ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks

M.Vamshi Krishna
Gokaraju Rangaraju Institute of Engineering and Technology.

Guide: K.Nagaja
Gokaraju Rangaraju Institute of Engineering and Technology.

ABSTRACT:

A body sensor network (BSN) is a wireless network of biosensors and a local processing unit, which is commonly referred to as the personal wireless hub (PWH). Personal health information (PHI) is collected by biosensors and delivered to the PWH before it is forwarded to the remote healthcare center for further processing. In a BSN, it is critical to only admit eligible biosensors and PWH into the network. Also, securing the transmission from each biosensor to PWH is essential not only for ensuring safety of PHI delivery, but also for preserving the privacy of PHI.

In this paper, we present the design, implementation, and evaluation of a secure network admission and transmission subsystem based on a polynomial-based authentication scheme. The procedures in this subsystem to establish keys for each biosensor are communication efficient and energy efficient. Moreover, based on the observation that an adversary eavesdropping in a BSN faces inevitable channel errors, we propose to exploit the adversary's uncertainty regarding the PHI transmission to update the individual key dynamically and improve key secrecy.

1. INTRODUCTION:

Recently, with the rapid development in biosensors and wireless communication technologies (e.g., Bluetooth and Zigbee), wireless body sensor networks (BSNs) (also called body area networks or medical sensor networks) have emerged as a promising technique for pervasive monitoring of patients' personal health information (PHI) . Instead of being measured face-to-face, with BSNs, patients' PHI can be monitored remotely, continuously, and in real time, and then processed and transferred to healthcare centers. A BSN is a wireless network of mainly implanted or wearable biosensors designed to deliver PHI to a local processing unit (e.g., tablet PC, laptop PC, and Smartphone), which is referred to as the personal wireless hub (PWH). Security and privacy for a BSN is very important, because the data collected are directly associated with a particular patient, which play a critical role in medical diagnosis and treatment. Due to the open and dynamic nature of BSNs, they are subject to various cyber attacks such as malicious modification. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments.

If patients' privacy is not strongly protected, their health data can be misused and the public acceptance of BSN is significantly hindered. Therefore, BSN applications must meet a set of mandatory privacy requirements of healthcare alliances such as HITRUST and legal directives such as those adopted in the U.S. and Europe . Ensuring security and privacy in BSNs is important for all walks of life]. For an ordinary patient, his/her medical sensor data may be useful to some parties such as insurance companies. An adversary may profit financially by selling these data obtained through eavesdropping on the BSN.

For a patient with an important status, such as a country's top administrator, an adversary may target to harm him physically by misreporting or spoofing his/her medical sensor data, resulting in improper diagnosis and/or treatment. Also, hacking the information transmitted in a wireless BSN might be much easier than hacking the information collected at a server due to the open and dynamic nature of a BSN. More importantly, compared to a server, physical compromise of a biosensor node is much easier.

1)Secure network admission:

It restricts network admission only to eligible PWHs and biosensors.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2) Secure transmission:

It provides confidential, authenticated, and integrity-protected transmission between each biosensor and PWH. However, designing a secure network admission and transmission protocol for BSNs is not an easy task. Generally, there are three major practical issues challenging the design. First, such a solution should take into account the rather limited memory space and computational capability available in biosensor nodes. Especially, its energy consumption should be minimal since biosensor nodes are powered by small batteries and required to operate for a long period of time. As a consequence, any security mechanism for BSNs should be carefully designed.

2: SURVEY AND BACKGROUND:

In the literature, various schemes have been proposed to address different aspects of securing BSNs. For example, recently, architecture called "SNAP" (Sensor Network for Assessment of Patients) has been proposed to address the security challenges faced by a WSN for wireless health monitoring. SNAP protects the privacy, authenticity, and integrity of medical data, with low-cost and energy-efficient mechanisms. However, we observe that the PHI from a biosensor node is transmitted to PWH in plaintext. Thus, an adversary can easily modify the PHI and/or inject polluted PHI into the network. Some researchers utilize physiological signals (e.g., heart rate interval, blood flow, and electrocardiography) obtained from the patient to enable biosensors to agree upon a pair wise symmetric key.

However, they demand that each biosensor can measure the same physiological parameter type; this assumption is rather restrictive and makes this approach not suitable for many BSN applications. However, MD5 is weak in collision resistance. Based on public key cryptography, some novel mechanisms have been proposed to ensure security of BSNs. propose to use ECC to set up symmetric keys between sensor nodes and the base station, and RC5 block cipher for the symmetric encryption/decryption for protecting data confidentiality and integrity. However, they are computation inefficient and cannot fulfill the stringent delay requirements in BSNs due to the use of the public key cryptography.

the ECC key agreement takes 7.198 s on a Tmote Sky mote, which features a 16-bit, 8-MHz MSP430 processor. In identity-based public key is used to encrypt all medical data, and the method balances security and privacy with accessibility. Also, traditional cryptographic mechanisms do not suffice given the unique characteristics of BSNs, and the fact that

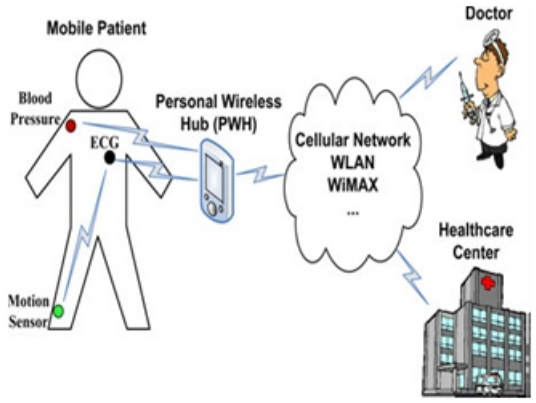


Fig.. System overview of a general BSN

BSNs are susceptible to a variety of node misbehaviors. An application-independent and distributed trust evaluation model for BSNs has been proposed to identify malicious behaviors and then exclude malicious nodes. Similar to most security schemes, trust management methods themselves can be vulnerable to attacks. To resolve this issue, an attack-resistant and lightweight trust management scheme. Although there are a lot of works about generic WSNs and MANETs security, these mechanisms are not directly applicable in BSNs due to the unique and challenging operational and security requirements of BSNs.

In particular, biosensors are limited in battery lifetime, computation, and communication capabilities, especially for implanted biosensors. For example, the random key scheme is a major class of key establishment protocols for WSNs. For the efficiency of these schemes, the probability that each node shares at least one key with a neighboring node (referred to as key-sharing probability) should be high. When the key pool size is large, each sensor needs to preload a large number of keys to achieve a high key-sharing probability. Moreover, many keys are exchanged between sensor node pairs to establish the pair wise key and, inevitably, high communication, computation, energy overhead is incurred.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Very recently, based on the random key scheme, a software design was presented for securing BSNs. Unfortunately, these requirements are too demanding for the biosensor nodes. In, a self-contained public key management scheme has been proposed for wireless ad hoc networks, in which a small number of cryptographic keys are stored offline at individual nodes before deployment. Also, to avoid the weaknesses of a public key infrastructure (PKI), as a special form of public key cryptography, identity based cryptography has been used in various areas of securing MANET. However, as described before, because of the use of the public key cryptography, they are computation inefficient, cannot fulfill the stringent delay requirements in BSNs, and are vulnerable to DoS attacks.

3. MODELS AND FEATURES:

A. Network Model:

A BSN is a multi hop wireless network of physiological and environmental monitoring biosensor nodes that are worn and/or implanted on a patient. We assume that each biosensor does not have any information about their immediate neighboring nodes in advance. A BSN is operated by the BSN administrator (e.g., the patient himself, the patient's relative, eHealth service provider, or medical practitioner). The biosensors collect PHI at regular intervals and forward it to PWH. Then, PWH transmits the aggregated PHI to the remote healthcare center over different wireless networks such as cellular, WLAN, and WiMAX. We assume that the biosensors communicate with PWH wirelessly, as wires running in a BSN will make it obtrusive.

The wireless medium is, however, not trustworthy. Note that, in this paper, we focus solely on securing the network admission and transmission within the BSN. Communication from PWH onwards can utilize conventional security mechanisms such as secure socket layer, given the considerable capabilities of the entities involved. All biosensor nodes in a BSN have limited power supply, memory space, and computational capability. Due to the constrained resources, computationally expensive and energy-intensive operations such as public key cryptography are not preferred for such nodes.

B. Adversary Model:

Due to the sensitive nature of the data BSNs collect and the broadcast nature of the wireless medium, BSNs potentially face many threats. They are imposed by either outside or inside attackers. Outside attackers can eavesdrop messages, drop messages by jamming the communication channel, modify messages, inject forged messages, or replay old messages. Regarding eavesdropping, it is generally assumed that the adversary picks up all radio communications of the nodes without any loss. However, we suggest here that this is not the case due to the following three reasons. First, the wireless channel is inherently error prone. Second, the radio quality of a biosensor is not very good (see Section VI-A) and its coverage area is small because often its transmitting power is set to a low level to maximize the battery lifetime. Yet, in order to remain undetected, the adversary needs to keep a distance from the BSN. Third, it is extremely difficult for the adversary to predict a patient's movement and follow him/her everywhere. As a result, an outside attacker inevitably suffers from information loss.

That is, the outside attacker picks up the radio communications of biosensor nodes with some loss. We refer such attackers as the eavesdrop-bounded adversaries. For inside attacks, the adversary may compromise PHW and a limited number of biosensor nodes to obtain their data and keying materials. Once a node is compromised, the adversary may discard its sensed data or packets received from other nodes. However, we assume that the BSN administrator will not be compromised. In practice, the adversary could plant a root kit or Trojan into a networked device. If the adversary can establish a link to directly retrieve unsecured data and have full control over the device, no security mechanism will work. Such a complete security breach is highly intrusive and susceptible to detection because the behavior of the victim's device is manipulated. In wireless communication environment, it is more often that the adversary steals the system secret and then uses the secret to decrypt the eavesdropped data or inject malicious messages. In such circumstances, using dynamic individual key significantly restricts the adversary. Also, we assume that the physical layer of a BSN could use techniques such as spread spectrum to prevent physical jamming attack if necessary.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

C. Unique Features and Application Requirements of BSNs:

1) Data Rate: Many MANETs and WSNs are employed to monitor events which often happen at irregular interval. On the other hand, BSNs are employed for monitoring humans' physiological activities and actions, which may occur in a more periodic manner. Hence, the applications' data rates are relatively more steady.

2) Mobility: Even though a patient with a BSN may move around, all biosensor nodes in the network are static relative to the patient.

3) Effectiveness and efficiency: The signals that body sensors collect can be effectively processed to obtain reliable and accurate physiological estimations. Also, their ultra low power consumption makes their batteries long lasting.

4) Latency: This requirement is dictated by the applications and may be traded for improved security and energy consumption. However, while energy conservation is always important, replacement of batteries in BSNs nodes is much easier than in WSNs, whose nodes can be physically unreachable after deployment. Thus, it may not be necessary to maximize battery lifetime in a BSN at the expense of higher latency. Besides, compared to MANETs and generic WSNs, a BSN is a network with small-scale structure and very short range of communications. Its nodes are limited in their power, computation, communication, and memory capabilities, especially for those implanted into the body.

D) Network Admission and Transmission Control:

We propose a polynomial-based authentication scheme. Before deployment, PWH and all biosensor nodes are loaded with a unique polynomial share of the same bivariate t-degree polynomial. Once deployed, each node identifies its neighboring nodes and PWH by mutual authentication and then establishes two kinds of secret keys. The detailed description is as follows. We require that in the system initialization phase, for each BSN, the BSN administrator randomly generates a bivariate degree polynomial f(x, y) = _t i,j=0aijxiyj over a finite field Fp , where p is a large prime number, such that it has the property of f(x, y) = f(y, x).

Also, the BSN administrator keeps the bivariate t-degree polynomial secretly. At the point of deployment, each biosensor node, say Sj, is embedded with a polynomial share of f(x, y), that is, f(sidj, y) and authenticated at a secure place, where sidj indicates the identity of node Sj . In the same way, PWH is embedded with a polynomial share of f(x, y), that is, f(pidi, y), where pidi indicates the identity of PWH. PWH will broadcast pidi periodically to declare PWH service existence. Our system supports the establishment of two types of keys for each biosensor node: an individual key shared with-PWHand a pair wise key shared with its neighboring nodes. The details of establishing these keys are given as follows. When a new biosensor, say Sj , is added into the BSN, upon receiving the broadcast message pidi , node Sj computes the individual key Kj = f(sidj, pidi) by evaluating f(sidj, y) at pidi .

The individual key can be used for secure communication between node Sj and PWH. According to the data rate feature of a BSN described in Section III-C, we assume that time is divided into equal and fixed collection rounds and each biosensor collects a single data item per round. At round r, every biosensor, say Sj , generates the cipher text crj with the individual key Kj as follows: crj = E({dataj , r},Kj), h(dataj ,Kj) (1) where dataj is the collected data item by node Sj at round r. Subsequently, it delivers {sidj, pidi, crj } to PWH, where sidj is the source ID while pidi is the destination ID.

One purpose of the round index r is to prevent replay attacks. Upon receiving such a message, PWH generates the individual key Kj = f(pidi, sidj) = f(sidj, pidi) by evaluating f(pidi, y) at sidj . Then, PWH uses Kj to perform D(E({dataj , r},Kj),Kj) = {dataj , r} to decrypt the cipher text. After that, PWH uses Kj to compute h(dataj ,Kj) and then compares it with the received h(dataj ,Kj). If the result is positive, PWH believes this message is from node Sj and has never been modified by the adversary. At the same time, if this is the first message from node Sj , PWH will record the mapping< sidj,Kj > for future use. A hash value is calculated from and transmitted along with dataj .When the SHA-1 keyed hash functions is used, the corresponding hash value is 20 bytes long. In general, this kind of overhead is often not desirable in an already resource constrained BSNs. Data transmission is a costly operation in wireless networks; sending one bit over a wireless medium requires over 1000 times more energy than a single 32-bit computation.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In order to reduce the transmission overhead, we propose the use of sub keyed hash function. A sub keyed hash function only returns some bits of a hash value produced by a keyed hash function.

E) SECURITY ANALYSIS OF THE PROPOSED PROTOCOL:

We evaluate the security of the proposed system by analyzing its fulfillment of the security requirements. Secure network admission: The security proof ensures that the proposed network admission and transmission subsystem is unconditionally secure and t-collusion resistant. That is, the coalition of no more than t compromised biosensor nodes knows nothing about the pair wise key between any two noncompromised nodes. At the same time, the coalition of no more than t compromised biosensor nodes knows nothing about the initial individual key between any noncompromised biosensor node and PWH.

Because the scale of each BSN is very small (i.e., from several to tens of biosensor nodes), in our system, it is suggested that t should be equal to the total number of the biosensor nodes in a BSN. Obviously, in this case, unless all biosensor are compromised, no pairwise or individual key could be revealed by adversaries. As described in Section IV-A, it is critical for our system to restrict the network admission Packet loss rate with the distance of different lengths. PWH and biosensors, which has the knowledge of a polynomial share of the same bivariate t-degree polynomial. Secure transmission: Same as the proof of the secure network admission, in the proposed protocol, symmetric encryption and sub keyed hash function are used to ensure confidential, authenticated, and integrity protected transmission between each biosensor and PWH.

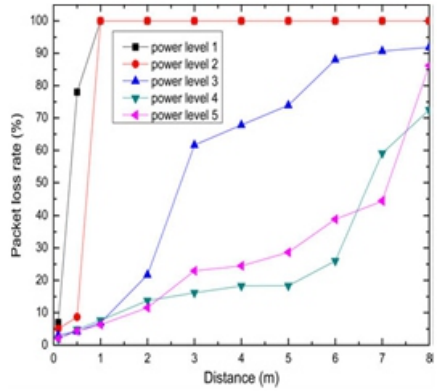


Fig.. Packet loss rate with the distance of different lengths.

4) SYSTEM ARCHITECTURE:

a) LPC2148 MICROCONTROLLER:

LPC2148 microcontroller board based on a 16-bit/32-bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combine microcontrollers with embedded high-speed flash memory ranging from 32 kB to 512 kB.8 kB to 40 kB of on-chip static RAM and 32 kB to 512 kB of on-chip flash memory; 128-bit wide interface/accelerator enables high-speed 60 MHz operation. In-System Programming (ISP/IAP) via on-chip boot loader software, single flash sector or full chip erase in 400 ms and programming of 256 B in 1 ms Embedded ICE RT and Embedded Trace interfaces offer real-time debugging with the on-chip Real Monitor software and high-speed tracing of instruction execution.

b)Zigbee Module:

The XBee/XBee-PRO RF Modules are designed to operate within the ZigBee protocol and support the unique needs of low-cost, low-power wireless sensor networks. The modules require minimal power and provide reliable delivery of data between remote devices. The modules operate within the ISM 2.4 GHz frequency band.

Features:

- High Performance, Low Cost
- Advanced Networking & Security
- Low Power
- Easy-to-Use

c) Temperature Sensor - The LM35:

The LM35 series are precision integrated-circuit temperature sensors, whose output voltage is linearly proportional to the Celsius (Centigrade) temperature

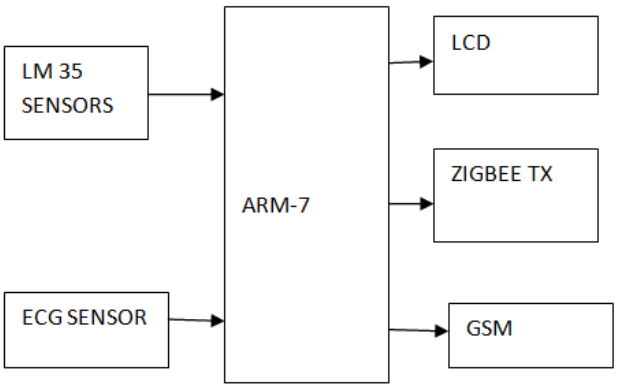
Features:

- Calibrated directly in ° Celsius (Centigrade)

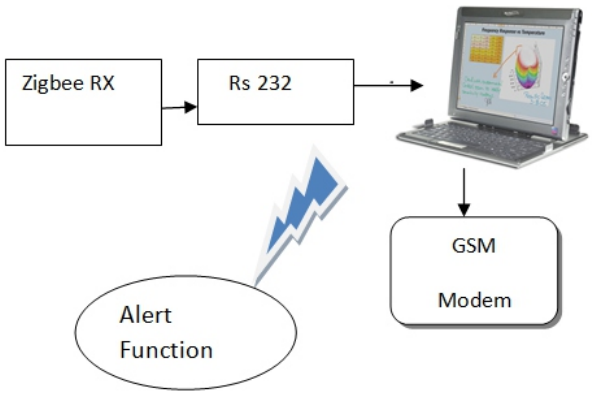
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- Linear + 10.0 mV/°C scale factor
- 0.5°C accuracy guaranteeable (at +25°C)
- Rated for full −55° to +150°C range
- Suitable for remote applications
- Low cost due to wafer-level trimming
- Operates from4 to 30 volts
- Less than 60 µA current drain
- Low self-heating, 0.08°C in still air
- Nonlinearity only ±¼°C typical
- Low impedance output, 0.1 for 1 mA load

Transmitting Section:



Monitoring Section:



e) GSM MODEM:

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz's GSM provides recommendations, not requirements.

The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS). The basic GSM network elements are shown in below figure .

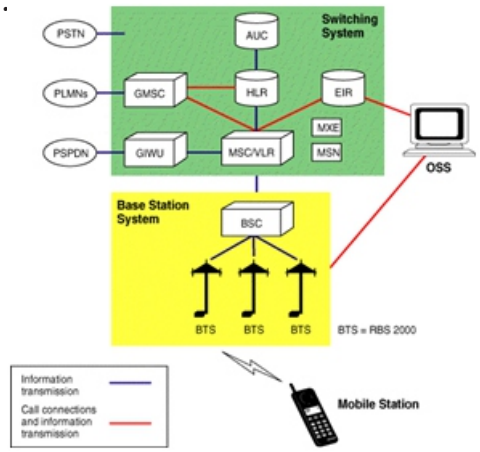


Fig: GSM Network Elements

CONCLUSION:

In this paper, we have explored the features of a BSN and then presented a novel secure and lightweight network admission and transmission protocol. Further, to reduce the computation and communication overhead, some additional mechanisms such as sub keyed hash function and the hardware-implemented AES algorithm are incorporated into the design of the proposed System. We measured the health condition of patient's health in terms of temperature and ecg values and these are transmitted to pc via zigbee and also gives a msg by using gsm.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The security analysis and experimental results have shown that our approach is feasible for real applications. Our experiments have also shown that the system overhead of the proposed protocol is affordable on resource-limited motes, which is much more efficient than the well-known approaches.

REFERENCES:

1]The US Congress. (1996). Health Insurance Portability and Accountability Act.Washington, DC.

[2] The European Parliament and the Council of the European Union, Directive 95/46/EC [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[3] K. Malasri and L.Wang, "Design and implementation of a secure wireless mote-based medical sensor network," Sensors, vol. 9, no. 8, pp. 6273–6297, 2009.
[4] C. Cordeiro and M. Patel, "Body area networking standardization: Present and future directions," in Proc. BodyNets, 2007.

[5] H.Wang and Q. Li, "Efficient implementation of public key cryptosystems on mote sensors," in Proc. Int. Conf. Inf.Commun. Security, 2006, pp. 519–528.

[6] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Security, vol. 8, no. 2, pp. 228–258, May 2005.

[7] D. He, C. Chen, S. Chan, and J. Bu, "SDRP: A secure and distributed reprogramming protocol for wireless sensor networks," IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4155–4163, Nov. 2012.

[8] W. He, Y. Huang, R. Sathyam, K. Nahrstedt, and W. Lee, "SMOCK: A scalable method of cryptographic key management for mission-critical wireless ad-hoc networks," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 140–150, Mar. 2009.

[9] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 380–400, May 2012.

[10] K. Malasri and L. Wang, "Addressing security in medical sensor networks,"in Proc. HealthNet., 2007, pp. 7–12.