AN ENERGY EFFICIENT DATA SECRECY SCHEME FOR WIRELESS BODY SENSOR NETWORKS

Jun Wu and Shigeru Shimamoto

Graduate School of Global Information and Telecommunication Studies,
Waseda University, Tokyo, Japan
junwu@akane.waseda.jp, shima@waseda.jp

ABSTRACT

Data secrecy is one of the key concerns for wireless body sensor networks (WBSNs). Usually, a data secrecy scheme should accomplish two tasks: key establishment and encryption. WBSNs generally face more serious limitations than general wireless networks in terms of energy supply. To address this, in this paper, we propose an energy efficient data secrecy scheme for WBSNs. On one hand, the proposed key establishment protocol integrates node IDs, seed value and nonce seamlessly for security, then establishes a session key between two nodes based on one-way hash algorithm SHA-1. On the other hand, a low-complexity threshold selective encryption technology is proposed. Also, we design a security selection patter exchange method with low-complexity for the threshold selection encryption. Then, we evaluate the energy consumption of the proposed scheme. Our scheme shows the great advantage over the other existing schemes in terms of low energy consumption.

KEYWORDS

Wireless Body Sensor, Security, Key Establishment, Hash, Selective Encryption

1. INTRODUCTION

Wireless body sensor networks (WBSNs) take an important role in telemedicine systems. In WBSNs, wireless sensor technology is used for health monitoring applications. Body sensors can be used to collect patients' medical data unobtrusively and ubiquitously around the clock without disrupting their normal daily lives. Moreover, advances in wireless communications technology have overcome most of the geographical, temporal, and even organizational barriers to facilitate a completely roaming way of transferring medical data.

In WBSNs, lack of adequate security features may not only leads to a breach of patients' privacy but also potentially allows adversaries to modify actual data resulting in wrong diagnosis and treatment [1], [2]. Also, health information collected from sensors needs to be secured and in many countries (for example USA) security is mandated [3]. Therefore, the security features should be implemented in WBSNs.

Although WBSNs share many of challenges and opportunities with general wireless sensor networks (WSNs), many WBSN-specific research and design questions have emerged that require new lines of inquiry. For example, a WBSN must have fewer and smaller nodes relative to a conventional WSN. Smaller nodes imply smaller batteries, creating strict tradeoffs between the energy consumed by processing, storage, and communication resources and the fidelity, throughput, and latency required by applications [4]. Therefore, the energy cost of the security designs for WBSNs should be lower than those of general WSNs. It is very necessary to investigate energy efficient data secrecy for WBSNs.

DOI : 10.5121/cseij.2011.1201

Many authentication models based on public/private key for MANET networks are complex [5]. Hence, symmetric encryption is a poplar way to design the data secrecy schemes for WSNs. Usually, the data secret design include two important issues: 1) Key establishment; and 2) Encryption during data exchange. We focus on energy efficient data secrecy on these two phases.

On one hand, the establishment of a shared secret key between a pair of nodes is the basis for other security services such as encryption. In this paper, we propose a key establishment protocol, which seamlessly integrates node IDs, seed value and nonce for generating cryptographic keys. Our protocol applies the one-way hash algorithm SHA-1 to ensure the security of the process of key establishment.

On the other hand, in general WSNs, strong encryption algorithms, such as Advanced Encryption Standard (AES), are usually used for the data secrecy. However, the energy consumption of strong encryption is relatively high. As a matter of fact, the security requirements in of medical data usually are quite different from those of general WSNs. A good example would be an audit report on a medical system. This report may be generated for an external auditor, and contain sensitive information. The auditor will check the report for the medical information that indicates possible cases of fraud or abuse. Assume that management has required that some personal information (i.e. “Names”, “Occupation”, “Home address”, etc.) should not be available to the auditor. Moreover, the data needs to be presented to the auditor in a way that allows the examination of all data, so that patterns in the data may be detected. Full encryption cannot suitable for this case, because only some parts of the data are secret. As a matter of fact, selective encryption is a proven technology in the field of secure multimedia communication [6]. The purpose of selective encryption is just to encrypt certain portions of the message with less overhead consumption. In this paper, we introduce selective encryption and adopt it for WBSNs.

The rest of this paper is organized as follows: In Sect. 2, we describe the related works about data secrecy with its energy consumption for sensor networks. In Sect. 3, we discuss preliminaries and assumptions including topology model, protocol model and attack model. We present our key establishment protocol in details in Sect. 4. The proposed threshold selective encryption scheme is shown in Sect. 5. Then, we discuss the security features of proposed scheme in Sect. 6. In Sect. 7, we evaluate the energy cost of the proposed scheme and make comparisons with other existing schemes. Finally, we conclude the paper in Sect. 8.

2. RELATED WORKS

Recently, data secrecy scheme for WSNs and WBSNs as well as their energy cost have been attracted a lot of attentions.

Yee Wei Law et al. [7] proposed a data secret scheme, KALwEN, which combines the cryptographic techniques of ECDH, combinatorial key pre-distribution, authenticated broadcast by one-way hash and threshold secret sharing. Haowen Chan et al. [8] proposed key establishment scheme for WSNs, which is called Peer Intermediaries of Key Establishment (PIKE). PIKE is a key-establishment protocol which uses one or more sensor nodes as a trusted intermediary to facilitate key establishment. Giacomo de Meulenaer et al. [9] investigated Kerberos protocol with symmetric key cryptography for WSNs. Also, they studied ECDH-ECDSA authentication protocol, which uses Diffie-Hellman key agreement based on Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithm (ECDSA). Also, the energy costs of both the Kerberos and ECDH-ECDSA on MICAz as well as TelosB nodes are analyzed. Patrick W. Fitzgibbons et al. [10] investigated the implementation of existing typical

protocol (such as Kerberos) on resource-restrained sensor nodes. The energy of related protocols is evaluated on several exiting sensor motes.

3. PRELIMINARIES AND ASSUMPTIONS

3.1. Network Architecture

Network topology must be considered before designing the key establishment protocol. There are five common kinds of topologies for WBSNs: point-to-point, star, mesh, tree and hybrid. The topology is the choice of application design. Indeed, mesh topology contains the features of all the other topology, because mesh topology is a network where all the nodes are connected to each other. Moreover, mesh topology are used in many application projects, such as BASUMA project [11].

Without loss of generality, we assume that our key establishment protocol is designed for WBSNs with mesh topology, so that our protocol can be used universally for all the topologies. The mesh topology is preferable when sensors need to communicate with each other. Usually, one of the nodes of a WBSN can be the aggregator. This aggregator can serve as a user interface, and bridging the WBSN to higher-level infrastructures and thus to other stakeholders.

3.2. Protocol Model

We consider a set of nodes interconnected by point-to-point links over which messages can be exchanged. We define that message-driven protocols are collections of interactive procedures, which specify a particular processing of incoming messages and the generation of outgoing messages. Key establishment and medical data exchange are message-driven protocols where the communication the communication takes place between pairs of nodes in the network.

3.3. Adversary Model

This paper considers attackers whose main goal is to obtain sensor data which they are not authorized to access. The adversaries could be either external intruders or network nodes who are unauthorized to access the target type of data [12]. We consider the attack models shown as follows.

Eavesdrop attack: the possible damage of a successful wireless attack starts with the ability to eavesdrop on the data transferred during the communication of two nodes, ends with the ability to fully impersonate other devices.

Replay attack: a message or a fragment of a message is taken out of its original context and replayed as a part of another message, in another protocol run, or even in a run of another protocol.

Denial of service (DoS) attack: adversary can launch large number of bogus packets to interrupt communication. Then the legitimate users or nodes are deprived of the services of a resource they would normally expect to have.

4. THE PROPOSED KEY ESTABLISHMENT SCHEME

4.1. Design of Key Establishment Protocol

In this paper, the cryptographic algorithm used to design the key establishment protocol is one-way hash algorithm SHA-1. SHA-1 is a cryptographic hash function designed by the National Security Agency and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. SHA-1 is the most widely used of the existing SHA

hash functions, and is employed in several widely-used security applications and protocols. The SHA-1 algorithm takes as input a message with maximum length of less than 2^{64} bits and produces as output a 160-bit message digest [13]. As a one-way hash function, the most important property of SHA-1is that it has no inverse function $x=F^{-1}(y)$, which means for a given x, it is easy to calculate $y=F(x)$.

Before design the key establishment protocol, we first define some notations used in the key establishment protocol, as shown in Table 1.

Table 1 Notations used by the key establishment protocol

Notation	**Meaning**
ID_I	The identity of node I
T	A timestamp generated by node A
$K_{A,B}$	The session key between node A and B
n_I	A nonce generated by node *I*, it is a randomized value to defend reply attack
$X\|\|Y$	A concatenation of message X and Y
SHA-1(K: M)	Use *SHA-1* to calculate the digest value of message M by key K
V_S	Seed value stored in each node
Msg.i	The ith message in the protocol
S_i	Verifier of the ith message

Our key establishment protocol is illustrated in Fig. 1. When a WBSN is deployed, each node of the network is assigned an identical seed value V_S. The length of V_S is 128 bits. V_S is stored in the protected storage of the nodes, so it is unreadable for external programs. Note that there are many existing designs the protected storage, such as the design in [14].

Let node *A* is the initiator of the key establishment process, and *B* shall be the node which *A* wants to set up a unique session key. Node *A* first generates a nonce n_A and a timestamp *T*. At the same time, *A* starts its timer that will fire after time T_{min}. Note that the nonce n_A is a 32-bit random value and the timestamp *T* is a sequence of characters, denoting the time at which a certain event occurred. Then she uses the 160-bit $n_A||V_S$ as the key of one-way hash algorithm SHA-1, and generates her master key K_A. Then she computes a digital digest of $V_S||n_A$, which is marked as S_0 working as a verifier. After that she sends node *B* a message, which contains n_A, ID_A , *T* and the verifier S_0. This message is marked as Msg. 1.

Upon receiving the *Msg*. 1 from node *A*, node *B* first checks whether the nonce has been received before and whether the message is created in a very recent time. If that is not true, node *B* will drop the packet from node *A*. Otherwise she will continue the next computation. She first computes K_A based on n_A, ID_A and V_S. Then she uses K_A to calculate digital digest S_0' based on n_A in *Msg*. 1 and V_S. After that she verifies the validity of *Msg*. 1. If S_0' does not equal S_0, she will drop the packet from node A. If S_0' equals S_0, she uses $V_S||n_A$ as the key of SHA-1 to compute her mater key K_B. Then she uses K_B as the key of SHA-1 to compute the session key $K_{A,B}$, and $ID_A||ID_B||n_A$ is the input to SHA-1 algorithm. After that she uses K_A as the key of SHA-1 algorithm to compute a digital digest of $ID_B||n_A$, which is marked as S_1 working as a verifier. At last, she sends node A a message, which contains ID_B and S_1. This message is marked as *Msg*. 2.

Upon receiving the Msg. 2, node *A* first uses K_A to calculate digest S_1' based on ID_B and n_A in the *Msg*. 2. Then she verifies the validity of *Msg*. 2. If S_1' does not equal S_1, she will drop the packet from node *B*. If S_1' equals S_1, she uses $V_S||n_A$ as the key of SHA-1 to compute K_B. After that she uses K_B as the key of SHA-1 to compute the session key $K_{A,B}$, and $ID_A||ID_B||n_A$ is the

input to SHA-1 algorithm. When *A*'s timer fires after T_{min}, she erase the seed value V_S and B's master key K_B, but keeps her own master key K_A. Then a session key $K_{A,B}$ is established between node *A* and node *B*.

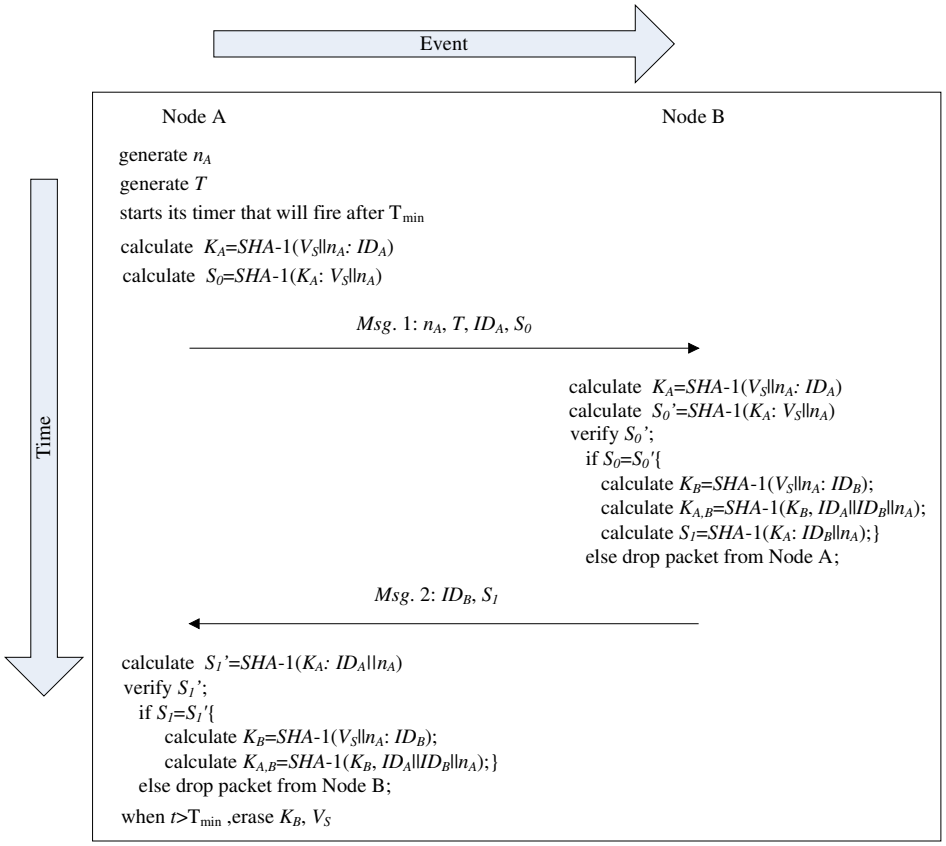

Figure 1. Key establishment protocol

4.2. Message Structure of Key Establishment

In the proposed key establishment protocol, a node identifier (node ID) consists of 64 bits. Furthermore, we count 32 bits for the nonce and 64 bits for the timestamp. An output of SHA-1 algorithm consists 160 bits. Therefore, the message structure of the proposed protocol is illustrated in Fig. 2. The lengths of *Msg*. 1 and *Msg*. 2 are 320 bits and 224 bits respectively.

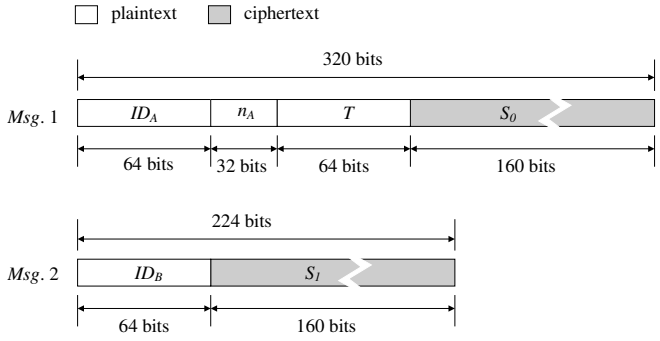

Figure 2. Message structure

5. THRESHOLD SELECTIVE ENCRYPTION FOR DATA EXCHANGE

After designing the key establishment, we focus on the encryption during data exchange. In this section, we propose a threshold selective encryption for WBSNs. Although a lot of selective encryption algorithms have been proposed for securing multimedia communication, the complexity of these schemes are relative high. Hence, the existing selective encryption schemes cannot be applied in WBSNs directly. In this section, we develop a threshold selective encryption as well as secure selection pattern transmission scheme, which satisfies the requirements on security and low energy cost of WBSN.

5.1. Encryption Process

During the deployment of WBSNs, an encryption threshold H ($H \in [0, 1]$) is set for each type of medical data. During the data exchange, a sender node generates a random value Y, where $Y \in [0, 1]$. Then, the sender node compares the value of Y with the pre-determined threshold H. Then, based on the result of the comparison, the sender node makes a decision whether the message should be encrypted or not. If the random value Y is greater than or equal to the threshold H, the sender node encrypts the data based on existing symmetric algorithm, such as AES. Otherwise, the sender node sends the data as plaintext. The key used to perform encryption is the symmetric key established by the method in Sect. 4. The principle of threshold selective encryption is shown in Fig. 3.

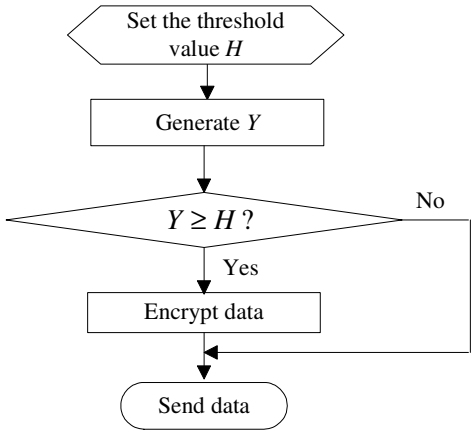

Figure 3. The process of threshold selective encryption

In our scheme, the sensitive data can be set a low threshold. The low threshold means the data have a high probability to be encrypted. If the data includes the highest secrecy, the responding threshold can be set as zero. In this case, the data must be encrypted. On the contrary, if the data dose not include any secrecy. The threshold can be set as one. In this case, the data will not be encrypted and be sent as plaintext. Note that value of the threshold depends on the application scenario and the requirements of the users. Moreover, the value of the threshold can be set based on the security requirements and the computation resources of the system. The users can get a trade-off between security and resource consumption.

5.2. Secure Selection Pattern Transmission

Once the sender node of the communication parties, it will let the corresponding receiver know the encryption pattern. Then the receiver node can know which part of the data is encrypted. Thus she can use the symmetric key to decrypt the corresponding parts of the data. The selection patter can also be eavesdropped by the attackers. Therefore, it must be transferred in a

secure way. Many existing selective encryption schemes use public key cryptography to exchange the selection patter, which is too expensive for resource-restrained WBSNs.

To address the above challenge, we propose a low-complexity secure exchange of selection patter. In our scheme, we add a selection stamp to every data block. The selection stamp marks whether the data block is encrypted or not. The receiver node can decide whether perform the corresponding decryption or not according to the selection stamp. Note that selection stamp is not the secret information of the individual. Also, the number of the bits in the encryption stamp is not large. Hence, using strong encryption to secure the stamp will course unnecessary energy cost. The structure of medical data with selection stamps is shown in Fig. 4. We embed the selection stamp into the original medical data. Then, we secure the exchange of selection stamp based on secure random checksums (SRCs).

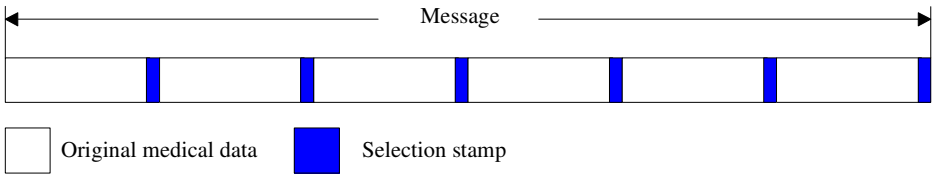

Figure 4. Medical data message with selection stamps

SRCs [15] are proposed as a simple alternative to more complex and computationally expensive homomorphic hashing functions. SRCs work well in Galois Fields of the form $GF(2^q)$, while homomorphic hashing takes place in modular fields of prime order, where arithmetic operations are more expensive.

SRCs are created by a server in possession of the complete file. The server node chooses a vector $r = [r_1 \ldots r_m]$ of random coefficients from the same field that is used for the source coding operations. The secure random checksum of an original block b is then defined as the sum of pairwise products of r and b:

$$\mathrm{SRC}(b) = \sum_{i=1}^{m} r_i b_i$$

Suppose that the original medical data file is divided into n blocks. Every block is followed a selection stamp. Selection stamp $P = [p_1, p_2, \ldots, p_n]$. Every selection stamp composed of m symbols $p_i = [p_{i1}, p_{i2}, \ldots, p_{im}]$. The structure of the original medical data with selection stamps is shown as Fig. 4. Then, the original medical data with the selection stamps is transferred to the receiver node by the sender node. Also, the SRCs together with r are transmitted to the user. Because of the linear nature of the computation, it is obvious that the SRCs of the original blocks can be used to calculate SRCs for any received encoded blocks. A peer that received a combined block c with associated identity g needs just to check the stamp as following:

$$\sum_{j=1}^{m} r_j c_j = \sum_{j=1}^{m} r_j \left(\sum_{i=1}^{n} g_i p_i\right)$$

where p_i refers to the selection stamp of the i^{th} original block of the file.

Based on the above secure design, the attackers cannot modify or replace the selection stamp. Thus the receiver node can decrypt the messages according the selection stamps. The selection stamps do not need to be encryption because they are not the private data of patients.

6. SECURITY ANALYSIS

In this section, we analyze the security of our scheme. We evaluate the security of our work by analyzing its resistance to the attacks described in sect. 3.

Eavesdrop attack resistance: During the key establishment, each node is assigned a seed value V_S when the node is deployed. Therefore, even if *Msg*. 1 or *Msg*. 2 in our protocol are eavesdropped, the attacker can not get the seed value V_S. And the attacker cannot get the session key $K_{A,B}$, because $K_{A,B}$ is calculated by $K_{A,B}=SHA\text{-}1(K_B, ID_A||ID_B||n_A)$. Attacker cannot derive V_S from S_0 because the property of SHA-1 described in sect. 3. During the medical data exchange, our scheme encrypts the secret data in the message based on the symmetric key. Thus the attackers cannot get the plaintext of secret data, because they do not have the symmetric key.

Replay attack resistance: During the key establishment, a sender node first generates a nonce n_A and a timestamp T. n_A and T are embedded into *Msg*. 1. When receiving a message, the receiver node checks whether the nonce has been received before. At the same time, the receiver node checks whether the message is created in a very recent time. If n_A has been received before or the message is not created in a very recent time, receiver node will regard the message is from an attack. If an attacker wants to modify n_A to implement replay attack, the receiver node will drop the packet because S_0' will not equal S_0 when the verification is implemented. During the medical data exchange, the replay attackers cannot get the symmetric key. Thus the receiver can distinguish the validity of the message based on the encrypted data. Hence the attacker cannot generate available replay attacks.

DoS attack resistance: the receiver node checks n_A and T of queries as soon as she receive it. Also, the receiver node verifies the verifiers. The receiver node will drop the packet soon if the check or the verifying cannot pass. Before verifying, few calculations will be implemented, which process SHA-1 algorithm twice. Also, before verifying S_0 and S_1, few values need be stored. In all, our protocol can resist DoS attack to some extent. During the medical data exchange, our scheme selectively encrypts the messages, hence the computation consumption is reduced. Also, every message is authenticated. This may avoid the attackers to spoof the packets of messages. Hence, our scheme can resist against DoS attacks to some extent.

In addition to the security capabilities listing above, our protocol can also resist some other attacks. For example, our protocol can resist node capture attack. If one of the nodes is captured, the attacker cannot get the seed value V_S, because that V_S is stored in the protected storage and it is unreadable for attackers. Moreover, n_A is different for each session. Hence, the attacker cannot get the session key.

7. ENERGY CONSUMPTION EVALUATION AND COMPARISON

7.1. Energy Consumption of Key Establishment

In this section, we evaluate the energy cost of the proposed scheme. We conducted our evaluation of the energy cost of cryptographic key establishment on a WINS sensor node from Rockwell Scientific [16]. Our motivation for using this specific sensor node is twofold. First, we wanted to use the same node as the authors of [10] so that we can directly compare the results. The second reason for choosing the WINS node is because this kind of sensor mote has been applied to perform monitor and control for health care.

Computation energy cost: The computation of our protocol is one-way hash computation. For the cost of computation, we make the approximation that the overall power consumption of the node while computing remains constant with the type of microcode operation performed.

Hence, the cost of particular computation can be assessed based on per cycle mean energy consumption and the total number of cycles of the computation. This simplifying assumption was verified by Yee Wei Law et al. in [17]. For the energy cost of SHA-1 algorithm, we use the implementation results of Patrick W. Fitzgibbons et al. [10]. They implemented SHA-1 on WINS node. And the energy cost of SHA-1 on 160-bit block is 2.16μJ. In our protocol, ten SHA-1 computation operations on 160-bit blocks have to be carried out in each run. Therefore, we can get the computation energy cost of our protocol on Rockwell WINS node 21.6μJ.

Communication energy cost: A WINS node sending data with a transmit power of 0.12 mW has an overall power consumption of about 771.1 mW. The overall power consumption increases to 1080.5 mW for a transmit power of 36.3 mW [16]. On the other hand, when the radio module operates in receive (Rx) mode, the WINS node consumes about 751.6 mW. Given the 100 kbit/s transmission rate of the WINS radio module, the transmission of one bit of data requires an energy between 7.71 μJ and 10.8 μJ on the sending node, and 7.52 μJ on the receiving node, respectively. The overall energy cost for transmitting (i.e. sending and receiving) a single bit of data is between15.2 μJ and 18.3 μJ. The communication energy cost is shown in Table 2.

Total energy cost: the overall energy cost of a key establishment protocol is not only determined by energy required for calculating cryptographic primitives, but also by the energy cost of radio communication between the involved nodes. Gathering the computation and communication costs found above provides the total costs for the protocol shown in Table 3.

Table 2. Communication energy cost

Message	**Length**	**Energy**
Msg. 1	320bits	4.86-5.86mJ
Msg. 2	224bits	3.40-4.10mJ
All msgs.	544bits	8.26-9.96mJ

Table 3. Total energy cost

Energy cost	**Energy**
Computation	21.6 μJ (0.24%-0.2%)
Communication	8.26-9.96 mJ (99.76%-99.8%)
Total	8.28-9.98mJ

Then we compare the energy of our protocol with other existing schemes. In order to verify whether the energy cost of our protocol is lower than that of existing schemes, we use the maximum energy 9.98 mJ to make comparisons. For the purpose of making comparisons under the same condition, we assume that the symmetric key cryptographic is AES and one-way hash algorithm is SHA-1 in the related schemes. And we also assume that the node platform is WINS node. For the SHA-1 and AES algorithm, we use the implementation results in [10]. In PIKE scheme [8], twelve AES operations as well as twelve SHA-1 operations have to be carried out. And 1248-bit data need to be transferred in PIKE. In KALwEN scheme [7], ECDH is the computation operation which courses the main energy cost. In addition, we choose Kerberos, Just-Vaudenary and Otway-Rees as the representatives of general protocols for comparison. Patrick W. Fitzgibbons et al. [10] implemented these general protocols on WINS node. The comparison between our protocol and above related protocols is shown in Fig. 5. Based on Fig. 5, we can see that our protocol is around respectively 2.3 times less costly than PIKE, 10 times less costly than KALwEN, 5.2 times less costly than Kerberos, 13 times less costly than Just-

Vaudanary, and 10 times less costly than Otway-Rees. In sum, the energy cost of our protocol is much lower than that of other existing protocols.

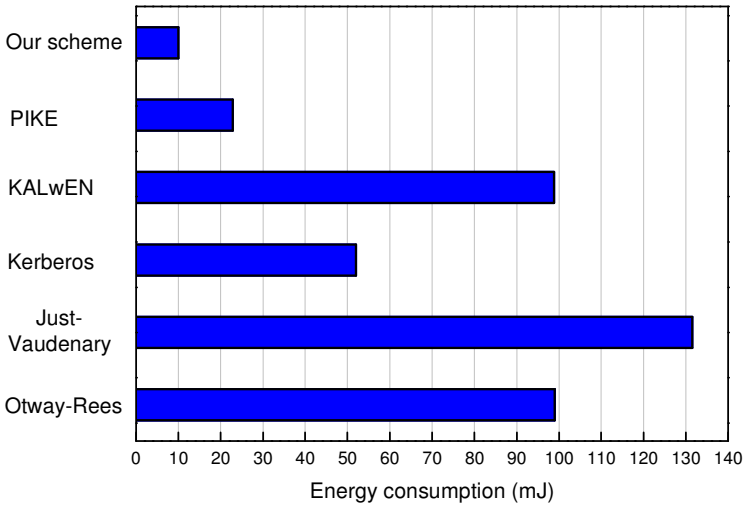

Figure 5. Comparisons of energy cost

7.1. Saving Energy Consumption during Data Exchange

In this section, in order to evaluate the saving energy of our scheme during data exchange, we implement a simulation experiment based on NetLogo [18]. We use AES as the symmetric cryptography algorithm to evaluate our scheme. Because the length of plaintext and cipertext are same for AES, we just evaluate the advantages of our scheme on encryption energy during data exchange. The energy required for the calculation of cryptographic primitives is simply the product of the average power consumption and the execution time. We setup a WBSN with 10 to 30 sensor nodes. Considering the relative mobility between the body sensors, we set these sensor nodes randomly move within a $2m \times 2m$ rectangle area. Each node randomly chooses its initial position, moves at a speed distributed randomly between zero and a maximum speed. We set the maximum speed as 0.1m/s.

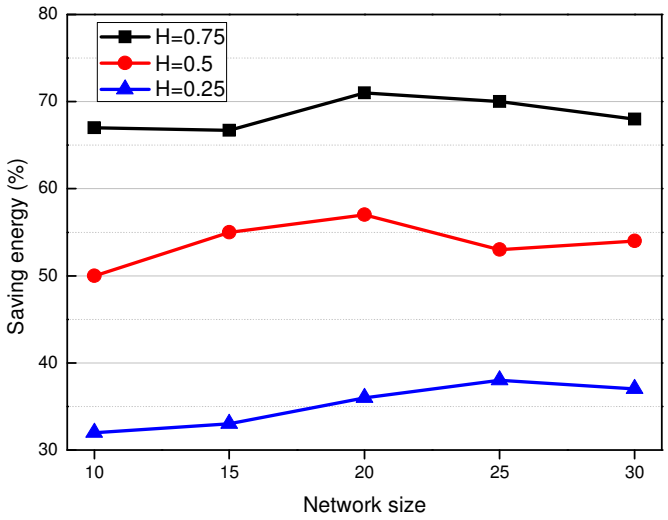

Figure 6. Saving energy vs. network size

Figure 6 shows the saving energy ratio on encryption of our scheme comparing with full encryption. As shown in Fig. 6, saving energy consumption depends on the encryption threshold *H*. If the encryption threshold increases, the ratio of saving energy increases.

8. CONCLUSIONS

In this paper, we propose energy efficient data secrecy scheme WBSNs. Our scheme includes two parts: key establishment and threshold selective encryption. In the proposed key establishment protocol, node IDs and seed value were combined with a nonce for generating cryptographic keys. SHA-1 algorithm was used in this protocol to generate the session key and ensure the validity of the messages. In the proposed encryption scheme, we introduced selective technology and adopted it into a low-complexity method for WBSNs. Also, a secure selection patter transmission scheme with low-complexity is proposed for our selective encryption. Through security analysis, our scheme can resist efficiently against the main attacks in WBSNs.

Furthermore, we evaluated the energy cost of our scheme and made comparisons with other existing schemes. Our scheme shows a great advantage over existing schemes in terms of low energy cost. Consequently, the proposed data secrecy scheme is applicable for energy restricted WBSNs, which take an important role in telemedicine. Moreover, because of the energy efficiency feature, the proposed data secrecy scheme can also be applied well in general WSNs.

ACKNOWLEDGEMENTS

This work was supported by Japan Society for the Promotion of Science (JSPS) under Grant-in-Aid for Scientific Research(C) (No.20560373) and by the Ph. D. Fellowship program of the China Scholarship Council (No.2008638003).

REFERENCES

[1] K. Venkatasubramanian and S. K. S. Gupta, Chapter 15: Security for pervasive Healthcare, Y. Xiao, Ed. CRC Press, 2007.

[2] K. Venkatasubramanian and S. K. S. Gupta, “Security for Pervasive Health Monitoring Sensor Applications,” In Proc. 4th International Conference on Intelligent Sensing and Information Processing, Dec. 2006, pp. 197-202.

[3] HIPAA-Report 2003, “Summary of HIPAA Health Insurance Probability and Accountability Act” US Department of Health and Human Service, May 2003.

[4] M. A. Hanson, H. C. Powell., A. T. Barth, K. Ringgenberg, B. H. Calhoun, J. H. Aylor, and J. Lach, “Body Area Sensor Networks: no. Challenges and Opportunities,” Computer, vol. 42, no. 1, pp. 58-65, Jan. 2009.

[5] J. Wu and S. Shigeru Shimamoto, “Usage Control based Security Access Scheme for Wireless Sensor Networks,” in the Proc. IEEE International Conference on Communications (ICC 2010), May 2010.

[6] H. Hofbauer and A. Uhl, “Selective Encryption of the MC EZBC Bitstream for DRM Scenarios,” in Proc. of the 11th ACM workshop on Multimedia and Security, pp. 161-170, 2009.

[7] Yee Wei Law, Giorgi Moniava, Marimuthu Palaniswami, “KALwEN: A New Practical and Interoperable Key Management Scheme for Body Sensor Networks”. In the Proc. of 4th International Conference on Body Area Networks (BodyNets 2009), Apr. 2009.

[8] H. Chan and A. Perrig, “PIKE: Peer Intermediaries for Key Establishment in Sensor Networks,” In Proc. of 24th IEEE International Conference on Computer Communications (INFOCOM 2005), vol. 1, pp. 524-535, Mar. 2005.

[9] G. Meulenaer, F. Gosset, F. Standaert and O. Pereia, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," In Proc. IEEE International Confernce on Wireless and Mobile Computing and Communication, Avignon, France, Oct. 2008, pp. 580-585.

[10] P. W. Fitzgibbons, D. Das, and L. J. Hash, "Constraints and Approaches for Distributed Mobile Ad-hoc Network Security," Tech. Rep. AD-A442043. Air Force Research Laboratory (AFRL), Internet draft available from http://hdl.handle.net/100.2/ADA44204, Nov 2005.

[11] BASUMA project, Internet draft available from http://www.basuma.de/

[12] J. Wu and S. Shimamoto, "Integrated UCON-Based Access Control and Adaptive Intrusion Detection for Wireless Sensor Networks," in Proc. of IEEE Global Communications Conference (GLOBECOM 2010), Dec. 2010.

[13] SHA-1 Standard, National Institute of Standards and Technology Secure Hash Standard, Federal Information Processing Standards Publication 180-1, 1995.

[14] A. Cilardo, A. Mazzeo, L. Romano, and G. P. Saggese, ," An FPGA-Based Key-Store for Improving the Dependability of Security Services," in Proc. of 10th IEEE International Workshop on Object-Oriented Real-Time Dependable Systems (WORDS 2005), Feb. 2005, pp. 389- 396.

[15] C. Gkantsidis, J. Miller, and P. Rodriguez, "Comprehensive View of A Live Network Coding P2P System," In Proc. of 6th ACM SIGCOMM Conference on Internet Measurement (IMC), pages 177–188, 2006.

[16] WINS Project, Rockwell Science Center, Internet draft available from http://wins.rsc.rockwell.com/

[17] Y. Law, J. Doumen, and P. Hartel, "Survey and Benchmark of Block Ciphers for Wireless Sensor Networks," ACM Transactions on Transactions on Sensor Networks, vol.2, no.1, pp. 65–93, 2006.

[18] S. Tisue and U. Wilensky, "Netlogo: A simple Environment for Modeling Complexity," International Conference on Complex System, Boston, May 2004.

Authors

Jun Wu was born in Hunan, China. He is currently pursuing the Ph.D. degree at Waseda University, Japan, funded by China Scholarship Council. He received the B.S. degree and M.S. degree from the Information Engineering College, Xiangtan University, Hunan, China, in 2002 and 2005, respectively. From July 2005 to September 2008, he was a lecturer in the Xiangtan University. His current research interests include wireless sensor networks and their information security. Mr. Wu is a student member of the IEEE.

Shigeru Shimamoto was born was born in Mie, Japan, in 1963. He received the B.E and M.E. degrees in communications engineering from the University of Electro Communication, Tokyo, Japan, in 1985 and 1987, respectively. He received the Ph. D. degree from Tohoku University, Japan in 1992. From April 1987 to March 1991, he joined NEC Corporation. From April 1991 to September 1992, he was an Assistant Professor in the University of Electro Communications, Tokyo, Japan. He has been an Assistant Professor in the Gunma University from October 1992 to December 1993. Since January 1994 to March 2000, he has been an Associate Professor in Department of Computer Science, Faculty of Engineering, Gunma University, Gunma, Japan. Since April 2002, he has been a Professor at GITS, Waseda University. In 2008, he also served as a visiting professor at Stanford University, USA. His main fields of research interest include sensor networks, satellite and mobile communications, optical wireless, Ad-hoc networks and body area network. Dr. Shimamoto is a member of the IEEE.