ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.11

An Efficient Authentication & Light Weight Security in WBAN

L.Prema[1], L.Devi (Ph.D)[2]
M.Phil, Student[1], Associate Professor[2]
Department of Computer Science
Muthayammal Arts and Science College, Nammakal, Tamilnadu, India

Abstract:
Low computational power of wireless sensors and the multicast form of transmission exhibited by WBAN make it susceptible to several security and privacy issues. Due to these, many security and privacy preservation approaches had been proposed to secure and preserve privacy of wearable WBAN systems. However, the inherent low computational power which characterizes WBAN nodes made most of these approaches inefficient for the networks. This paper proposes a lightweight two-way but coordinated perturbation scheme for obfuscating both the identities and measurements of the sensor in the wearable WBAN system. The coordinated generation of perturbs eliminates security and privacy problems associated with reconstruction by the receiver. The propose scheme was analysed and its estimated speed was compared with five state of the art schemes proposed in. The results showed that the scheme outperforms these schemes in terms of computational overhead. The scheme was also evaluated by simulating the scheme using digital ECG sensors as WBAN nodes. The simulation results not only confirm the estimated speed but also showed that the scheme left no semantic pattern in the transmitted data.

Keywords: Wireless Body area network; Electro cardiogram signal.

I.INTRODUCTION

Acquisition of accurate health knowledge of human anatomy and condition is the major operation that helps health-care professionals or doctors in handling health related issues of their patients. Most of the major health complications can easily be averted if useful information is readily available for health-cares professionals. The wireless body area network has emerged as a new technology for healthcare delivery. It monitors and communicates patient's vital body parameters and movements through small wearable or implantable sensors over short-range wireless communication. Although, WBAN easily solves the problem of timing and non-availability of patients health information in health-care system, however wireless communication is not secured. This subjects health information to different forms of attacks. Preservation of identity and securing data transfer from the user to the server or sensors data stored in the server are the major challenges of WBAN. Examples of these security challenges are snooping, routing attacks and spoofing which affect the data confidentiality, data integrity, data availability and privacy of the sensor node.

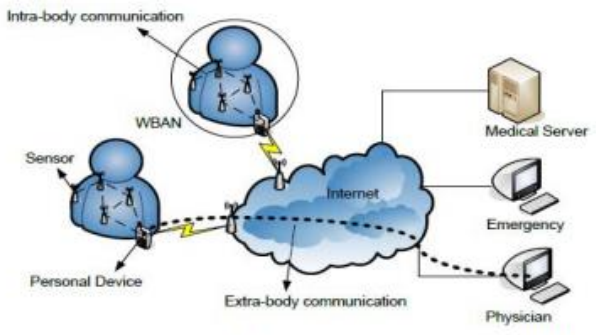


Figure 1. Example of intra-body and extra-body communication in a WBAN

The emergency data have the highest priority during the data transfer operation. Several schemes had been proposed to secure health information in resources constraint WBAN. However, most of these schemes are either network specific or based on public or private key infrastructure which requires considerable memory and com- Several schemes had been proposed to secure health information in resources constraint WBAN. However, most of these schemes are either network specific or based on public or private key infrastructure which requires considerable memory and com-putational resources. These make them unsuitable for resources constraint network such as WBAN. In view of this, a lightweight but efficient security and privacy mechanism is required for WBANs routing protocol in order to protect sensitive data and wearer privacy during data transfer.

II.RELATED WORK

The authors proposed a lightweight and robust security-aware data assist data transmission protocol for M-health systems by using a certificate less generalized signcryption to secure data their certifcateless generalized signcryption scheme consists of three cryptographic primitives: signcryption, signature, or encryption, within one single algorithm. In [36], authors proposed a healthcare system framework that collected medical data from WBANs transmits them through an extensive wireless sensor network infrastructure and finally publishes them into wireless personal area networks (WPANs) via a gateway. They engaged the groups of send-receive model scheme to implement both key distribution and secure data transmission, and homomorphic encryption based on matrix to ensure privacy. In public key encryption two keys are used for In order to reduce the computation cost incurred by some WBAN schemes, a certificate less public auditing scheme with privacy preserving and revocation in group sharing data model was proposed in. Although their scheme supports properties of multi-user sharing data, public auditing, forward security and revocation of illegal group members. However, the amount of computation cost required will overwhelm WBAN. Another lightweight scheme for WBAN was proposed in. In this work, authors presented a secure

lightweight and energy efficient authentication scheme called BANZKP. The scheme was based on cryptographic protocol, Zero Knowledge Proof (ZKP) and a commitment scheme. They used ZKP to confirm the identity of the sensor nodes while the commitment scheme was used to deal with replay attacks. Information retrieval in WBAN is another issues which are being addressed to improve the operations in healthy. Attribute-based encryption is in two forms: Key Policy Attribute Based Encryption (KP-ABE) and Ciphertext-policy attribute-based encryption (CP-ABE). For data in the cloud like Patient Health Record (PHR), CP-ABE is the most suitable as patient can decide an access policy using attributes and encrypts data based on the corresponding attributes. In, the authors proposed a patient-centric and fine-grained data access control in multi-owner settings. To achieve fine-grained and access control control of PHR, they implemented KP-ABE to encrypt patient's PHR.. Also, to achieve reduced key distribution problems, they divided the system into multiple security domains with each domain manages only a small number of users. Their revocation scheme involves computing a re-key by updating the ciphertexts of all the affected attributes. However, the use of KP-ABE results in higher key management complexity and cost of computation because users have to posses many attributes from different authorities to guarantee security of PHR, thus unfit to secure WBAN. Ramesh et al in [17] also proposed multi-authority scheme based CP-ABE with attribute revocation for cloud data storage.

III.METHODOLOGY

Due to the sensitive and broadcast nature of WBAN face the lots of threats. Outside attackers can eavesdrop all messages, modify messages, replay old messages. It was not usually to fix the fixed keys for data transmission between the BAN nodes and also BAN nodes and Mobile .Because the single encryption key will provide a large amount of cipher text for hackers to crack the data. Compared to the wireless sensor networks, it is easier to launch attacks in WBAN .To address above challenges this paper makes the following contribution. We are developing the WBAN with wireless communication facility. We have built the following wearable sensors. The secure one way hash function can be used for generating the keys. A one way hash function take arbitrary length input data and produce fixed key values. It is challenging to securely deliver the data from the sensor head to mobile nodes. In each WBAN, exactly one sensor is chosen as cluster head. The cluster head collect all information and transfer it to mobile nodes. We have used the skipjack for securing data between cluster head and mobile nodes.

1. Body Area Network Implementation for Healthcare

Due to the sensitive and broadcast nature of WBAN face the lots of threats. Outside attackers can eavesdrop all messages, modify messages, replay old messages. It was not usually to fix the fixed keys for data transmission between the BAN nodes and also BAN nodes and Mobile .Because the single encryption key will provide a large amount of cipher text for hackers to crack the data. Compared to the wireless sensor networks, it is easier to launch attacks in WBAN .To address above challenges this paper makes the following contribution. We are developing the WBAN with wireless communication facility. We have built the following wearable sensors.

2. ECG Sensor

ECG works mostly by detecting and amplifying the tiny electrical changes on the skin that are caused when the heart muscle "depolarizes" during each heartbeat. At rest, each heart muscle cell has a charge across its outer wall. Reducing this charge towards zero is called de-polarization, which activates the mechanisms in the cell that cause it to contract.

3. Pulse Oximeter

Pulse oximetry is a non-invasive method allowing the monitoring of the saturation of a patient's hemoglobin. A sensor is placed on a thin part of the patient's body, usually a fingertip or earlobe, or in the case of an infant, across a foot. Light of two wavelengths is passed through of the absorbance due to the pulsing arterial blood alone, excluding venous blood, skin, bone, muscle, fat

4. Temperature Sensor

The temperature sensor in which some physical change occurs with temperature, plus some means of converting this physical change into a numerical value (e.g. the visible scale that is marked on a mercury-inglass thermometer. We have made the low cost RF board which has the following features. The heart of the RF board is micro controller and radio transceiver. The following fig 1 describes the general WBAN architecture. Our sensor applications hardware consist of temperature sensor, ECG sensor, pulse oximeter. The heart of our RF board is micro controller. The RF board is attached to the sensors and we uses CC2430 as Texas instrument as RF and MCU. The CC2430 is small and low power consumption ships for zigbee communication. The sensor nodes are collecting the signals from human body. The filtering process is used to increase the signal strength and also reduce the noise from the signal. Then an analog to digital conversion is applied to the signal for conversion of analog to digital signal. The digital signal is stored in micro controller. The micro controller will transmit the data via radio transceiver. Three sensor nodes are built on the common PCB board. The 80bit key is split into 10 bytes like k0 to k9. Each round takes 4 bytes use as its sub key. The skipjack A rounds and B rounds closely related to their internal structure. The structure of round B is inverse of round A. To decrypt a cipher text, it reverses the key schedule and the order of the rounds as well as all the arrows in the feistel structure. The following fig 6 shows the secure data transmission between the sensor nodes and mobile device or laptop. The sender information is encrypted by using skipjack algorithm and then calculates the hash value for key and sensor data. These results sent it to the receiver side. The receiver again calculates the hash value for encrypted message. If both values are equals, then only the authentication is successful

5. Security

The secure one way hash function can be used for generating the keys. A one way hash function take arbitrary length input data and produce fixed key values. It is challenging to securely deliver the data from the sensor head to mobile nodes. In each WBAN, exactly one sensor is chosen as cluster head. The cluster head collect all information and transfer it to mobile nodes. We have used the skipjack for securing data between cluster head and mobile nodes.

IV. EXPERIMENTAL SETUP

Qualitative Security Threats Assessment As the system is in laboratory scale implementation and testing, we conduct risk assessment with the assumption of user's activities of daily living while the user is using the device for the remote healthcare monitoring service consisting of data collection, processing, transmission, storing and sharing. Two of the

major security threats are caused by the user's daily use and data sharing. The communication links of IEEE 802.15.4, IEEE 802.11g, and Internet protocol are also regarded as vulnerable points of security threats. When the user has a wireless device in his/her Wireless Body Area Network (WBAN), the vital signals are being sensed by the sensor transmission node, the vital signals can be targeted when intruders synchronize the wireless bandwidth using IEEE 802.15.4 bandwidth as an unauthorized source. It causes a confidentiality issue and an availability issue. When the intruders alter the vital signals in the sensor transmission node, it will cause misinterpretation of the user's vital signals by the automated analysis software tool in the remote web portal system and/or by the health professionals as it causes an integrity issue.

Proposed Security Features The features for security and privacy in transferring data consists of monitoring human body signals needs Authentication, integrity, access control, non-repudiation and encryption features. For the security features of the system, we need to adopt the concept of scalability and compatibility by adopting the Elliptic Curve Cryptographic algorithm, Mutual Authentication and Group key Agreement protocols. It should include the security features integrated into the cryptographic protocol and the data structure. The verification of security features in the system will also have to assess power consumption and computing resources.

Enabling Technology Resolving Security Threats We reviewed security perspectives for the remote health monitoring system which offers an inexpensive, yet flexible and scalable, wireless platform to deliver, train and monitor data provided by biosensors. For sustaining the high level of security in all the applications in the system, we consider importing cryptographic functions with a plug and-play (PnP) gadget that can be setup quickly by a non-professional and the pervasive monitoring becomes possible without interruption in patient's daily routines. For the strong level of security, we need to implement Advanced Encryption Standards (AES) 128 cryptographic algorithm in the hardware accelerator of the user's sensor node module. There is a new block cipher suitable for low resource device in the research community and one of them is HIGHT (aka high security and light weight) block cipher with 64-bit block size and 128 bit key size. For the cryptographic algorithm of TinyOS, elliptic curve cryptographic algorithm, ECIES, and key distribution protocol, ECDH, and digital signature algorithm, ECDSA, have been introduced. With these cryptographic algorithms, we need to investigate and perform feasibility research on real world implementation and field testing of security features in the remote health monitoring system.

Cryptography As wireless body area sensor networks alter sensitive physiological info, sturdy cryptographic functions are unit preponderating necessities for developing any secure attention application. These cryptographic functions give patient privacy and security against several malicious attacks.. Further, the selection of cryptography system depends on the computation and communication capability of the sensor nodes. Some argue that asymmetric crypto systems are typically too high-priced for medical sensors and interchangeable crypto systems don't seem to be versatile enough.

Key Management Key management protocols are measure basic necessities to develop a secure application. These protocols are used to set up and distribute varied forms of cryptographic keys to nodes within the network. Generally, there are three styles of key management protocols, namely, trusty server, key pre-distribution and self imposing.

Secure Routing

In home care or disaster eventualities sensor devices might require sending their data to alternative devices outside their immediate radio vary. Therefore, routing and message forwarding could be a crucial service for end-to-end communication. So far, several of routing protocols are projected for sensor networks; however none of them are designed with strong security as a goal. Karlof-Wagner mentioned the actual fact that routing protocols suffer from several security vulnerabilities, like associate degree offender may launch denial-of-service attacks on the routing protocol.

Resilience to Node Capture

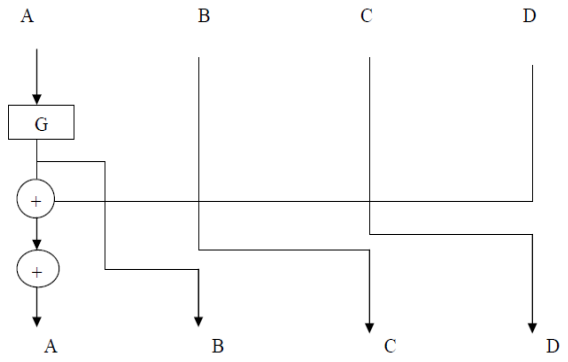
Resilience against node capture is one in all the foremost difficult issues in sensor networks. In real time healthcare applications, the medical sensors are placed on a patient's body, whereas, the environmental sensors are placed on hospital premises (e.g., ward room, operation area etc.) which can be simply accessible to attackers. Thus, an attacker might be able to capture a sensor node, get its cryptanalytic info and alter the sensor programming consequently. Later, he/she will place the compromised node into the network, which may endanger application success. The current cryptographic functions (i.e., node authentication and identification) might discover and defend against node compromised attacks to a point, however these compromised node attacks can't be detected instantly that could be a massive issue for healthcare application.

Trust Management Trust signifies the mutual association of any two trustworthy nodes (i.e., sensor node and information aggregator node), that are sharing their data. In trust is outlined as "the degree to that a node ought to be trustworthy, secure, or reliable throughout any interaction with the node". Boukerc he-Ren, evaluated the trust for mobile healthcare system.

Secure Localization WBANs facilitate mobility for patient's comfort, thus patient location estimations are required for the success of healthcare applications. Since, medical sensors' sense physiological information of a personal, they additionally ought to report the patient's location to a far off server. As a result, medical sensors need to remember of patient location, i.e., referred to as localization. In the authors mentioned localization systems that were divided into: distance/angle estimation, position computation and localization algorithms, and more, they mentioned attacks on localization.

Data Security

The wireless communication and sensor technologies have provided lot of benefits still there are many problems about the security and privacy in WBAN. Security issues in WBAN are very important. Because we need to protect the very sensitive medical information from unauthorized users. We have developed the low cost and low energy, low overhead method for securing the data. The existing conventional security methods are not suitable for resource constrained sensor networks. The skipjack algorithm most appropriate for sensor network.



Evaluation Measures

The A rounds and B rounds are described here:

A(a ,b ,c ,d) = (d +Gk(a)+counter ,Gk(a),b , c) ,

B(a ,b ,c ,d) = (d ,Gk(a), a +b + counter , c)

The Gk box takes 16 bit input and 4 byte sub key. For each round 32 bit sub key is derived from 80 bit key. The 80 bit key is split into 10 bytes like k0 to k9. Each round uses 32 bit key as sub key. The first round uses k0… k3, the second round uses k4,…,k7 and the third round uses k8,k9,k0,k1. We have described the design procedure and results on tele-healthcare in nursing homes through wireless sensor networks. Our research in this field included medical sensor design, signal transmission, medical privacy and security and so on. Our results showed the feasibility of applying wireless sensor networking to medical monitoring anytime and anywhere. The adversaries able to eavesdrop all information within BAN. The proposed scheme is to keep data confidentiality and authenticity. Our future work is to build a larger-scale networking system with more lightweight security schemes. Here we analyze the security of our proposed algorithm. Encryption and decryption are performed in sender and receiver side. The adversary eavesdrops on information from sensor nodes. The proposed algorithm encrypts all data before the data transmission .So, the adversary not able to capture the information. The skipjack was able to provide an encryption time of 25 µs per byte. The AES was also provide an encryption time of 50 µs per byte. The RC5 had an average encryption time of 33 µs per byte. The skipjack was also best algorithm in terms of memory .Because it needed only average 2600 bytes of RAM. The other algorithms needed 8000 bytes. The following fig 8 shows the average encryption time of various algorithms. We see that AES require more encryption time than skipjack. The fig 9 shows the amount of storage needed for different algorithms

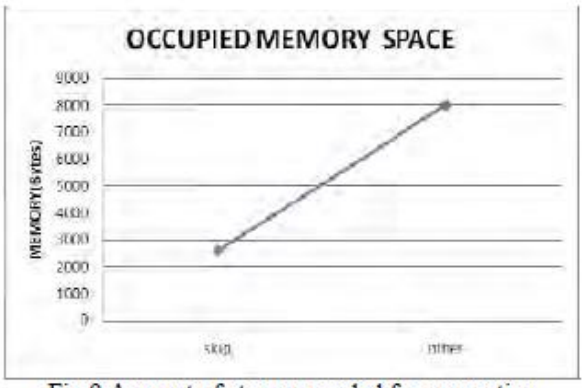


Fig 9 Amount of storage needed for encryption

V.CONCLUSION

The secure communication within the BAN is required to keep the patient's privacy and security. In this paper, we present skipjack algorithm in which security and privacy is to be maintained in authenticated manner. Our major contributions in this paper include 1) Hash based authentication approach in both sender and receiver side 2) Skipjack algorithm for secures data transmission. Our studies show that the proposed scheme is a light weight and energy efficient scheme. We provided the detailed discussion on privacy and security in health care applications. We have implemented the wireless healthcare monitoring system and demonstrated the proposed model is more practical. Our results showed the feasibility of applying wireless sensor networking to medical monitoring anytime and anywhere. Our future work is to build a larger-scale networking system with more lightweight security schemes. WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. It brings out a replacement set of challenges in terms of sensor deployment and density, energy potency, security and privacy and wireless technology. In this paper, we've reviewed the present development on Wireless Body Area Network and that we targeted in security problems faced by this technology. During this paper, we discussed the security attacks and requirements in WBAN. We presented the existing security mechanisms in WBAN. In this paper, we also presented the difference between WBAN and WSN.

VI. REFERENCES

[1]. Bagga and Baldwin. 1998. Entity-Based Cross- Document Coreferencing Using the Vector Spcae Model. In Proceedings of HLT/ACL.

[2]. Gideon S. Mann and David Yarowsky. 2003. Unsupervised Personal Name Disambiguation. in Proceedings of CONIL.

[3]. Michael Ben Fleishman. 2004. Multi-Document Person Name Resolution. in Proceedings of ACL.

[4]. Ron Bekkerman and Andrew McCallum. 2005. Disambiguating Web Appearances of People in a Social Network. in Proceedings of WWW.

[5]. Xianpei Han and Jun Zhao. 2009. Named Entity Disam biguationby Leveraging Wikipedia Semantic Knowledge. in Proceedings of CIKM.

[6]. David Milne and Ian H. Witten. 2008. Learning to Link with Wikipedia. in Proceedings of CIKM.

[7]. T. Zhang, K. Liu, and J. Zhao, "Cross lingual entity linking with bilingual topic model," in IJCAI, 2013, pp. 2218–2224.

[8]. D. Nadeau and S. Sekine, "A survey of named entity recognition and classification," Lingvisticae Investigationes, vol. 30, no. 1, pp. 3–26, Jan. 2007.

[9]. J. R. Finkel, T. Grenager, and C. Manning, "Incorporating non-local information into information extraction systems by gibbs sampling," in ACL, 2005, pp. 363–370.

[10]. A. Mikheev, M. Moens, and C. Grover, "Named entity recognition without gazetteers," in EACL, 1999, pp. 1–8.

[11]. D. Klein, J. Smarr, H. Nguyen, and C. D. Manning, "Named entity recognition with character-level models," in CONLL, 2003, pp. 180–183.

[12]. S. Geman and D. Geman, “Stochastic relaxation, gibbs distributions, and the bayesian restoration of images,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 6, no. 6, pp. 721–741, Nov. 1984.

[13]. S. Guo, M.-W. Chang, and E. Kiciman, “To link or not to link? a study on end-to-end tweet entity linking,” in NAACL, 2013.

[14]. A. Sil and A. Yates, “Re-ranking for joint named-entity recognition and linking,” in CIKM, 2013, pp. 2369–2374.

[15]. K. Q. Pu, O. Hassanzadeh, R. Drake, and R. J. Miller, “Online annotation of text streams with structured entities,” in CIKM, 2010, pp. 29–38.

[16]. A. Bagga and B. Baldwin, “Entity-based cross-document coreferencing using vector space model,” in COLING, 1998, pp. 79–85.

[17]. G. S. Mann and D. Yarowsky, “Unsupervised personal name disambiguation,” in CONLL, 2003, pp. 33–40.

[18]. T. Lin, Mausam, and O. Etzioni, “Entity linking at web scale,” in AKBC-WEKEX, 2012, pp. 84–88.

[19]. N. Nakashole, G. Weikum, and F. Suchanek, “Patty: a taxonomy of relational patterns with semantic types,” in EMNLPCoNLL, 2012, pp. 1135–1145.

[20]. J. Volz, C. Bizer, M. Gaedke, and G. Kobilarov, “Discovering and maintaining links on the web of data,” in ISWC, 2009, pp. 650–665.