ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

Secure and Energy Efficient Hierarchical Public-Key Cryptosystem For Data Protection In Wireless Sensor Network

O. Sheela, PG Student and T. Samraj Lawrence, Asst. Professor.
Francis Xavier Engineering College, Tirunelveli
Email Id: sheelaoerter@gmail.com

Abstract - In Wireless Sensor Networks (WSN), the wireless connections are prone to different type of attacks. Therefore, security of the data that transfer over the wireless network is a measure concern in WSN. Due to the limitation of nodes' energy, efficient energy utilization is also an important factor. Hence to provide security along with efficient energy utilization of sensor nodes, Secure and Energy Efficient Hierarchical Public-Key Cryptosystem (HiPC) scheme is proposed. To serve a large amount of sensors, HiPC provides a hierarchical cluster-based framework consisting of a several Area Clusters and a Backbone Network. To provide security Elliptic Curve Cryptography (ECC) is used. For energy efficient data transmission, Low Energy Adaptive Clustering Hierarchy (LEACH) is used to select the Cluster Head dynamically. Each Cluster Head collects the data from their own cluster and transmit to the Destination through the Gateway (GW) in the Backbone Network. However, limited by the coverage of Gateway, Source Gateway may not be directly linked with the Destination Gateway in a single hop, so needs to hop through other Gateways to reach the Destination. Data encryption using Elliptic Curve Cryptography provides high security with small key size than the existing RSA. Key management includes key computation, key exchanges, data encryption and decryption. Cluster-based cryptographic mechanism provides efficient energy utilization of sensor nodes along with security and lower message overhead. Thus, HiPC can protect the confidentiality of sensitive data with low computation complexity, and keep appropriate network performance for Wireless Sensor Network.

Keywords - Elliptic Curve Cryptography, LEACH Protocol, Wireless Sensor Network, Hierarchical Cluster, Data Protection, Public-Key Cryptosystem.

1. INTRODUCTION

Wireless sensor networks (WSNs) comprise a large number of spatially distributed small autonomous devices (called sensor nodes) cooperatively monitoring environmental conditions and sending the collected data to a command center using wireless channels [1]. Because of the size and cost of sensor nodes there is a constraint on energy, memory, computation speed and bandwidth. Most of the applications of WSN needs secure communication.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

Because of the absence of the physical protection and the unattended deployment wireless communication and sensor nodes are prone to different type of attacks such as: impersonation, masquerading, spoofing and interception etc. Hence, a security mechanism in WSN is an important concern. Different security mechanisms in WSN are described in [2] and [3].

For implementing key management in WSN, it is important to select appropriate cryptographic methods. The constraints of sensor nodes in WSNs should meet by the Cryptographic methods. These cryptographic methods could be evaluated by size of the code, size of the data, time taken for processing, and consumption of the power by the sensor nodes. Security mechanisms can be implemented by using public key cryptography or symmetric key cryptography. Most important public key algorithms include RSA, and Elliptic Curve Cryptography (ECC).

In RSA to implement security operations thousands of multiplication instructions are performed, which is time consuming. It was found that encryption and decryption operations in RSA usually take on the order of tens of seconds. Recent studies have shown that it is possible to apply public key cryptography to sensor networks by selecting proper algorithms and associated parameters. Most of the literature studies gives emphasis on RSA and ECC algorithms. Researchers are more attracted towards ECC, because it provides same level of security with much smaller key size. For example, RSA with 1024 bit key provides a valid level of security whereas ECC with 160 bit key provides same level of security. The operation of the RSA private key limits its use in sensor nodes. ECC has no such problem because both the private key and public key operation use the same point multiplication operations.

II. RELATED WORKS

Haythem Hayouni, Mohamed Hamdi, Tai-Hoon Kim discussed about Encryption Schemes in Wireless Sensor Networks. As Wireless Sensor Networks (WSN) continues to grow, so does the need for effective security mechanisms. Enhancing the efficiency of these networks requires more security to provide integrity, authenticity and confidentiality of the data flowing through the network. Encryption is one of the most common tools used to provide security services for WSNs. There has been an enormous research potential in the field of encryption algorithms in WSNs. Algorithms, protocols, and implementation consist the main aspects the security specialist should consider to assess the efficiency of the protection approaches. It reviews the most significant approaches that have been proposed to provide encryption-based security services for WSNs. It also emphasize on the weaknesses of the approaches[4].

The Rivest-Shamir-Adleman (RSA)-based public key solution is also used to protect data privacy [5]. However, few works can provide solutions for strong data confidentiality and low message overhead simultaneously.

Kristin Lauter [6] discussed about the advantages of Elliptic curve cryptography for Wireless security. It provides an overview of elliptic curves and their use in cryptography. The focus is on the performance advantages to be obtained in the wireless environment by using elliptic

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

curve cryptography instead of a traditional cryptosystem like RSA. Specific applications to secure messaging and identity-based encryption are discussed.

Besides, to keep the privacy of data, other research focuses on encryption algorithms, including attribute-based encryption [10], fuzzy attribute-based signcryption [11].

In [7], Kamlesh Gupta, Sanjay Silakari discusses about ECC over RSA for Asymmetric Encryption. Cryptography is used to transmit the data securely in open network. ECC is a when compared to RSA and discrete logarithm systems, is a better option for the future. For this reason ECC is such an excellent choice for doing asymmetric cryptography in portable devices right now. The smaller ECC keys it turn makes the cryptographic operations that must be performed by the communicating devices to be embedded into considerably smaller hardware, so that software applications may complete cryptographic operations with fewer processor cycles, and operations can be performed much faster, while still retaining equivalent security. This means, in turn, reduced power consumption, less space consumed on the printed circuit board, and software applications that run more rapidly make lower memory demands. In brief, for communication using smaller devices and asymmetric cryptosystem, ECC is needed.

Ramesh K and Somasundaram K discussed about cluster head Selection algorithms in Wireless Sensor Network sensor nodes. In Wireless Sensor Network, life time is the most critical parameter. Many researches on these lifetime extension are motivated by LEACH scheme, which by allowing rotation of cluster head role among the sensor nodes tries to distribute the energy consumption over all nodes in the network. Selection of cluster head for such rotation greatly affects the energy efficiency of the network [8].

Most important public key algorithms include RSA, and Elliptic Curve Cryptography (ECC). In RSA to implement security operations thousands of multiplication instructions are performed, which is time consuming. It was found that encryption and decryption operations in RSA usually take on the order of tens of seconds.

The Rivest-Shamir-Adleman (RSA)-based Public key solution is also used to protect data privacy [12]. However, few works can provide solutions for strong data confidentiality and low message overhead simultaneously. Cluster hierarchy is highly flexible and easily managed because of its great extensibility for large scale sensor networks [13].

In the existing system, the security of the data communication is provided through RSA. RSA is a public key cryptography. The data is encrypted using the public key and it is decrypted using the private key. It uses 1024 bit key. Data are directly sent and received through the Gateway. Each data element is encrypted and only the users with the appropriate decryption keys can decrypt the data. It is a centralized architecture. The main disadvantage of the existing system is message overhead occurred due to centralized architecture. Since RSA uses 1024 bit key, it needs high energy for computation.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

III. HIERARCHICAL ARCHITECTURE FOR DATA PROTECTION

In the proposed system, Hierarchical Public-Key Cryptosystem is used. To overcome message overhead, Hierarchical structure is proposed. To serve a large amount of sensors, Hierarchical Public-Key Cryptosystem (HiPC) provides a hierarchical cluster-based framework consisting of a Backbone Network and several Area Clusters. Backbone Network are formed by connect together many Gateways. Sensor Nodes in the WSN are group together based on area to form an Area Cluster (AC). Area Cluster consists of Cluster Head (CH), Sensor Nodes and the Gateway. Hierarchical structure consists of Source Node, Cluster Head, and Gateway.

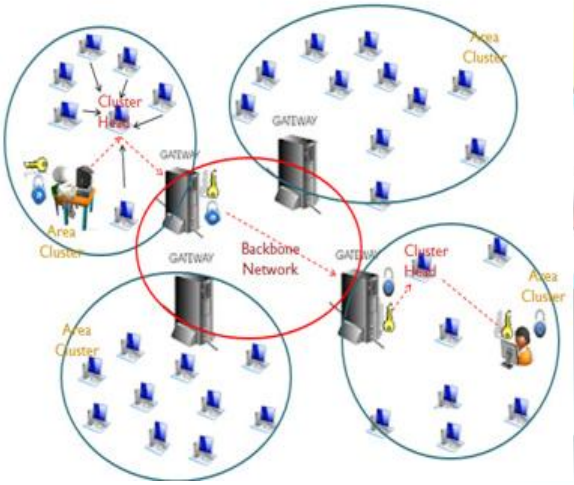

Figure 1 System Architecture

Each Area Cluster is Hierarchical. For energy efficient data transmission, Low Energy Adaptive Clustering Hierarchy (LEACH) is used to select the Cluster Head dynamically.

The Cluster Head collects the data from the Source Node and transmit it to the Destination through the Gateway (GW) in the Backbone Network. Key management includes key computation, key exchanges, data encryption and decryption.

The system architecture is shown in Figure 1. The encrypted data from the source is gathering by the Cluster Head, one of the nodes in the Area Cluster. And the Cluster Head transmit the data to the Gateway. In the Gateway the data is again encrypted. The double encrypted data is passed through the Backbone Network to the destination.

In the destination Area Cluster the data gets decrypted in the Gateway and transmit to the destination node through the Cluster Head. In destination again the date gets decrypted to get the original data. Encryption and decryption process is done using Elliptic Curve Cryptography. Dynamic Cluster Head selection is done using LEACH mechanism.

The system implementation is done in three processes: Cluster Head Selection, Encryption Process, and Decryption Process.

A. Cluster Head Selection

First, the Cluster Head for both Source and Destination Area Cluster is selected by using the Low Energy Adaptive Clustering Hierarchy (LEACH) mechanism. By using LEACH protocol, Cluster Head is selected dynamically. Sometimes the Source Node or the Destination Node itself acts as the Cluster Head. By LEACH, threshold value of the each node is calculated.

The threshold function is defined as

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

$$T(n) = \begin{cases} \frac{p}{1-p\left(r \bmod \left(\frac{1}{p}\right)\right)} & if n \in G \\ 0 & otherwise \end{cases}$$

Where n is the given node, p is the a priori probability of a node being elected as a Cluster Head, r is the current round number and G is the set of nodes that have not been elected as Cluster Heads in the last 1/p rounds. Each node during Cluster Head selection will generate a random number between 0 and 1. If the number is less than the threshold (T (n)), the node will become a Cluster Head.

B. Encryption Process

The data is first encrypted in the source using the public key of the sender using Elliptic Curve Cryptography. Cluster Head (CH) collects the encrypted data from the source and transmits to the Gateway. In Gateway (GW) again the encrypted data is encrypted with the public key of the Gateway.

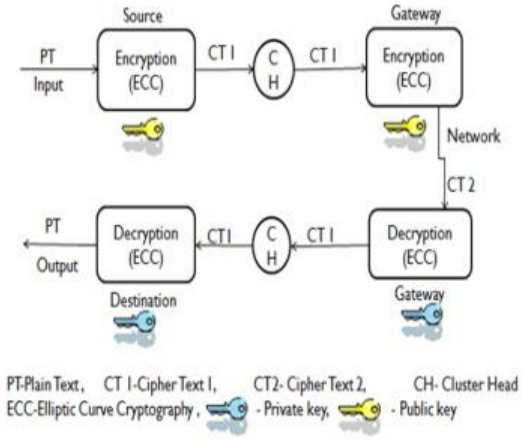

Figure 2 Encryption/Decryption Process

C. Decryption Process

The Gateway of the destination decrypts the data with the private key of the Gateway. Then Cluster Head gather the data from the Gateway. Cluster Head transmits the encrypted data to the destination. In destination, the encrypted data is decrypted using the receiver private key. The Cluster Head is automatically changed during the data transmission. Figure 2 shows the encryption and decryption process of the data using Elliptic Curve Cryptography.

Encryption/Decryption Algorithm:

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Every user has a public and a private key. Public key is used for encryption/signature verification. Private Key is used for decryption/signature generation. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Let A be a sender node that sent a message 'M' to the receiver node B. Let Gateway G_a is the Gateway in the sender Area Cluster and G_b is the Gateway in the receiver Area Cluster. Let Pu_a, Pu_b are the Public Key of A and B. Let Pr_a, Pr_b be the Private key of A and B. Every nodes can have their own private key. Suppose message is sent from A to B through G_a, G_b. Randomly select 'k' from 1 to (n-1). 'n' be the number of nodes. 'P' is a point on the Elliptic Curve

$$y^2 = x^3 + ax + b$$

The public key is calculated by

$$Pu_a = k * P$$

$$Pu_b = k * P$$

The message M is first encrypted by A using its the pubic key.

$$C_1 = k * P$$

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

$C_2 = M + k * P$

C_1 and C_2 are the Ciper Text of A. Again the C_1 and C_2 are encrypted in G_a by its Public key using ECC algorithm. Christo Ananth et al. [9] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results.

Now the C_1 and C_2 are sent to the receiver Gateway in the Backbone Network.

In G_b decryption is done using ECC algorithm by using its Private Key. Now the Encrypted message is decrypted using the Private Key Pr_b in the receiver node B by the below formula

$$M = C_2 - Pr_b * C_1$$

Thus the original message M is get by the node B. For key exchange, Diffie Hellman Key exchange algorithm is used.

IV RESULTS

For network and computation performance analysis, we evaluate the HiPC in the famous network simulator, ns2. 50 nodes are group together to form 7 cluster. Each have an Gateway. Cluster Head for both the source and destination Area Cluster is selected by using the LEACH protocol as shown in the Figure 3.

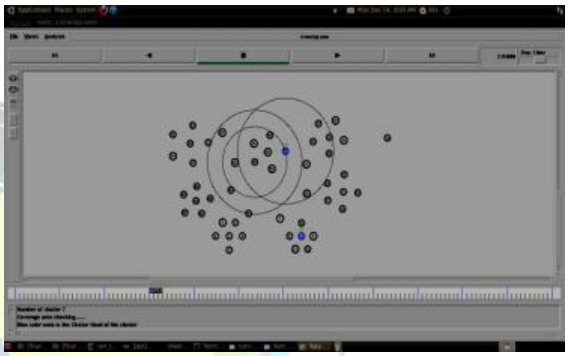

Figure 3 Cluster Head Selection

The data send by the sender is first encrypted using ECC. Then it can be collected by the Cluster Head in the Area Cluster. It can be send to the Gateway (GW). The data is again encrypted in GW using ECC for the second time as shown in Figure 4.

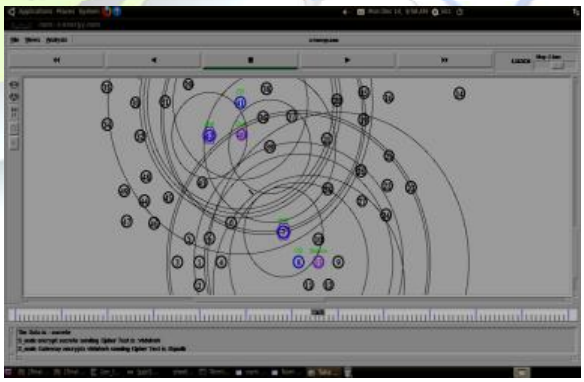

Figure 4 Encryption Process using ECC

The Destination Area Cluster receives data through the Gateway which is

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

connected to the Backbone Network. The dynamically selected Cluster Head receives the data from the Gateway and transmit it to the receiver. The data get decrypted using ECC is received by the receiver as shown in the Figure 5.

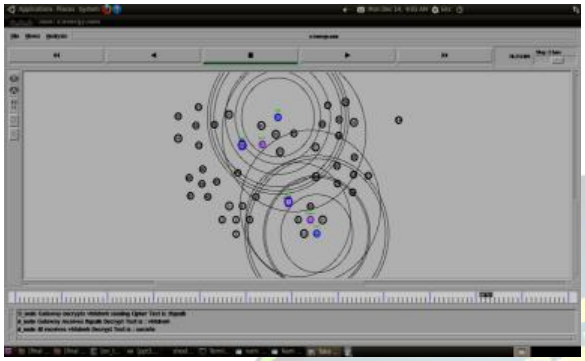

Figure 5 Decryption Process using ECC

The packet delivery ratio of the data encryption using both the existing RSA and the proposed HiPC is shown in the Figure 6. It shows that the packet delivery rate of data is more in ECC than the RSA.

In Figure 7, the comparison of the throughput of both RSA and HiPC

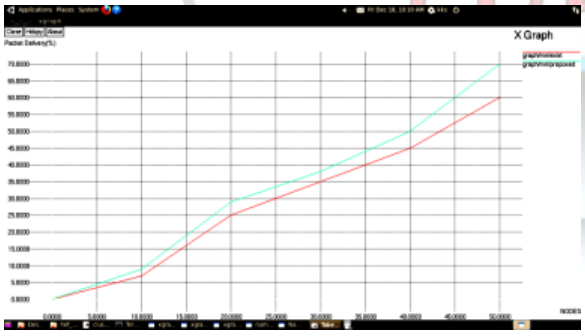

Figure 6 Comparison of Packet Delivery

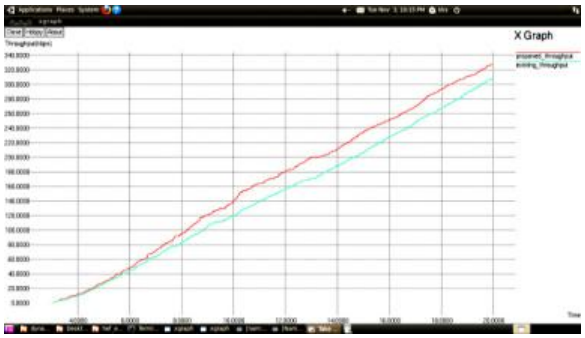

Figure 7 Comparison of Throughput Graph

is shown as graph. It shows that the throughput is high for ECC than the RSA algorithm used for encryption and decryption of data.

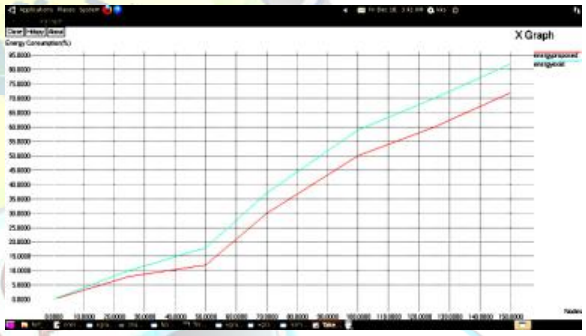

Figure 9 Energy Consumption comparison Graph

Figure 9 shows the comparison of the existing RSA and the proposed HiPC energy consumption graph.

V CONCLUSION AND FUTURE WORK

In the proposed system, security for the data transmission is provided using Elliptic Curve Cryptography (ECC) which provides high security than the traditional RSA with smaller key size. Computation is also less because the use of the ECC with smaller key size. Energy need for

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

computation is also less, which lead to low energy consumption in sensor nodes. Simulation results shows that the proposed system provide high security, low computational complexity than the existing RSA. Thus, the Cluster based Cryptographic mechanism; Secure and Energy Efficient Hierarchical Public-Key Cryptosystem (HiPC) provide high security for data transmission and it is also highly energy efficient.

The future plan is to develop a trust and reputation management system to monitor the behavior of nodes and identify security attacks in advance. Also implement the protocol for data and key encryption. Moreover, it is plan to implement it in large scale sensor networks to evaluate overall message throughput and latency. It can protect the confidentiality of sensitive data with low computation overhead, and keep appropriate network performance for wireless sensor networks. Also doing the same process to do at only time for encrypt and decrypt, it will help to minimization of time and delay. Also the data will be sending secure.

VI REFERENCES

[1] Junqi Zhang,Vijay Varadharajan, "Wireless sensor network key management survey and taxonomy"; Journal of Network and Computer Applications, vol. 33, pp.63-75, 2010.

[2] X Chen, K Makki, K Yen and N Pissinou; "Sensor Network Security: A Survey";IEEE communication survey and tutorials, vol. 11, pp. 52-73, 2009.

[3] Yong Wang, Garhan Attebury, Byrav Ramamurthy; "A Survey of Security Issues In Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, volume 8, pp. 2-23, 2nd quarter 2006.

[4] Haythem Hayouni, Mohamed Hamdi and Tai-Hoon Kim, 'A Survey on Encryption Schemes inWireless Sensor Networks' 7th International Conference on Advanced Software Engineering & Its Applications, 2014.

[5] Soufiene Ben Othman, Abdelbasset Trad and Habib Youssef, 'Performance Evaluation Of Encryption Algorithm For Wireless Sensor Networks', International Conference on Information Technology and e-Services, 2012.

[6] Lauter K, 'The advantages of elliptic curve cryptography for wireless security', IEEE Wireless Commun., Vol. 11, No. 1, pp. 62–67, 2004.

[7] Kamlesh Gupta and Sanjay Silakari, 'ECC over RSA for Asymmetric Encryption: A Review', IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, 2011.

[8] Ramesh K. and Somasundaram K. , 'A comparative study of clusterhead selection algorithms in wireless sensor networks', International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, 2011.

[9] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[10] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," IEEE Trans. Parallel Distrib.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

Syst., Vol. 22, No. 4, pp. 673–686, 2011.

[11] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body Area network security: A fuzzy attribute-based signcryption scheme," IEEE J. Select. Areas Commun. (JSAC), Vol. 31, No. 9, pp. 37–46, 2013.

[12] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," IEEE Trans. Inf. Technol. Biomed., Vol. 13, No. 6, pp. 946–954, 2009.

[13] Y. Cheng and D. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," Ad Hoc Netw., Vol. 5, No. 1, pp. 35–48, 2007.

[14] Chin yang Henry Tseng, Shiau-Huey Wang, and Woei-Jiunn Tsaur, 'Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection', IEEE Transactions on Reliability, Vol. 64, No. 3, 2015.