A Secure Data Transmission Scheme for Body Sensor Network

Guangxia Xu[1], Yu Liu[2], Yunpeng Xiao[1], and Yanbing Liu[3]
[1] School of Software Engineering, Chongqing University of Posts and Telecom., Chongqing 400065, China.
[2] School of Communication Engineering, Chongqing University of Posts and Telecom., Chongqing 400065, China.
[3] Institute of Mobile Internet & Information Security,
Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.
Email: {xugx@cqupt.edu.cn; freefish426@hotmail.com; 651735619@qq.com; liuyb@cqupt.edu.cn}

***Abstract*—**Personal privacy has been realized as the most important security issue in wireless sensor networks. While there are much researches on privacy information protection, most of them shared the same condition that the sensing action happened anywhere at any time and few of them tackle the problem in the body sensor network (BSN). To address the problem, this paper proposes a system model according to BSN's specific features. The proposed model includes a hierarchical structure and an adversary model which originated from the traditional wireless sensor network. Based on the proposed model, an efficient green Secure Data Transmission Scheme is provided to protect users' privacy against the global eavesdropper. Next we conduct extensive simulations for proposed scheme by deploying it on the TinyOS, and compare it against a representative privacy-preserving scheme. The result shows that the scheme proposed in this paper has lower energy consumption and quicker response time, thus it fits for BSN more preferably.

***Index Terms*—**body Sensor Networks, synchronous, privacy-preserving, TinyOS

I. Introduction

As a branch of wireless sensor network (WSN), body sensor network (BSN) is a crucial application in the public network. It has great application requirements and significance in some e-Health service areas, such as remote medical care, special crowd custody, primary care etc. Body sensor network is a kind of network attached on the human body that composited by a set of tiny sensors capable of communication and a BSN aggregator (or BSN coordinator). Every tiny sensor can be attached on the body or implanted in the body. BSN aggregator is the network manager and also the gateway between BSN and external network such as 3G, WiMax, Wi-Fi. The human physiological data can be safely transmitted and exchanged by BSN aggregator. BSN is not only a new universal health care, disease control and prevention solution but also an important perception part of Internet of Things (IOT).

The increase of aging population around the world and the shortage of medical relative resources (budget outlay, doctor, nurse and sickbeds) make the development of medical and health care systems becoming the global demand. Hence, firstly, BSN technology is urgently needed to effectively solve the difficulty of expensive medical treatment problem and get access to quality medical services (especially in rural areas). Secondly, most conventional medical treatments are taken after symptoms instead of real-time diagnosis and disease prevention. In this case, BSN as a representative of the new technologies can provide effective assistance. BSN can supply classification study or analysis for the existing physiological parameters data, warn possible disease by analyzing the real-time signal or data, or preserve important physiological information during the course of illness for later diagnosis and treatment.

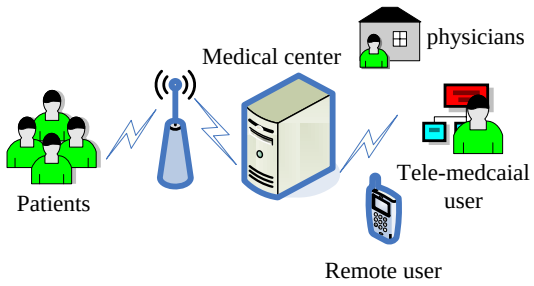

Figure 1. A typical architecture of a BSN-based health monitoring system

Although BSN has a broad prospect of application and practical value, it still will face with numerous challenges. A typical architecture of a BSN-based health monitoring system is illustrated in Fig. 1. Sensors of various functions can collect human physiological information such as ECG (electroencephalography), EEG (electroencephalogram), EMG (electromyography), body temperature, blood pressure etc. and send data to BSN aggregator. Then through wire or wireless connection, sensitive information are transmitted to medical data center or doctor's site for further diagnosis and monitoring. However, the biggest threat of the BSN

Manuscript received April 18, 2013; revised May 3, 2013.This work is supported by the Natural Science Foundation of Chongqing (cstc2012jjA40053); the Scientific Research Fund of Chongqing University of Posts and Telecommunications(A2012-12); the National Science Foundation of China (Grant No. 61272400).
Corresponding author email: xugx@cqupt.edu.cn
doi:10.12720/jcm.8.5.307-314

©2013 Engineering and Technology Publishing

system is how to protect the patient's personal health information (PHI) from being abused, illegally collected or disclosed. If the PHI such as ECG, EEG, and EMG etc. can be unauthorized access easily, they may refuse to use BSN system in case of information leak. Consequently, security of PHI is crucial for the application and promotion of BSN. But the traditional cryptography method is not enough to protect the patient's privacy because of the open channel nature of wireless communication. An adversary can make use of the method of eavesdropping on the network traffic or analyzing the traffic patterns to obtain some contextual information of a patient[1]. For example, even the messages being transmitted between BSN aggregator and base station have been encrypted, which means content privacy was guaranteed, the adversary still can analyze the traffic densities, traffic rate and the movement of data packets to gain location information or relationship between sender and receiver.

There are plenty of researches on WSN aiming at protecting location privacy and realizing anonymity communication; however they are not suitable for BSN system because of different application scenarios and system architectures. First, most of proposed schemes considered a homogeneous network, which need abundant sensor nodes being deployed in target area. Nevertheless, in BSN, only few wearable, implantable, or portable medical wireless sensors are needed to monitor the patient's physiological conditions [2]. So in healthcare or hospital scenarios, scalable and application oriented wireless network is required. Secondly, due to the sensors deployed in human body, signal source is stabilized and it's unremittingly transmitting messages to base station. This makes BSN system quite a different system from incident monitoring network which the location of signal source is inconclusive.

Hence this paper proposes a privacy-preserving scheme to protect contextual privacy of BSN from eavesdropping. The reminder of this paper is organized as follows: Section 2 states some related works in privacy-preserving. Section 3 describes the system model of proposed scheme and some evaluation metrics. Section 4 introduces the details of SDT scheme. Section 5 evaluates energy consumption and other metrics of SDT. Finally, a conclusion is given in Section 6.

II. Related Work

Plenty of approaches have been worked on anonymity and privacy problem of wireless sensor networks. Location privacy of source node gains lots of attention in event monitoring sensor networks. Threats against content privacy has been researched deeply, hence there already have been many effective encryption and authentication methods. However contextual privacy is still in dangerous, because wireless tunnel can be eavesdropped easily.

Ying *et al*. [3] proposed a location privacy routing protocol (LPR). LPR focuses on defeating packet-tracing attack by providing path diversity contrast to single-path routing protocol such as Phantom routing and DEEP. When event happened around some sensor node, this sensor node will randomly pick two nodes to forward message: one of them is in closer list, the other in further list. Finally, the message arrive the base station and the traffic pattern is imperceptible to local adversary. But obviously LPR is incapable of defending a global adversary, because the message always trend to the base station.

An eHealth security system SAGE presented by Xiaodong Lin et al. [2] utilized broadcasting nature to realize contextual privacy. SAGE uses Tate Pairing encryption algorithm to guard patients' privacy. However, SAGE brings extra time delay because of asymmetric cryptography and broadcasting queuing time increasing along with patient amount. Meanwhile SAGE requires a large sum of physicians to maintain privacy level, and does not support remote query. These disadvantages are not suitable for telemedical application.

An intuitive approach hiding real event message in event detection network is randomly sending out fake message. However time delay is inextricable. More optimized solution is to send real event packets as soon as the event happens, and program the nodes to make it independently distributed sending messages with a certain rate. By doing this, the distribution of the whole message queue shows statistically to the adversary [4]. Basel Alomair et al. well studied the stare-of-art approach and proposed a statistically framework for wireless sensor network to provide a higher level of security.

Phillip Reindl et al. [5] proposed a Control Packet based Anonymity (CPA) to achieve source node anonymity. Source node broadcasts message to all neighbors continuously. When there isn't a real event happened, CPA just sent a dummy message to reduce communication overhead. Even so CPA still costs much for the whole network and generates time latency.

Approximate grid topology and homogeneous network were considered to realize anonymous communication protocol (ACP) [6]. Every sensor node will randomly transmit packet generated by a continuous uniform random number and a certain formula. However, due to its randomness, time delay can not be ensured, and energy consumption of ACP needs further consideration. So a heterogeneous and appropriate network is considered in this approach to fit practical telemedical application.

III. System Model

A. Network model

As mentioned above, there are plenty of sensor nodes being deployed in human body as steady signal sources. So considering a heterogeneous network structure will better fit practical application requirements since applying a large sum of extra resources extremely

©2013 Engineering and Technology Publishing

constrained sensor nodes in medical or military environment is not convenient [7]. In this paper, a three-layer network construction using clustering structure is supposed in Fig. 2.

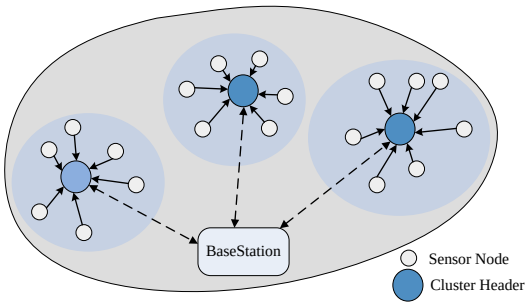

Figure 2. Three-layer network construction

- The first layer is the base station which is responsible for data storage and processing, and in charge of managing all cluster head nodes. In healthcare BSN system it may be medical data center or central processing center.
- The second layer consists of the cluster heads. In this BSN system cluster heads are regarded as been pre-deployed in healthcare scenarios, and they are responsible for gathering sensor nodes' information. Cluster heads are assumed to have abundant energy and enough storage memory in order to transmit all cluster members' data to base station.
- The third layer is composed of all BSN aggregator carried by users. Every BSN sensor collects user's physiological information and sends all data to BSN aggregator, and then aggregator transmits the data to medical data center via wireless network. BSN aggregator is constrained by energy, storage space and compute capacity. In addition, BSN aggregator is not able to sense information but just collects from other sensors.

B. Adversary Model

Similar to the model considered in other papers [8]-[10], the adversary is assumed to be capable of conducting global eavesdroppers and the behavior of adversary is external, passive. Global eavesdropper means the adversary has a global view of the whole network topology and can simultaneously monitor all communication patterns of all participants. "External" means the adversary neither compromise any sensor node nor inject any character in transmitting message. "Passive" means that the adversary can intercept all sensor nodes in the network simultaneously, but it does not conduct any active attack. Besides, the adversary is assumed to have abundant memory and energy to record traffic patterns and perform statistical tests.

In particular, even though adversary is able to directly observe the patient instead of analyzing the traffic patterns, the physiology or disease information of the patient can not be observed without linking to specific physician, since the adversary can't deciphering the encrypted messages [11].

C. Evaluation Metrics

1) Anonymity level

Anonymity level is defined as the probability V that a specific node can't be distinguished from other nodes in an anonymous set S. Supposing node A is a source node and it needs to be concealed in an anonymous set S, $|S|$ represents the total number of nodes in set S. Then the anonymity level of a protocol can be defined as $V = 1-(1/|S|)$ [12]. This formula indicates that the anonymity has a direct relationship with the number of anonymous set. Source-destination fuzziness needs to be realized in this paper. So if both source and destination anonymous are taken into consideration, we can further define $V_o = 1-(1/|S_S||S_D|)$ [13]. S_S , S_D indicate the independent set of source and detonation respectively.

2) Unlinkability

Unlinkability means the adversary can't obtain relation information and break contextual privacy between source and destination by conducting Linking Attack. Untraceablility has a resemblant meaning representing that the adversary can't trace packet sent from either source or destination to defeat contextual privacy. Thus Packet Tracing Attack is invalid.

3) Energy consumption

For BSN with constrained power, energy is a crucial factor to evaluate the performance of a security scheme. So we will reveal the energy consumption of proposed scheme SDT by analyzing the extra traffic and calculating expenditure.

4) Time delay

Because our network structure is different from other approaches and due to the special needs of transmitting human physiological data, we will focus our evaluation on the mean delay time of PHI transmission and calculating.

IV. Secure Data Transmission Scheme

In this section, this paper presents the proposed privacy-preserving scheme for keeping source-destination fuzziness consequently to guarantee contextual privacy in BSN system.

To meet the security needs, all MAC and routing protocol messages are assumed to be encrypted. Hence PHI leakage will not happen during transmission and sender's ID, IP address will not be disclosed. So the only way for adversary to get information is analyzing traffic patterns. Meanwhile, Key management protocol is also assumed to be applied so that symmetric keys can distribute among base station, cluster heads and sensor nodes. Accordingly no data packets will be disclosed, and the relationship between nodes can be authenticated. Besides, time synchronization has been applied since it is

©2013 Engineering and Technology Publishing

one of the basic subassembly for wireless sensor network application [14].

A. Network Topology Initialization and Transmission Negotiation

Typical healthcare BSN system topology was illustrated as Fig. 3. All cluster heads are pre-deployed before system initialization, and the total numbers of them can also be increased or decreased [15]. It is reasonable for application in hospital or sanatorium. Sensor nodes represent BSN aggregators of patients, they were clustered after initialization. In this paper, patients are assumed to be mobilizable within its cluster head's communication range. The system where patients are free to move will be studied in the further research.

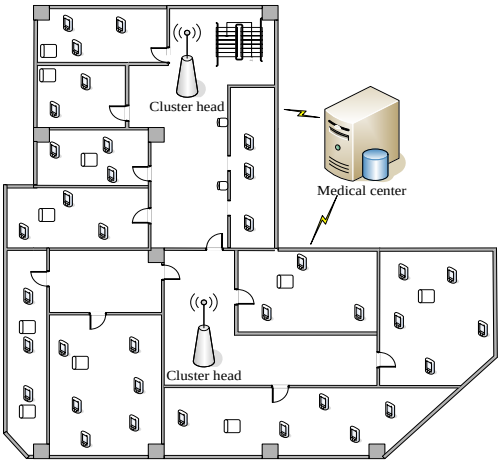

Figure 3. Typical healthcare BSN system topology

For convenience sake, we list terms and notions used in this paper as Table I.

TABLE I. TERMS AND NOTIONS

S_S	Source nodes set of all patients
S_D	Destination set of all physicians
$S_m(m=1,2\cdots y)$	Patients set in every single cluster
$c_m(m=1,2\cdots y)$	Cluster heads
M	Message packet
V	Anonymity level
T_S	Data send time of BSN aggregator
T_F	Data forward time of cluster head
K_{cAES}	encryption key of cluster head
K_{bAES}	encryption key of base station
K_{AES}	encryption key of BSN aggregator
h	generated by all n messages' ID using a hash function

When start-up, base station sends "joining in message" to all cluster heads to query whether it will join into the net. In case of replay attacking, message should include a Nonce number. Cluster head will use the Nonce number to encrypt response message by pair-wise key. After the cluster heads registering at the base station successfully, they will continue this procedure by broadcasting "clustering message" to gather their cluster members. When initialization is finished, base station will get the whole network topology and all cluster heads will recognize their members. New cluster head and BSN aggregator are also allowed joining in network topology later.

After topology initialization, data transmission is expected to process in the next step. Hence in order to defeat traffic analyze attack and other contextual privacy related assault, a Secure Data Transmission Scheme is applied in this scheme. Generally speaking, BSN sensors collect human physiological parameters according to the schedule time interval and send the data to medical center. Relatively stable signal source causes relationship disclosing of communicating parties easily.

Hence while topology being established, base station will add an arranged "data forwarding time" in "joining in message" and send it to all cluster heads. For convenient sake, we suppose all tBSN sensors have proximate data collecting cycle, which is also reasonable because the target physiological parameters are similar. "Data forwarding time" can be set as $T_F = \theta \cdot T_S$. θ is a time parameter used to adjust forwarding frequency of cluster head. And every cluster head will include a "data send time" T_S in "clustering message" sending to its cluster members which stand for BSN aggregator data sending cycle. T_S can be set according to the actual data collecting cycle of BSN sensors. The network topology initialization process is shown in Table II.

TABLE II. CLUSTER HEADS AND SENSOR NODES JOINING PROCEDURE

J_{msg} -join message.	
Nonce -random number.	
1.	Base station broadcast message packet $M_j = \{J_{msg}, T_F, Nonce\}$
2.	Cluster head return $M_r = (K_{cAES}\{J_{msg}, Nonce\}, K_{cAES}\{ID_{head}\})$
3.	Base station comparing M_r with $M_{base}, M_{base} = K_{bAES}\{J_{msg}, Nonce\}$
4.	if $M_r = M_{base}$ cluster head joining success. Add cluster head to topology list L_{base} .
5.	else drop M_r .
6.	Cluster head broadcast $M_{j,c} = \{J_{msg,c}, T_S, Nonce\}$
7.	BSN aggregator return $M_{r,c} = (K_{AES}\{J_{msg,c}, Nonce\}, K_{AES}\{ID_{node}\})$
8.	Cluster head comparing $M_{r,c}$ with M_C , $M_C = K_{cAES}\{J_{msg,c}, Nonce\}$
9.	if $M_{r,c} = M_C$ BSN aggregator joining success. Add BSN aggregator to topology list $L_{cluster}$.
10.	else drop $M_{r,c}$.
11.	Finally cluster head send topology list $L_{cluster}$ to base station, add $L_{cluster}$ to L_{base} . $M_{map} = (K_{AES}\{L_{cluster}, ID_{cluster}\})$

©2013 Engineering and Technology Publishing

B. Data Transmission Procedure

Table III illustrates data transmission procedure of BSN aggregator. Once "data forwarding time" and "data send time" are confirmed, data collecting and transmitting can proceed. BSN aggregator receives physiological parameters gathered by BSN sensors and stores the data in its buffer, and then it will check its buffer every data cycle T_S. If there were data packets in message queue, the aggregator will send them out after encrypting. Else the BSN aggregator will send a dummy data packet avoiding time correlation and packet tracing attack [16].

TABLE III. BSN AGGREGATOR DATA TRANSMISSION PROCEDURE

S-Dummy packet= K_{AES} {CF, empty}
S-PHI= K_{AES} {CF, ID, M }
CF represent message flag if CF=ture, message is real one if CF=false, message is empty. M is message data load.
1. When every new data cycle T_S
2. check if (data buffer is empty == True)
3. send S-Dummy when $(n+1)T_S$
4. else if (data buffer is empty == False)
5. send S-PHI when $(n+1)T_S$
6. Wait $(n+2)T_S$

Table IV illustrates data transmission procedure of cluster head. At the second layer of the network, cluster head receives physiological data sent by BSN aggregators in its cluster and stores them in its buffer. Then it will check its buffer every data cycle T_F. If there are data packets in queuing, then cluster head will forward them in C-PHI data packet format, or cluster head will send a dummy data packet.

TABLE IV. CLUSTER HEAD DATA TRANSMISSION PROCEDURE

C-Dummy packet= K_{cAES} {CF, empty}
C-PHI= K_{cAES} { CF, ID_c , n , h , [$M_1 \cdots M_n$] }
n represent message amount in this packet h generated by all n messages' ID using a hash function to validate data integrity, $h = H(ID_1 \mid ID_2 \mid \cdots \mid ID_n)$.
1. When every new data cycle T_F
2. check if (data buffer is empty == True)
3. send C-Dummy when next T_F
4. else if (data buffer is empty == False)
5. send C-PHI when $(n+1)T_F$
6. Wait $(n+2)T_F$

C. Data Receive and Store

When the medical center receives data from cluster heads, it decrypts all messages and stores them in database classify by sensor's IDs which represent different patients. It is assumed the same condition with SAGE that all messages receiving and deciphering by medical center for efficiency. Different from proposal SAGE, physiological data won't be broadcasted to all physicians. Doing this can bring convenience that physicians can login in within permission through any terminal and querying every patient in any time (See Fig. 1). Meanwhile the family members of patients can also login in the healthcare system to keep a watchful eye on patient's health condition without concern of personal privacy leakage. This is very remarkable feature in the application of telemedicine system.

V. PERFORMANCE EVALUATION

In order to protect patient's privacy, security metrics should be considered carefully. Since contextual privacy is considered in this paper, we deem a success if the adversary can't link the relationship between source and destination. Because our scheme aims to specify that healthcare application which is different from other anonymity schemes [4]-[6]. So we mainly compare our scheme with SAGE which was also designed for telemedicine.

A. Anonymity level

As described above, the anonymity level of the proposed scheme is (1):

$$V_o = 1-(\frac{1}{|S_S||S_D|}) = 1-(\frac{1}{|\prod_1^y S_m||S_D|}) = 1-(\frac{1}{|\prod_1^y S_m|}) \quad (1)$$

$V_o \in [0,1]$, $V_o = 0$ represents the lowest anonymity level, while $V_o = 1$ represents the anonymity level is high. In our scheme both physicians and family members can access PHI after authentication, so $|S_D| = 1$ because they are independent. Every patient is concealed in its cluster because they behave the same. Corresponding metric of SAGE is (2):

$$V_{sage} = 1-(\frac{1}{|S_S||S_D|}) = 1-(\frac{1}{|S_D|}) \quad (2)$$

The reason why $|S_S| = 1$ is that every patient in SAGE is independent and won't be concealed in any anonymity set. Hence the adversary can distinguish each patient effortlessly. But SAGE owns an anonymity set for all destinations. So in order to keep a relatively high anonymity level, S_D should be a larger value, for example 500 or more. But it may not be realistic that a hospital has so many doctors. For proposed scheme it is reasonable that there are many patients.

B. Unlinkability

According to our scheme, the link privacy can be formally defined as follows if the adversary attempts to break it [2]. Definitions of the attack use a game between a challenger *C* and an adversary *A*.

Game of linking attack

©2013 Engineering and Technology Publishing

1) M sets of patient $S=\{S_1, S_2 \cdots S_m\}$ are available to both challenger C and an adversary A. Meanwhile, exact number of patients in every set $|S_m|$ is also available to both sides. For convenience of calculations, $|S_m|$ gets an equal value $|S_{fix}| = x$.
2) The challenger knows patients' and the BSN aggregators' pair-wire key. At some moment, the challenger picks a random number $i \in \{1, 2 \cdots x\}$, generates a $G = K_{AES}(i)$ and sends it to cluster head.
3) Then cluster head picks a random number $j \in \{1, 2 \cdots y\}$, generates a $G' = K_{cAES}(i, j)$, and forwards it to the medical data center.
4) The adversary A makes guess on i and j in {0, 1} range after receiving the message, and gets the result i' and j'. Finally the adversary wins the game if $i' = i$ and $j' = j$.

The advantage of *A* defeating the link privacy property of G and G' can be defined according to SAGE scheme as (3):

$$Adv_A^{dy} = x \cdot \Pr[i' = i] \cdot y \cdot \Pr[j' = j] - 1 \qquad (3)$$

For any potential adversary *A*, if the advantage Adv_A^{dy} is insignificant or close to zero, we regard that the relationship of source and destination is unlinkable.

To prove SDT in this game enjoys the unlinkable privacy, we can show that the sender of G' needs to be found within cluster heads set $c = \{c_1, c_2 \cdots c_y\}$. Then if the adversary points out sender of G in $|S_{fix}|$, he will win the game.

Theorem 5.1: The link privacy of patient in SDT is guaranteed.

Proof: Content privacy of patient has been kept, thus the adversary *A* only can attempt to defeat contextual privacy by eavesdropping. In the eye of the adversary, every cluster head in set C is under suspicion of message G''s sender. Hence $\Pr[j' = j]$ is limited to $\frac{1}{y}$. For the same reason, probability $\Pr[i' = i]$ of finding out message G's sender is limited to $\frac{1}{x}$, since every BSN aggregator in a single cluster is equal suspicious. By analyzing we get (4):

$$\begin{aligned} Adv_A^{dy} &= x \cdot \Pr[i' = i] \cdot y \cdot \Pr[j' = j] - 1 \\ &= x \cdot \frac{1}{x} \cdot y \cdot \frac{1}{y} - 1 = 0 \end{aligned} \qquad (4)$$

the proof is done.

From above theorem we know the link privacy as (5):

$$\Pr[source, patient] = \Pr[i' = i] \cdot \Pr[j' = j] = \frac{1}{xy} \qquad (5)$$

So it is necessary to maintain large amount patient and appropriate number cluster heads. Fortunately it is reasonable in practical terms that there are many patients in hospital.

C. Energy Consumption and Time Delay

Unquestionably, due to extremely constrained resources of wireless sensor nodes, scheme overhead also requires consideration. In SDT we adopt AES encryption algorithm to reduce calculation and transmission consumption comparing to SAGE. Meanwhile, SDT brings more dummy packets transmission consumption, which can be cut down by adjusting forwarding cycle T_F. SAGE modified a Tate Pairing algorithm [17]. However it was designed for computer and didn't been implanted into real sensor nodes. Therefore, SAGE was lack of energy consumption evaluating of sensor nodes. Thus we adopt a latest Tate Pairing algorithm Tiny Pairing [18] to make an analysis, which is specially designed for wireless sensor and also can achieve 80 bit security. Tiny Pairing is a better algorithm than Tiny Tate [19], which was the first algorithm implanted in wireless sensor. AES encryption algorithm in TinyOS only supports 32 bit encryption as contrast.

Specially, time delay of PHI arriving medical center is crucial in telemedicine system. As a result of synchronous data transmission, there definitely is a time delay between real event and transmission cycle. Time delay of SAGE is mainly caused by broadcasting queuing and Tate Pairing calculation. The more patient PHI needing broadcasting, the more queuing time will cost. Since in SAGE the medical center needs to broadcast every patient's PHI one by one, time delay will rise as the number of patients increases. Vergados *et al.* [20] gave some typical bio-signal transmission requirements as Table Ⅴ. For representative, temperature was adopted in emulation. Temperature information rate is 80b/s, which means every second 80/8*1=10 byte data need transmitting to meet requirements.

TABLE V. TYPICAL BIO-SIGNAL TRANSMISSION REQUIREMENTS

Biomedical Measurements	Band width (Hz)	Sample rate (Hz)	Information rate (b/s)
ECG	0.01-250	1250	15000
Heart rate	0.4-5	25	600
Temperature	0-1	5	80

The time delay caused by SDT mainly due to T_S and T_F. Since all BSN aggregators get the same data sending cycle T_S in SDT, transmission delay mainly cause by forwarding cycle $T_F = \theta T_S$. The worst situation is that the biomedical message receiving time just staggers the data sending cycle. Then after receiving message cluster head have to wait for an additional forwarding cycle T_F to send it out. Simulations were conducted under Ubuntu 11.04, TinyOS 2.1.1, and Avrora emulator. In simulation experiments, we set BSN aggregator to send data every

©2013 Engineering and Technology Publishing

0.5s. Forwarding cycle $T_F = \theta T_S$ determines the maximum delay.

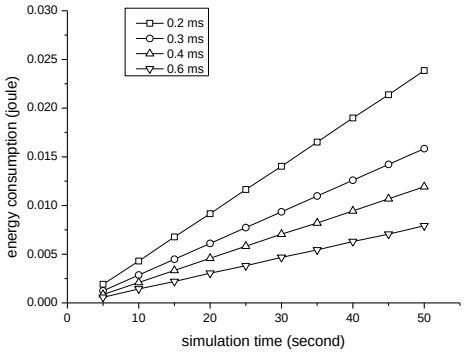

Figure 4. Energy Consumption among Different T_F

In order to achieve the balance between energy consumption and time delay, several values of T_F are set as Fig. 4. As illustrated in Fig. 4, the energy consumption significantly is reduced when T_F increases from 0.2s to 0.3s. The energy consumption changes relatively less when T_F increases to 0.4s or 0.6s, hence T_F is determined to be equal to 0.3s.

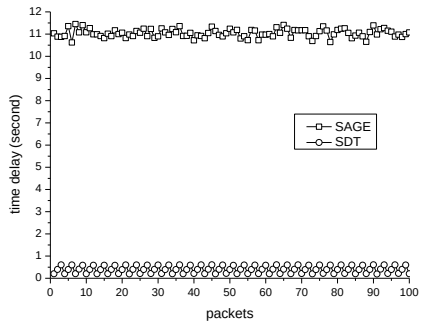

Figure 5. Time delay contrast between SAGE and SDT

Fig. 5 shows the time delay between Tate Pairing and AES encryption algorithm when they were implanted into sensor node such as Micaz. We sent out 100 packets during simulations, and the simulation result shows that Tate Pairing takes much more time delay. For medical applications, such high time delay is unacceptable.

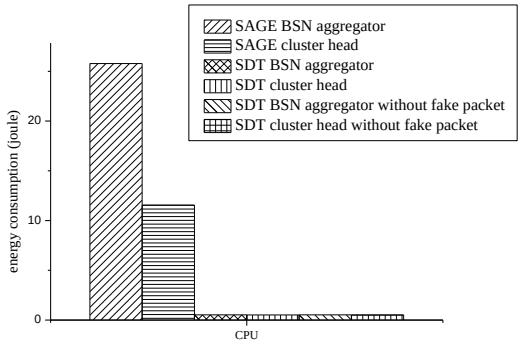

Figure 6. CPU energy consumption

Fig. 6 illustrates the CPU consumption between SAGE and proposed scheme. We also include CPU consumption information when proposed scheme only forwards real packet. By doing this, we can know extra consumption caused by send out fake packet clearly. As shown below, Tate Pairing costs vast energy because of complex calculation. And fake packets consume little CPU energy.

Fig. 7 shows radio energy consumption of SAGE, proposed scheme, and proposed scheme without fake packets. SAGE consumes more power because of data broadcasting. In SDT, the cluster nodes will transmit false packets, which consume almost the same amount of power as SAGE. When the cluster nodes are not transmitting false packets, the power consumption slightly reduces. But due to the large quantity of cluster nodes, and the real message forwarding state they are always in (which means the false packets forwarding is not frequently happened), the power consumption is not obviously reduced even when the cluster nodes are not transmitting false packets.

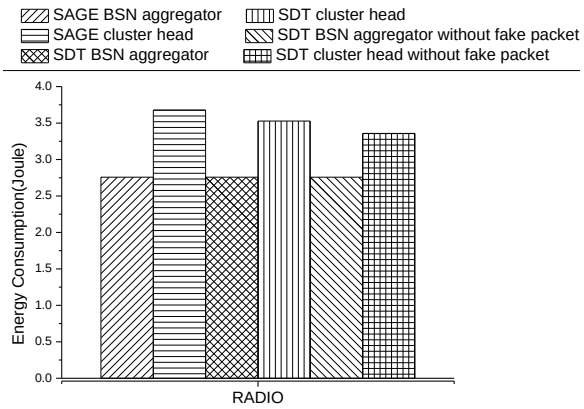

Figure 7. Radio energy consumption

Consequently, proposed scheme trades few energy consumption and security for less time delay in medical applications. Moreover, our proposed scheme is much more convenient because it provides different and many terminals to login in any place.

VI. CONCLUSIONS

Looming privacy problem is the key obstacle of telemedical technology. Once the suitable solution of the problem comes out, it will bring significant influence to telemedical technology and put telemedical into actual use. In this paper, a Secure Data Transmission Scheme called SDT is proposed specifically for tele-medical use. Considering the practical reality, SDT provides better contextual privacy and less time delay with small extra energy consumption. In addition, remote queries are allowed and the number of physicians is not limited in this scheme, which will better satisfy the requirements of telemedical application. Through theory and simulation evaluation, the proposed scheme has demonstrated excellent performance. In the future, we will work on patient mobility and network scalability.

ACKNOWLEDGEMENT

©2013 Engineering and Technology Publishing

This work is supported by the Natural Science Foundation of Chongqing (cstc2012jjA40053); the Scientific Research Fund of Chongqing University of Posts and Telecommunications (A2012-12); the National Science Foundation of China (Grant No. 61272400).

REFERENCE

[1] H-L. Hung and J-H. Wen, "Reduce-complexity fuzzy-inference-based iterative multiuser detection for wireless communication systems," *International Journal of Communication Systems*, vol. 25, no. 4, pp. 478-490, April 2012.

[2] X. D. Lin, R. X. Lu, X. M. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365-378, May 2009.

[3] Y. Jian, S. G. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *Proc. 26th IEEE International Conference on Computer Communications*, May 2007, pp. 1955-1963.

[4] B. Alomair, A. Clark, J. Cuellary, and R. Poovendran, "Statistical framework for source anonymity in sensor networks," in *Proc. Global Telecommunications Conference, Globecom, IEEE - Globecom*, 2010, pp. 1-6.

[5] P. Reindl, X. J. Du, K. Nygard, and H. L. Zhang, "Lightweight source anonymity in wireless sensor networks," in *Proc. IEEE Global Telecommunications Conference*, 2011, pp. 1-5.

[6] P. J. Pan and R. V. Boppana, "ACP: Anonymous communication protocol for wireless sensor networks," *IEEE Consumer Communications and Networking Conference* , 2011, pp.751-755.

[7] A. R. Khan, S. A. Madani, K. Hayat, and S. U. Khan, "Clustering-based power-controlled routing for mobile wireless sensor networks," *International Journal of Communication Systems*, vol. 25, no. 4, pp. 529-542, April 2012.

[8] K. Mehta, D. Gang Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Proc. International Conference on Network Protocols*, Oct 2007, pp. 314-323.

[9] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *Proc. IEEE 27th Conference on Computer Communications*, April 2008, pp. 51-55.

[10] T. Hayajneh, R. Doomun, P. Krishnamurthy, and D. Tipper, "Source-destination obfuscation in wireless ad hoc networks," *Security and Communication Networks*, vol. 4, no. 8, pp. 888-901, 2011.

[11] C. F. Lee, H. Y. Chien, and C. S. Laih, "Server-less RFID authentication and searching protocol with enhanced security," *International Journal of Communication Systems*, vol. 25, no. 3, pp. 376-385, March 2012.

[12] D. Huang, "Traffic analysis based unlinkability measure for ieee 802.11b-based communication systems," in *Proc. 5th ACM Workshop on Wireless Security*, 2006, pp. 65-74.

[13] R. Doomun, T. Hayajneh, P. Krishnamurthy, and D. Tipper, "Secloud source and destination seclusion using clouds for wireless Ad hoc networks," in *Proc. IEEE Symposium on Computers and Communications*, July 2009, pp. 361-367.

[14] S. Yoon, C. Veerarittiphan, and M. L. Sichitiu, "Tiny-sync: Tight time synchronization for wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 3, no. 2, June 2007.

[15] Z. C. Papazachos and H. D. Karatza, "Scheduling of frequently communicating tasks," *International Journal of Communication Systems*, vol. 25, no. 2, pp. 146-157, February 2012.

[16] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Pervasive and Mobile Computing - PerCom*, vol. 2, no. 2, pp. 159-186, April 2006.

[17] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in *21st Annual International Cryptology Conference*, Santa Barbara, California, USA, 2001, pp. 213-229.

[18] A. S. Ahmed, "An evaluation of security protocols on wireless sensor network," *TKK T-110.5190 Seminar on Internetworking*, 2009.

[19] L. B. Oliveira, D. F. Aranha, E. Morais, *et al.*, "TinyTate: Computing the tate pairing in resource-constrained sensor nodes," in *Proc. Sixth IEEE International Symposium on Network Computing and Applications*, July 2007, pp. 318-323.

[20] D. J. Vergados, D. D. Vergados, and I. Maglogiannis, "Applying wireless diffserv for QoS provisioning in mobile emergency telemedicine," *IEEE Global Telecommunications Conference. GLOBECOM*, Nov 2006, pp. 1-5.

Guangxia Xu earned her PhD degree at Chongqing University in 2011. She is an associate professor of the School of Software Engineering at Chongqing University of Posts and Telecommunications. Her current research interests include dependable computing, distributed systems, security of wireless network and flash memory.

Yu Liu. Graduate student of Chongqing University of Posts and Telecommunications. His research interests include security of wireless network, internet of things and body sensor network.

Yunpeng Xiao. PhD candidate of Beijing University of Posts and Telecommunications. His research interests include complex network, human dynamics and recommendation system.

Yanbing Liu earned PhD degree at University of Electronic Science and Technology of China in 2007. He is a professor of the School of Computer Science at Chongqing University of Posts and Telecommunications. His current research interests include traffic analysis of wireless, traffic modeling, resource assignment and resource allocation.

©2013 Engineering and Technology Publishing