Based on Fundamental Security Requirements in WBAN

Technique	Confidentiality	Authentication	Integrity	Data freshness	Non repudiation	Energy consumed	
TinySec	Network wide key	achieved	Yes	No	Achieved due to biokey	TinySec-Auth	0.000165
						TinySec-AE	0.0000176
Hardware Encryption	AES	achieved	Yes	Yes	Achieved due to digital signature	25.82 µ J	
ECC	Private key	achieved	Yes	Yes	No	0.24mJ	
Biometric	Symmetric key	achieved	Yes	Yes	No	4592 µ J	

V. CONCLUSION

The idea of remote monitoring of patients in healthcare system is derived from growing advances in WSNs. During this paper we have discussed the various security concerns while using WSN network with medical or health care systems. The success and reliability of such WBAN networks is depending on use of efficient and effective network security solution for protecting the patient's sensitive information. There are four core different types of security solutions we discussed in this paper. We summarized their performances in terms of FRR, FAR, advantages and disadvantages and security requirements. From all discussed security solutions for WBAN systems, biometric based security techniques are better and efficient as compared to other methods.

REFERENCES

[1] P.Abina, K.Dhivyakala, L.Suganya, S.Mary Praveena, "Biometric Authentication System for Body Area Network", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, March 2014.

[2] Tassos Dimitriou, Krontiris Ioannis, "Security Issues in Biomedical Wireless Sensor Networks", Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL '08. First International Symposium on Date of Conference: 25-28 Oct. 2008.

[3] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber, "SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network)", International Journal of Advanced Science and Technology Vol. 12, November, 2009.

[4] Lin.Yao.Bing,"A Biometric Key Establishment Protocol for Body Area Networks", IJDSN, 2011.

[5] Sofia.Najwa.Ramli "A Biometric-Based Security for Data Authentication in Wireless Body Area Network (WBAN)", IEEE, 2013.

[6] P.Abina "Biometric Authentication System for Body Area Network", IEEE 2014.

[7] Shreyas S.Tote "Data Authentication in Wireless Body Area Network (WBAN) Using A Biometric-Based Security", IJREST 2015.

[8] N. Gura, A. Patel, A. Wander, H. Eberle and S. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit CPUs", Cryptographic hardware and embedded systems-CHES 2004: 6th International workshop, Cambridge, MA, USA, August 11-13, 2004: proceedings, Springer-Verlag New York Inc., vol. 6, (2004), pp. 119.

[9] C. Jiang, B. Li and H. Xu, "An efficient scheme for user authentication in wireless sensor networks", Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, Niagara Falls, Canada, (2007).

[10] Young Sil Lee, Esko Alasaarela and Hoon Jae Lee, "An Efficient Encryption Scheme using Elliptic Curve Cryptography (ECC) with Symmetric Algorithm for Healthcare System", International Journal of Security and Its Applications Vol.8, No.3 (2014), pp.63.

[11] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), November 2004, pp. 162–175.

[12] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov, "Interoperability and security in wireless body area network infrastructures," in Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2005, pp. 3837–3840.

[13] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," Department of Computer Science, University of Virginia, Tech. Rep. CS-2006-1, 2006.

