Authenticated Health Monitoring Scheme for Wireless Body Sensor Networks

Chunming Rong
Dept. of Elect. Engineering & Computer Science
University of Stavanger
4036, Stavanger, Norway
chunming.rong@uis.no

Hongbing Cheng
Dept. of Computer Science& Technology
Nanjing University
Nanjing 210093, China
Cheng.hongbing@uis.no

Abstract- Security and privacy are the main concern for patients to seek wireless body sensor network monitoring their health. Considering the limitations of power, computation capability and storage resources, it is a big challenge to find out suitable secure scheme for patients when relying on wireless body sensor networks to monitor their healthy information. Many schemes based on asymmetric and symmetric have been investigated for such kind problems. In this paper, we present an authenticated identity-based key encryption scheme for patients to secure their healthy privacy based on wireless body sensor networks monitoring their health. We review briefly about identity-based encryption and decryption first, and then describe an authenticated key establishment and encryption scheme based on the basic Boneh-Franklin algorithm for wireless body sensor networks. Finally we compare the proposed scheme with other technique with analysis and simulations. The results show that the proposed scheme is efficient and secure.

Key Words—identity-based cryptography, network security, wireless body sensor network**.**

1. INTRODUCTION

Wireless sensor network (WSN) has received considerable attention during last decade [1], and advances in wireless sensor networking have created new opportunities in health care and monitoring systems. We call such network as Wireless body sensor networks [2] (also known as bodynets or Body Area Networks), when working, data will be collected and reported automatically, reducing the cost and inconvenience of regular visits to the physician. Therefore, many more study participants may be enrolled, benefiting biological, pharmaceutical, and medical-applications research. Wireless body sensor networks have the potential to revolutionize healthcare, and are comprised of wearable devices with attached sensors that can measure various physiological and environmental signals. The integration of the abundance of existing specialized medical technology with wireless body networks will be popular in the future, and these systems will depend on and co-exist with the installed infrastructure, augmenting data collection and real-time response from the interest. Examples of areas in which future medical systems can benefit the most from wireless body sensor networks are in-home assistance, smart nursing homes, and clinical trial and research augmentation. These will be the great benefit for the elderly persons because the world has more and more aged population. In general, sensor body networks usually consist of a large number of ultra-small autonomous devices. Each device, called a node, is battery powered and equipped with integrated sensors, digital signal processors (DSPs) and radio frequency (RF) circuits. Wireless body sensor networks are facing several important security challenges because of special characteristics and limitations, including key establishment, authentication, privacy, secure routing, robustness to denial of service attacks and node capture. Particularly for the applications where wireless body sensor networks are developed in a hostile environment or used for some confidential purposes, security and privacy becomes an important topic. In order to establish a reliable body network, we have to design secure protocols to deal with problems in key establishing and cryptography during setting up a wireless body sensor network.

As we known, most wireless body sensor network is deployed in a random mode. Nodes do not have any information about neighbors and topology of the network ahead. Therefore, a simple approach for key establishing is to let all nodes store an identical secret *master key*. Any pair of nodes can use this master secret key to securely establish a new pair wise key. Anyway, this mechanism does not show desirable network resilience: if any single node is compromised, the security of the entire wireless body sensor network is compromised. Even though, it is possible to store the master key in some tamper-resistant hardware to avoid such risk, but it will increase the cost and energy consumption of each node. Furthermore, tamper-resistant hardware sometimes is not so reliable. One variant on this idea is to use a single shared key to establish a set of link keys for per pair of communicating nodes and then erase the networkwide key after establishing the session keys. However, this variant of the key establishment process does not support addition of new nodes after initial deployment.

There is another extreme scheme were proposed [3, 4], which considered a key predistribution scheme in which each sensor node stores S-1 keys (S is the number of nodes in the

Conference'10, Month 1–2, 2010, City, State, Country.

BODYNETS 2012, September 24-26, Oslo, Norway

DOI 10.4108/icst.bodynets.2012.249945

sensor network). This scheme guarantees perfect resilience because compromised nodes do not leak information about keys shared between two normal nodes. Unfortunately, this scheme is impractical for sensors with an extremely limited amount of memory because S can be very large.

Though computing cost is still a crucial problem for public-key cryptography system compared with symmetric cryptography system, research results [5,6] indicate that Elliptic Curve Cryptography (ECC) has some advantages in memory requirement and computing cost, maybe it will be suitable for wireless body sensor networks.

On the other hand, Shamir proposed the idea of Identity-Based Encryption (IBE) in 1984[7]. The idea of an identity-based encryption is that the public key can be an arbitrary string, for example, an email address, a name or a role. A fully-functional identity-based encryption scheme was not found until recently by Boneh and Franklin [8]. Since then the ideas of IBE have been used to design several other identity-based schemes for different purposes. It is well known that IBE-based algorithms based on ECC. Therefore, it is interesting to investigate the possibility to apply IBE in key establishment in Wireless body sensor networks. This is the objective of our paper.

The rest of the paper is organized as follows. Section 2 describes the basic Boneh-Franklin IBE scheme. Section 3 proposes an authenticated key establishment and encryption scheme for Wireless body sensor networks based on IBE. Section 4 gives detail comparison of the scheme in terms of efficiency and security through analysis and simulation. Conclusion is drawn in Section 5.

2. BASIC BONEH-FRANKLIN IBE SCHEME

In 1984, Adi Shamir proposed the concept of identity-based cryptography firstly. In his paper, Shamir presented a new model of asymmetric cryptography in which the public key of any user is a characteristic that uniquely identifies himself/herself, like an e-mail address.

In 2001, Boneh and Franklin proposed a practical algorithm based on IBE technique. To describe the basic Boneh and Franklin IBE algorithm, we use Zq to denote the group $\{0, \ldots, q-1\}$ under addition modulo q. For a group G of prime order we use G^* to denote the set $G^* = G\backslash O$ where O is the identity element in the group G. We use Z^+ to denote the set of positive integers. Firstly, we give some definitions and then the Boneh-Franklin IBE scheme.

Definition 2.1 A map $\hat{e}: G_1 \times G_1 \to G_2$ is called a bilinear pairing if, for all $x, y \in G_1$ and all $a, b \in Z$, we have $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$.

Definition 2.2 The Bilinear-Diffie-Hellman problem (BDH) for a bilinear map $\hat{e}: G_1 \times G_1 \to G_2$ such that $|G_1|=|G_2|=q$ is prime is defined as follows: given g, g^a, g^b, $g^c \in G_1$, compute $\hat{e}(g, g)^{abc}$, where g is a generator and $a, b, c \in Z$. An algorithm A is said to solve the BDH problem with advantage ε if

$$\Pr[A(g, g^a, g^b, g^c) = \hat{e}(g, g)^{abc}] \geq \varepsilon,$$

Where the probability is over the random choice of a, b, c, g, and the random bits of A.

Definition 2.3 A randomized algorithm G that takes as input a security parameter $k \in Z^+$ is a BDH parameter generator if it turns in time polynomial in k and outputs the description of two groups G_1, G_2 and a bilinear function $\hat{e}: G_1 \times G_1 \to G_2$, with $|G_1|=|G_2|=q$ for some prime q. Denote the output of the algorithm by $G(1^k) = < G_1, G_2, \hat{e}, q >$.

Definition 2.4 We say that G satisfies the BDH assumption if no probabilistic polynomial algorithm A can solve BDH with non-negligible advantage**.**

We now give the basic Boneh-Franklin IBE algorithm for identity-based encryption based on bilinear pairings on elliptic curves.

Algorithm1. The Basic Boneh-Franklin (BBF) scheme

Step 1: Run G on input k to generate a prime q, two groups G_1, G_2 of order q, and an admissible bilinear map $\hat{e}$: $G_1 \times G_1 \to G_2$. Choose a random $\alpha \in G_1$.

Step 2: Pick a random $s \in Z_q^*$ and set $\beta = \alpha^s$.

Step 3: Choose cryptographic hash functions for some n, H_1: $\{0, 1\}^* \to G_1^*$, H_2: $G_2 \to \{0, 1\}^n$. For the security proof, we view the all hash functions as random oracles. The message space is $M = \{0, 1\}^n$.

The ciphertext space is $C = G_1^* \times \{0, 1\}^n$. The output system parameters are $\pi = \{q, G_1, G_2, \hat{e}, n, \alpha, \beta, H_1, H_2\}$. The master key is $s \in Z_q^*$.

Step 4: Computes $Q_{Id} = H_1(Id) \in G_1^*$.

Step 5: Sets the private key K_{Id} to be $K_{Id} = (Q_{Id})^s$ where s is the master key.

Step 6: Choose a random $r \in Z_q^*$.

Step 7: Set the ciphertext to be

$$c = \langle r\alpha, m \oplus H_2(g_{Id}^r) \rangle,$$

$$\text{where} \quad g_{Id} = \hat{e}(Q_{Id}, \beta) \in G_2$$

Step 8: Compute and output plaintext

$$m = V \oplus H_2(\hat{e}(K_{Id}, U)).$$

Algorithm1 is the description of the basic version of Boneh-Franklin IBE algorithm. The basic version consists of two hash functions.

3. AN AUTHENTICATED SCHEME FOR WBSN

Based on the Boneh-Franklin IBE algorithm presented above, this section focuses on designing an efficient authenticated encryption scheme for wireless body sensor networks.

Note that, in Wireless body sensor networks, the nodes' initialization phase should be down prior to deploying the nodes. It could be realized in two modes. One is to use a base station to run the initialization phase and distribute all the parameters to nodes. The other is to distribute all the parameters to all sensors in

manufactory phase. In the first mode, the base station is only needed to generate parameters and send them to all nodes. After that, it exists no longer in a wireless body sensor network. The second mode is mostly like the MAC address in a network adapter. We can store a unique sensor Id in each sensor according to a worldwide identity or a customized identity. Therefore, the first mode can be considered as a special case of the second mode. In our scheme we use the Boneh-Franklin IBE algorithm to accomplish node's key establishment and encryption/decryption.

Furthermore, from the administration point of view, the initialization phase could be performed within a scope of patients of the body wireless body sensor networks, for example, a military unit, a fire department, a company, etc al. The master key is only stored in the base station of an organization. When a new sensor is needed to add or to replace one node in a network, an administration system completes the initialization process and puts it into the networks. This enhances effectively the security of the wireless body sensor networks. It will be discussed in detail in the analysis in the following section.

Now we define in detail our scheme in algorithms 2.

Algorithm2. An Authenticated Key Establishment and Encryption Scheme for WBSN

Based-on Boneh-Franklin IBE algorithm, we design an authenticated encryption/decryption scheme for wireless sensors networks as follows.

1) Setup: Before communications in Wireless body sensor networks. Given a security parameter $k \in Z^+$, the algorithm works as follows.

Run G on input k to generate a prime q, two groups G_1, G_2 of order q, and an admissible bilinear map $\hat{e}$: $G_1 \times G_1 \to G_2$. Choose a random $\alpha \in G_1$.Pick a random $s \in Z_q^*$ and set $\beta = \alpha^s$. Choose cryptographic hash functions for some n, H_1: $\{0,1\}^* \times G_2 \to G_1^*$, H_2: $G_2 \to \{0,1\}^n$, H_3: $\{0,1\}^n \times \{0,1\}^n \to Z_q^*$, H_4: $\{0,1\}^n \to \{0,1\}^n$ .For the security proof, we view the all hash functions as random oracles. The message space is $M = \{0,1\}^n$.

The ciphertext space is $C = G_1^* \times \{0,1\}^n$. The output system parameters are $\pi = \{q, G_1, G_2, \hat{e}, n, \alpha, \beta, H_1, H_2, H_3, H_4\}$. The master key is $s \in Z_q^*$.

Where q is a prime number, G_1 and G_2 are two groups of order q, $\hat{e}$: $G_1 \times G_1 \to G_2$ is a bilinear map, n is the length of plaintext, $\alpha \in G_1$, $\beta = \alpha^s$, $s \in Z_q^*$ is the master key, H_1, H_2, H_3, and H_4 are four hash functions with random oracles respectively. The master key should be kept in a secret place and the parameters can be distributed to all nodes.

2) Extract: For a given string $Id \in \{0,1\}^*$ (Id is node's public key. It could be a random string) the algorithm does: Computes $Q_{Id} = H_1(Id) \in G_1^*$ .Sets the private key K_{Id} to be $K_{Id} = (Q_{Id})^s$ where s is the master key.

Extract generates private keys corresponding to given primitive ID of every node in Wireless body sensor networks.

We require the hash functions in algorithm 1 to satisfy the standard consistency constraint, takes as input t_g, $c \in C$, and a private key K. It return $m \in M$. namely when K is the private key generated by algorithm Extract when it is given ID as the public key, then

$\forall m \in M$: Decrypt(t_g, c, K) = m where c = Encrypt(t_g, ID, m)

We add the followings algorithms to the system. Suppose we have a semantically secure symmetric cryptosystem. We represent its encryption and decryption functions with a key K by E_K , D_K, and assume the key is $K \in \{0,1\}^*$.

We define authenticated encryption and decryption algorithms for our scheme:

3) Authenticated-Encrypt: input: a health message (which is sent from a node to another node (nodes) in wireless body sensor networks), a private key (the nodes which are senders), and an ID(the nodes which are receivers),output: a ciphertext. The detailed operation is as follows.

Input: a health message $m \in \{0,1\}^*$. a private key d_A, an ID B, and the system parameters. Choose a random $\mu \xleftarrow{R} \{0,1\}^n$,compute $r = H_3(\mu, m)$and $s := e(d_A, H_2(B))$ Then output the ciphertext $c := \langle r, \mu \oplus H_1(r,s), E_{H4(\mu)}(m) \rangle$

4) Authenticated-Decrypt: input: a ciphertext (which is generated in Authenticated-Encrypt), an ID (the nodes which are senders), a private key (the nodes which are receivers), and output: the corresponding plaintext. The detailed operation is as follows.

input: a ciphertext $< U,V,W >$.an ID A, a private key d_B, Compute $s := e(H_2(A), d_B)$, $\mu := V \oplus H_1(U,s)$, $m := D_{H4(\mu)}(m)$

Check that $U = H_3(\mu, m)$. If not, reject the ciphertext, otherwise output the plaintext m.

Consistency is clear since $e(d_A, H_2(B)) = e(H_2(A), H_2(B))^a = e(H_2(A), d_B)$ by bilinearity.

Now we require these two authenticated algorithms to satisfy the standard consistency constraint. Additionally, for all health monitoring messages m, and for any two nodes A and B, their ID is arbitrary string with corresponding private keys d_A, d_B, we require

Authenticated-Encrypt (M, d_A, B)= Authenticated-Encrypt (M, A, d_B)

Note that Authenticated-Encrypt is faster than plain Encrypt because there is one less exponentiation and no point multiplication.

Note also that now both algorithms benefit greatly from caching: if nodes in wireless body sensors networks want to send many messages to each other, they can both compute s once and cache the result, obviating the need for an expensive Weil pairing computation during encryption and decryption which makes their communication as fast as asymmetric cipher and MAC.

More details about the efficiency and security of our scheme can be found in our earlier research work in reference [9].

4. ANALYSIS AND SIMULATION

We will analyse and simulate the proposed scheme in this section. For a node in WBSN, an ideal memory requirement is only to store all private keys shared with neighbors. In the proposed scheme, the total memory requirement consists of storage of parameters π and private keys used in asymmetric key system. Compared with the ideal case, the overhead of our scheme is the part for key establishment. It is relatively small. Moreover, once the communication phase is finished, the parameters can be deleted. Therefore, memory requirement of our scheme is optimal.

Public keys in the proposed scheme are arbitrary strings. They can be names, roles, email addresses, etc. This makes it possible for a sender to send a message whenever he wants; while in public-key infrastructure scheme, public keys should be generated and distributed to senders before sending a message. Our key predistribution scheme for WBSNs benefits from this property. Private keys in the proposed scheme are derived from the identities by a trusted Private Key Generator (PKG) using a master key, both public and private keys are created by users themselves. This gives the reason that why public-key infrastructure scheme is not considered as a good choice for key agreement and encryption in WBSNs. In a system with RSA algorithm, an authentication process is executed before the establishment of a secure communication; whereas in our scheme, this process is added in encryption and decryption procedures.

It is evident that our scheme based on ECC. Research results show that the traditional RSA algorithm with 1024-bit key (RSA – 1024) provides the currently accepted security level, and is equivalent in strength to ECC with 160 bit keys (ECC-160) and to symmetric key with 80 bits[10]. Therefore, the length of the keys is shorter than that of the traditional RSA algorithms. As a result, it economizes the storage resources and computational cost.

Compared to the proposed scheme, in key predistribution scheme, an extra key distribution must be performed prior to the deployment of a body sensor network. Secret keys are stored in nodes after distributing operation. There are two extreme cases in storing secret keys. One is to let each sensor keep in memory only one secret key (a global master secret key) shared by all nodes in a body sensor network. The other is to let each node carry all *S-1* secret pairwise keys, where S is the total number of nodes in a body sensor network. Evidently, these two mechanisms are impractical. A random key pre-distribution scheme and its variants are proposed in Refs. [11,12], where at least q keys selected from a key pool are stored in each node. When a node wants to communicate with another node, a key discovery operation should be performed. However, in our scheme, each node stores only the public parameters and owner private key, neither key predistribution nor key discovery is needed. Our scheme with 160 bit keys can provide currently a sufficient security level. Therefore, in terms of memory requirement and key discovery in WBSNs, our scheme has a better performance than key predistribution scheme. But in encrypting and decrypting operations it seems that symmetric key algorithms offer a better performance in computing cost. A detailed comparison could be an interesting future work. A glance at the computation cost gives that our scheme in encryption mainly requires four hash-function evaluations, two XOR operations, and one map computation.

Now, we will design some simulations to test the proposed scheme, we will consider three schemes in simulations, that are The proposed scheme, Public-key infrastructure scheme and Random key predistribution scheme. We will compare our scheme with others from three aspects in simulations, the two aspects are i) energy consumption of node, and ii) probability of node be captured. Note that in simulations, encryption algorithm's key size in our scheme is set to 160-bit, RSA algorithm's key size in public-key infrastructure scheme is set to 1024-bit and AES algorithm's key size in random key predistribution scheme is set to 128-bit.

We set simulation environment as follows: a personal computer has Dualcore CPU 2.0GHz, 2.0GHz and 2G DDR memory and operating system on it is Fedora 10, the simulation software is Ns-2, which is used extensively in the research area of Wireless body sensor networks. We use visual C++6.0 and TCL programming language to realize above three schemes. In simulations, we set 100-1000 nodes in a square of $400\times400m^2$ evenly and randomly, the transmission radius of each node is 80 meter, and the station is set at the left of the square, the destination nodes in the area of $60\times60m^2$, we adopt the model of energy consumption for nodes in[13],the model shows that, node will cost 400μJ energy when receives a bit of data and will cost 720μJ when sends a bit of data, in order to get the simulations results quickly, and ensure the simulation results is impartial at the same time, we set the initialization energy value of nodes is 10J.we choose a directed diffusion protocol in[14]as the network layer protocol in our simulations.

Figure 1 shows the simulation average results of energy consumption ratio about the same selected destination node under running three schemes 800 seconds respectively, in simulation, we repeated each scheme 20 times and observed the destination node's energy value every 100 seconds, from the results of energy consumption ratio we can conclude that our scheme consumed the least energy among all schemes.

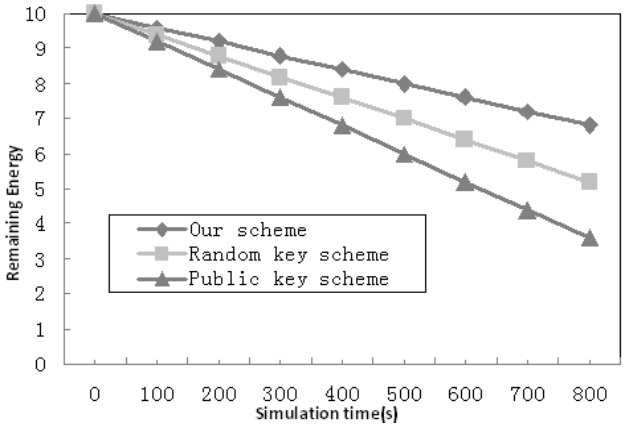

Figure 1 remaining energy of node in simulation

Figure 2 shows the mean probability of nodes be captured in different networks scale when w three schemes were run

respectively, in simulations we choose a mechanism called off-the-shelf in [15], which can modify the parameters set in destination nodes when feed it into networks' information stream. After running each scheme, we can judge whether the checked node has been captured from the parameters saved in the node. We adopt a strategy in [16], which described as follows: Setup an examination procedure called verifier; it can check whether the parameters in the test node had been changed, if the checked parameters in the node are different to the predetermined parameters, we can take the node as been captured. According to above strategy, we run three schemes 20 times under different number of node. The simulation results reveal that the proposed scheme is the most reliable.

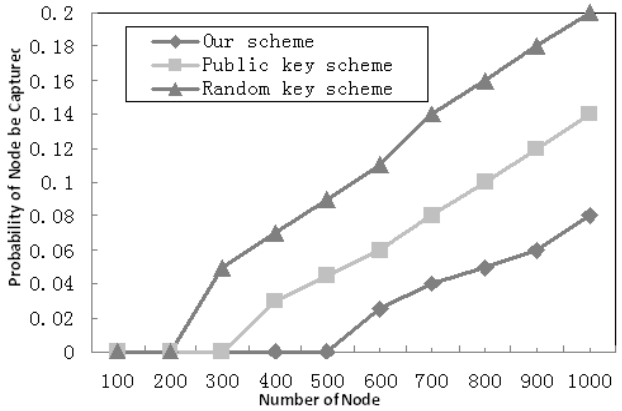

Figure 2 probability of nodes be captured under different number of nodes

5. CONCLUSIONS

In order to make health monitoring data secure for patients, in the paper, we propose an authenticated key establishment and encryption scheme for Wireless body sensor networks. The scheme includes key establishment, distribution and authenticated encryption/decryption phases, Analysis in efficiency and security shows that our scheme has some advantages in terms of key management, storage requirement and security. We compare the proposed scheme with the asymmetric and symmetric key techniques with detailed simulations. Results show that the proposed scheme has some advantages in the applications of wireless body sensor networks.

Acknowledgement

This work was supported in part by the "Six Kinds Peak Talents Plan" project of Jiangsu Province under Grant No. 11-JY-009; the Nature Science Foundation of Jiangsu Normal Higher University under Grant No. 11KJB510003; China Postdoctoral Science Foundation funded project under Grant No.2012M511732 and Jiangsu Province Postdoctoral Science Foundation funded project Grant No.1102014C.

References

[1] AKYILDIZ I.F, SU W, SANKARASUBRAMANIAM Y, "Wireless body sensor networks: A survey" [J]. computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

[2] C C. Y. POON AND Y-T ZHANG, "A NOVEL BIOMETRICS TO SECUREWIRELESS BODY AREA SENSOR NETWORKS FOR TELEMEDICINE AND M-HEALTH", IEEE Communications Magazine , vol: 44, no: 4, April 2006, pp. 73-81.

[3] PIETRO R D, MANCIN I L V, AND ANDMEI A "Random key assignment for secure Wireless body sensor networks," [C].in ACM Workshop on Security in Ad Hoc and Body wireless body sensor networks (SASN '03), pp. 62-71, 2003.

[4] ANIKET K, IAN G. DISTRIBUTED PRIVATE-KEY GENERATORS FOR IDENTITY-BASED CRYPTOGRAPHY[A]. Security and Cryptography for Networks[C]. 2010.436-453.. 4

[5] GURA N, PATEL A, WANDER A, EBERLE H et al. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," [C].in Proceedings of the Workshop on Cryptography Hardware and Embedded Systems (CHES 2004), Boston, August 11-13 2004.

[6] MALAN D J, WELSH M, AND SMITH M D, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography,"[C].in The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, pp. 71-79, October 2004.

[7] SHAMIR A, "Identity-based cryptography and signature schemes," [J]. Advances in Cryptology, CRYPTO'84, Lecture Notes in Computer Science, vol. 196, pp. 47-53, 1985.

[8] BONEH D AND FRANKLIN M, "Identity-based encryption from the Weil pairing," [J]. in Advances in Cryptology, CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, pp. 213-229,2001.

[9] Boyen X, "Multipurpose Identity-based signcryption, a Swiss army knife for identity-based cryptography," [C]. in Proceedings of the 23rd Interna. Conf. On Advances in Cryptology, Lecture Notes in Computer Science, vol. 2729, pp. 383-399, 2003.

[10] ABDALLA M, BIRKETT J, CATALANO D, et al. Wildcarded identity-based encryption[J]. Journal of Cryptology, 2011, 24(1): 42-82..

[11] CHENG H B, YANG G, WANG J T, HUANG X. An authenticated identity_based key establishment and encryption scheme for Wireless sensor networks [J]. The Journal of China University of Posts and telecommunications, 2006, 13(2):31-38.

[12] KALPAKIS K, DASGUPTA K, NAMJOSHI P. Efficient algorithms for maximum lifetime data gathering and aggregation in Wireless sensor networks. ACM Computer Networks, 2003,42(6):697-716.

[13] INTANAGONWIWAT C, GOVINDAN R, ESTRIN D, HEIDEMANN J, SILVA F. Directed diffusion for Wireless body sensor networking. IEEE/ACM Trans. on Networking, 2003,11(1):2-16.

[14] C. INTANAGONWIWAT, R. GOVINDAN, D. ESTRIN, J. HEIDEMANN, AND F. SILVA, "DIRECTED DIFFUSION FOR WIRELESS SENSOR NETWORKING", IEEE Trans. Networking, vol. 11,no. 1,pp.2 -16 2003

[15] HARTUNG C., BALASALLE J., AND HAN R., "Node Compromise in Body wireless body sensor networks: The Need for Secure Systems," Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado, Boulder, 2004.

[16] SESHADRI,A., et al., "Swatt: Software-based Attestation for sensor node device" Proc. IEEE Symposium on Security and Privacy, Oakland, CA, May 2004.