ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

# An Improved Scheme of Encryption for Energy Efficient Security in Wireless Sensor Networks

Vandana[1], Reeti Kamboj[2]

Department of Electronics & Communication Engineering, Maharishi Ved Vyas Engineering College, Jagadhri, India[1,2]

**ABSTRACT**: With the increasing use of Wireless Sensor Networks (WSN) in more and more fileds, security of data transfer becomes a major concern in research filed [12]. The secret key cryptography is not able to provide a sense of security in WSN given the nature of deployment area in the most of the applications. Key distribution remains a major problem in secret key cryptography [4]. Recently many public key cryptography based algorithms have been defined. In these foremost is homomorphic algorithms[14] but they are very costly on scarce resource in WSN i.e. Battery life. This paper proposes a new encryption scheme for achieving energy efficiency and security for LEACH-C [9] protocol in wireless sensor network. The proposed scheme uses a hybrid scheme comprising both type of encryption schemes i.e. Secrete key cryptography and public key cryptography both. In the proposed scheme the session key is distributed to various nodes using public key cryptography scheme which enhances security of network and also consumes less energy. For data aggregation plain method (in-network data aggregation) is used. The proposed method is compared with public key cryptography with concealed data aggregation and in network data aggregation. The result shows that the proposed scheme achieved higher energy efficiency as compared to other two comparable schemes without compromising security environment in data transfer.

**KEYWORDS:** Public Key Cryptography, Secret Key Cryptography, Concealed Data Aggregation, In Network Aggregation, LEACH-C

## I. INTRODUCTION

Wireless sensor networks consist of small nodes that sense their environment, process data, and communicate through wireless links [1] [10]. They are expected to support a wide variety of applications, many of which have at least some requirements for security [2].

Cryptographic algorithm for authentication and encryption can be implemented in two ways: using public keys or private keys. When using public keys, the key value of every node is public information, and is therefore known by all other nodes. When a node wants to communicate privately with another node, the source node simply encrypts data using the public key of the sink node. In this case, only the sink node can correctly decrypt the data. This method is called asymmetric key encryption because the two communicating nodes use different keys during the session.

When using private keys, nodes must first agree on a key before they can communicate securely. One possibility is to use public keys to encrypt data from which private keys can be derived. Private Key algorithms are based on symmetric key encryption because both communicating nodes use the same keys for encrypting and decrypting data [3]. In wired data networks, nodes rely on pre-deployed trusted server to help establish trust relationships but in WSN, these trusted authorities do not exist because sensor nodes have limited memory, CPU power, and energy, hence cryptographic algorithms must be selected carefully. The proper analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations [12]. The security requirements in WSNs include Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks, Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients, Integrity, which ensures that a message sent from one node to another, is not modified by malicious

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

intermediate nodes, Authorization, which ensures that only authorized sensors, can be involved in providing information to network services, Authentication, which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node, Non-repudiation, which denotes that a node cannot deny sending a message and Freshness, which implies that the data is recent and ensures that no adversary can replay old messages [4].

This paper is organized into five parts. In section 1, WSN and its security requirement is introduced. Section 2 describes security problem and its associated solutions and formulations. Section 3 explains methodology, simulation environment and parameters used in analysis. Section 4 deals with result and discussion followed by conclusion.

## II. MOTIVATION

In a sensor mote a small amount of resources are left for security to be implemented. This is insufficient to even hold the variables for asymmetric public key based cryptographic algorithms like RSA and Diffie-Hellman. Thus public key based systems do not work for sensor networks. Because of the resource constraints another solution is to use global keys. This is feasible but a global key based system does not provide the desired level of security. On the contrary, complete pair-wise keying between nodes provides the best possible security, but it is not a choice for sensor network because of the resource constraints [5].

The simplest method of key distribution is to preload a single network-wide key into all nodes before deployment[14]. Only one single key is stored in the nodes' memory and once deployed in the network, there is no need for a node to perform key discovery or key exchange since all the nodes in communication range can transfer messages using the key which they already share. On the other hand, this scheme suffers a severe drawback that compromise of a single node would cause compromise of the entire network through the shared key. Thus it fails in providing the basic secure requirement of a sensor network by making it easy for an adversary trying to attack [8].

An alternative key distribution scheme is fully pairwise keys scheme, i.e., every node in the sensor network shares a distinct key with every other node in the network. The main problem with this pairwise key scheme is its poor scalability. The number of keys that must be stored in each node is proportional to the total number of nodes in the network. Since sensor nodes are resource-constrained, this brings significant overhead which limits the scheme's applicability except for it can only be effectively used in smaller networks.

The method of Kerberos-like key distribution is popular in a lot of networks environment. In sensor networks, we can use a trusted, secure base station as an arbiter to provide link keys to sensor nodes. The sensor nodes authenticate themselves to the base station, after which the base station generates a link key and sends it to both parties securely. An example of such a protocol is SNEP, a part of the SPINS security infrastructure [6] [7]. However, this kind of schemes suffers high energy consumption, which makes it inapplicable in most of sensor network applications. A detail discussion and research initiatives taken in the past decade have been presented in the next chapter.

The proposed work is about to use some security techniques in LEACH-C protocol to provide a full proof security by using less energy and more rounds of transmission to BS. For this, several alternates are proposed to increase the overall security scenario and consume less energy. Finally proposed schemes are explained and these are compared for energy consumption.

## III. METHODOLOGY

This section discusses methodology for simulation and various schemes of encryption those can be used in WSN and their energy consumption behavior. These encryption schemes may constitute both types of encryption techniques; public key cryptography and secret cryptography. Our main idea in this thesis is to make a tradeoff between security and energy requirements in WSN.

There are two major techniques for data encryption which provide security and authentication for data. Secret key cryptography (SKC) provides high level of security and consumes less resources as compared to public key cryptography (PKC), but key distribution and management is a major problem of SKC [15]. It also doesn't provide

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

authentication and leaves this activity on the shoulders of third party which is not viable for Wireless Sensor Network scenario. The PKC provides data security and as well as authentication but constitutes complex computation and consumes more energy as compared to SKC. Public Key cryptographic Algorithms (Homomorphic encryption) is a form of encryption which allows specific types of computations to be carried out on ciphertext and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. For instance, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers.

Data aggregation is an essential data processing primitive in sensor networks. Sensor nodes forward data towards the sink. Sensor nodes closer to the sink receive data from nodes further away; they aggregate the information into concise digests. The aggregated data is encrypted using Privacy Homomorphic algorithms. This enables end-to-end security. Thus implements confidentiality and integrity to the data being transferred. This results into significant energy savings over having each node forward their respective readings directly to the sink.

***Selection of Sensor Node*:**

Piotrowski et al. [13] investigated four types of nodes; MICA2DOT, MICA2, MICAz, and TelosB, and estimated the power consumption for most common RSA and ECC operations. Their work gives an indication of how public key cryptography influences a wireless node's lifetime. In our simulation we consider the most efficient sensors i.e. TelosB of Texas Instruments. The specification for TelosB is with 3V power supply is as following:

TelosB with TI MSP430F1611 at 8 MHz, 4mA*3V □ 12 mW,–>> 12 mW / 8MHz = 1.5 nWs,

***Power consumption caused by applying different Algorithms of Cryptography:***

The application of cryptography involves many mechanisms that create the environment for the main operations like encryption, decryption, signature generation and verification. The cost of modular exponentiation (RSA) or point multiplication (ECC) is of course the main indicator of the implementation's efficiency. But besides these two operations cryptography requires also additional operations, e.g., hash value calculations, random number generation and testing if a number is a prime.

Sensor nodes are assumed of the type of TelosB containing ZigBee transceiver CC2420. Below is the power consumption for signature generation and verification and key exchange for client side and server side of TelosB estimated by Piotrowski and others [13]. Other power consumption rating for different data communication we have assumed as

**Table 1** Power consumption calculated at 3V supply voltage. Power consumption per bit at transmission speed of 250 kbit/s with 0 dBm output power

| | | |
|---|---|---|
| Length | Length of the field Area | 200 m |
| Width | Width of the field Area | 200 m |
| bsX | x coordination of base station | 100 m |
| bsY | y coordination of base station | 300 m |
| initEnergy | Initial energy of each node | 5000 Ws |
| transEnergy | Energy for transferring of each bit (ETX) | 0.209e-6 Ws/bit |
| recEnergy | Energy for receiving of each bit (ETX) | 0.226e-6 Ws/bit |
| fsEnergy | Energy of free space model | 10e-12 Ws/bit |
| mpEnergy | Energy of multi path model | 1.3e-15 Ws/bit |
| aggrEnergy | Data aggregation energy | 5e-9 Ws/bit |
| SigEnergy | Signature generation energy | 68.97e-3 Ws/bit for RSA-1024 |
| SivEnergy | Signature verification energy | 2.70e-3 Ws/bit for RSA-1024 |
| KeyExEnergy | Key exchange energy | 15.40e-3 Ws/bit of key |
| EncEnergy | Encryption Energy (AES) | 2.025e-7 Ws/bit |

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

***Proposed Simulation of Encryption Schemes***

In this thesis, we have considered three encryption schemes for simulation purpose. These are described in the following paragraphs.

**Scheme 1: Public Key Cryptography Scheme with concealed data aggregation (PKC-CDA):**

In the first scheme, the sensor nodes encrypt data using RSA homomorphic algorithm signature generation. Cluster heads aggregate the whole data into one without decrypting it and again sending data to base station. This type of scheme is also called Public Key Cryptography Scheme (PKC) with concealed data aggregation.

**Scheme 2: Public Key Cryptography Scheme with using in-network data aggregation (PKC-INA):**

In this scheme, the sensor nodes encrypt a newly generated session key using homomorphic algorithm signature. The sensor node use this session key to encrypt data using AES algorithm and then homomorphic encrypted session key and session key encrypted data is sent to the Cluster heads(CHs). CHs decrypt data using session key which is retrieved by CH's own private key and then aggregate the whole data into one and again use homomorphic encryption for sending session key and session key encrypted data to base station. This type of scheme is also called Homomorphic Encryption Scheme (HES) using in-network data aggregation or simply Public Key Cryptography Scheme with using in-network data aggregation (PKC-INA)

**Scheme 3: Key distribution based scheme (KDS):**

In this scheme, Base Station first distributes a common session key for each round which is encrypted by individual node's public keys. Each sensor node decrypts the session key using its own private key. This is also called key exchange mechanism. Once distribution of key is completed data can be sent to CH and BS using SKC's AES Algorithm. We call this Key Distribution based Scheme (KDS).

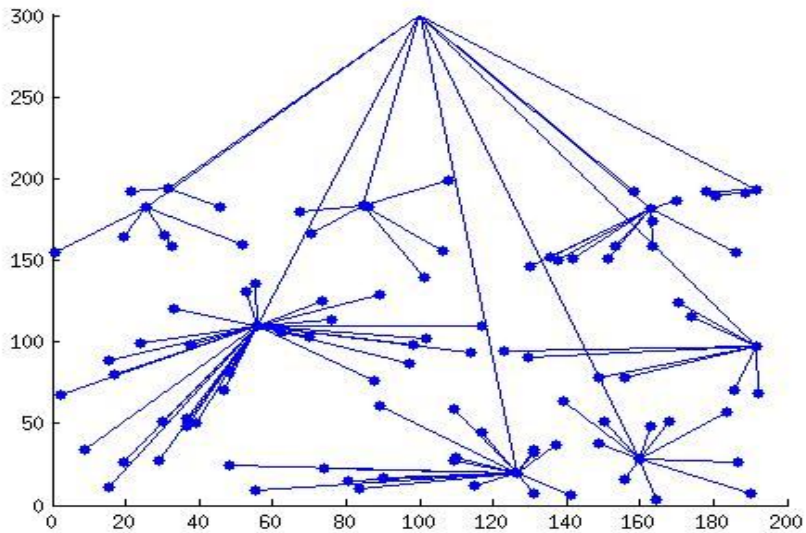


**Figure 1 WSN Node Deployment**

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

***LEACH Simulations- Algorithm***

100 nodes positions are generated randomly in a 200*200 m2 area and a BS is also placed at (100, 300) position. The result of this deployment is shown in figure 4.1. The Base station (BS) is far away from the node deployment area. In the starting every node is having equal energy i.e. 5000 Joules and all nodes are live nodes

The algorithm for above deployment and simulation is given below:

**Step 1:** Create the network architecture with desired parameters

**Step 1.1** Create the field Area

**Step 1.1.1** x and y Coordinates of the base station

bsX=x coordination of BS

bsY=y coordination of BS

**Step 1.1.2** Create the node model randomly

x coordination of nodes

y coordination of nodes

**Step 1.1.3** initially there are no cluster heads, only nodes 1 for 'N' =non-CH node, 2 for 'C' = CH node,3 for 'D'= Dead node

**Step 1.2** Energy Model (all values in Joules)

- Specify Initial Energy of node
- Specify Energy for transferring/ receiving of each bit (ETX)
- Transmit/receive Amplifier types
- Energy free space;
- Energy multi path
- Data Aggregation Energy
- Signature generation energy
- Signature verification energy
- Key exchange energy
- Encryption Energy (AES)

**Step 2:** plot field area with its nodes and BS

**Step 3:** for each round

**Step 3.1** Create the new node architecture using max energy leach algorithm (LEACH-C) in beginning of each round. Max Energy leach algorithm in which nodes are selected CHs according to their remaining energy and number of CHs is fixed as p*liveNodes. [9].

**Step 3.2:** if (any cluster is formed during round)

Find Energy dissipation patterns for nodes (Ref section 4.10)

End if

End for

Step 4: Display number of packets sent from CH, energy dissipation per round and dead node pattern for each round

Finally when clusters are formed then packets are sent from non-CH nodes to CH nodes and finally CHs nodes sent their packets to BS. The CHs also consumes energy in data aggregation and receiving. All nodes consume transmitting energy. Energy dissipation for nodes is a factor of distance from BS. This decides whether to use free space or multipath transmitter. In our simulation we take a distance d0 as sqrt(Efs/Emp).This becomes the criterion for using free space energy or multipath energy scenario. Every cluster node consumes its energy for transmission of data in circuitary, receiving of data from non- cluster head nodes, data aggregation and data radiating to BS.

## IV. RESULT AND DISCUSSION

Following table shows the results obtained from the experimentations done as per the setup explained in the previous section. Three algorithms have been implemented in this thesis. In the first algorithm, sensor nodes encrypt data using

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

RSA based homomorphic algorithm signature generation. Cluster heads aggregate the whole data into one without decrypting it and again sending data to base station. This type of scheme is also called Public Key Cryptography Scheme (PKC) with concealed data aggregation (PKC-CDA).

Further a new scheme is considered in which a newly generated session key using RSA homomorphic algorithm signature. The sensor node use this session key to encrypt data using AES algorithm and then RSA encrypted session key and session key encrypted data is sent to the Cluster heads(CHs). CHs decrypt data using session key which is retrieved by CH's own private key and then aggregate the whole data into one and again use RSA encryption for sending session key and session key encrypted data to base station. This type of scheme is also called Homomorphic Encryption based Scheme (HES) using in-network data aggregation or Public Key Cryptography Scheme (PKC) with in-network data aggregation (PKC-INA).

Third algorithm uses RSA based key distribution in which base station first distributes a common session key for each round which is encrypted by individual node's public keys. Each sensor node decrypts the session key using its own private key. This is also called key exchange mechanism. We call this Key Distribution based Scheme (KDS).

**Table 2. Experimentation Results**

| Algorithm | Life (Rounds) | FND (Rounds) | HND (Rounds) | PS to BS | Residual energy (jouls) | Encryption Security Level |
|---|---|---|---|---|---|---|
| **PKC-CDA** | 623 | 602 | 608 | 9132 | 540 | Very high |
| **PKC-INA** | 624 | 606 | 613 | 9187 | 13 | High |
| **KDS** | 3086 | 3066 | 3071 | 46084 | 9 | High |

The underlying routing protocol for these schemes is Max Energy Leach which is efficient in energy equi-distribution in the network which helps in elongated life time and delayed death of network. In this method a fix number of CHs are selected based on the residual energy of nodes that are alive. The live non-CH nodes become a part of cluster with the nearest CH. Once clusters are formed CHs collects data from its cluster nodes and send it to BS by following one of the above described schemes of data encryption. This scheme is also called LEACH-C. In the table it is clearly shown that proposed SCHEME3: (RSA Key Exchange Based LEACH-C) performs better as compared to other methods. The RSA Key Exchange Based LEACH-C performs nearly five times better than other schemes. If we consider a network dead if 50% nodes are dead then RSA Key Exchange Based LEACH-C is performing better than other schemes. If we consider 90% dead node criterion for network life then still performs better than other two algorithms.

If we compare the number of dead nodes as per our simulation results RSA Key Exchange Based LEACH-C seems to perform better, but there nodes once start dying accelerates network decay very fast. Due to the implementation of these schemes with LEACH-C algorithm the network disintegration is very late in all schemes.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

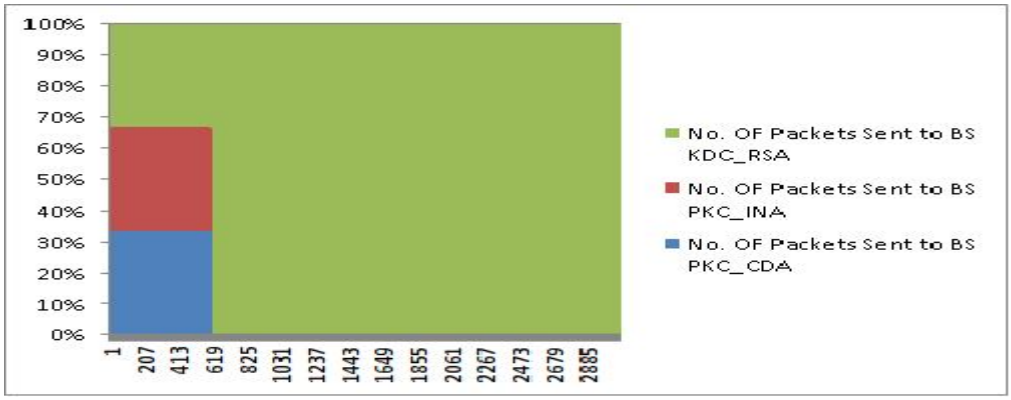


Figure 2: Results for no of packet sent to BS

If we consider no of packets sent to BS then RSA Key Exchange Based LEACH-C scheme is clearly winner. This has sent highest number of packets to BS. This is also true if we consider the ratio between packet sent and no. of rounds performed by the algorithm. This can be confirmed by the figures 2 to 4. These shows the comparative analysis of these algorithms for all the parameters of remaining energy, no. of packet sent to BS and no. of dead nodes.

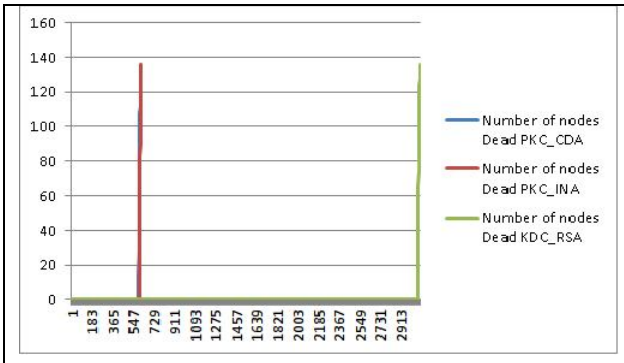


Figure 3: Results for No of dead nodes

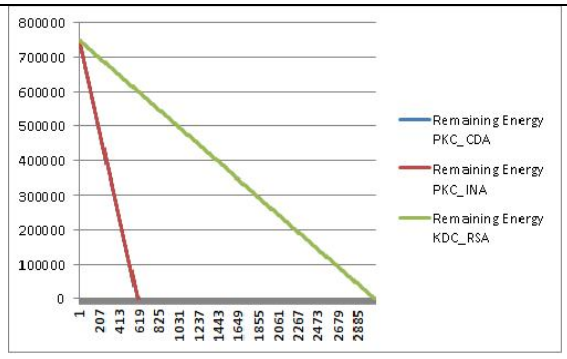


Figure 4: Experimentation Results for remaining energy per round

## V. CONCLUSION

We have measured performance of three cryptographic scheme for secured data routing in WSN. Parameters for performance measurements are Residual Energy, Dead Nodes, Packets sent to BS. These parameters are shown in above figures and are plotted against number of rounds. If we consider residual energy and total number of rounds then proposed RSA Key Exchange Based LEACH-C performs better than other two schemes. But residual energy at the end of total number of round shows that Max Energy LEACH most uniformly distributed energy dissipation among nodes in all the schemes because of use of LEACH-C in all schemes. In these experiments we have found that better performance can be achieved using RSA based key distribution for providing high security with very high energy efficiency. Although public key cryptography based scheme such as PKC with CDA provide very high security but it is very costly.

## REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks, vol. 38, Issue 4, pp. 393-422, 2002.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2014**

[2] C.Y Chong, S. P. Kumar., Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE , vol. 91, no. 8, pp. 1247- 1256, 2003.
[3] Du, W., Wang, R., and Ning, P., "An Efficient Scheme for Authenticating Public Keys in Sensor Networks," Proceedings of ACM MobiHoc'05, Illinois, USA, 2005, pp. 58-67.
[4] T. Feng, C. Wang, W. Zhang, and L. Ruan. Confidentiality Protection for Distributed Sensor Data Aggregation. In IEEE The 27th Conference on Computer Communications (INFOCOM 2008), pages 56–60, 2008.
[5] Gaubatz, G., Kaps, J.-P., Ozturk, E., and Sunar, B., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 146-150, 2005.
[6] Gupta, V., Wurm, M., Zhu, Y., Millard, M., Fung, S., Gura, N., Eberle, H., and Shantz, S. C., "Sizzle: A Standards-based End-to-End Security Architecture for the Embedded Internet," SMLI TR-2005-145, June 2005.
[7] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. 2002. SPINS: security protocols for sensor networks. Wireless Networks, vol. 8, no. 5, pp.521-534, 2002.
[8] Haque, M. M., Pathan, A.-S. K., Choi, B. G., and Hong, C. S., "An Efficient PKC-Based Security Architecture for Wireless Sensor Networks," Proceedings of the IEEE Military Communications Conference (IEEE MILCOM 2007), Orlando, Florida, USA, October 29-31, 2007.
[9] W. Ye, J. Heizemann, and D. Estrin. An energy-efficient MAC protocol for wireless sensor networks. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. vol.3, pp. 1567- 1576, 2002.
[10] M. Ilyas and I. Mahgoub., Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, International Journal of Distributed Sensor Networks, vol. 4, no. 4, pp. 369- 369, 2008.
[11] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones. Applying Secure Data Aggregation techniques for a Structure and Density Independent Group Based Key Management Protocol. In Third International Symposium on Information Assurance and Security (IAS 2007), pages 44–49, 2007.
[12] Pathan, A.-S. K., Lee, H.-W., and Hong, C. S., "Security in Wireless Sensor Networks: Issues and Challenges," Proceedings of 8th IEEE ICACT 2006, Volume II, 20-22 February, Phoenix Park, Korea, pp. 1043-1048, 2006.
[13] Piotrowski, K., Langendoerfer, P., and Peter, S., "How Public Key Cryptography Influences Wireless Sensor Node Lifetime," Proceedings of ACM SASN 2006, Virginia, USA, pp. 169-176, 2006.
[14] Woo Kwon Koo, Hwaseong Lee, Yong Ho kim, Dong Hoon Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks", International Conference on Information Security and Assurance,2008.
[15] Sen, J. (2013). "An efficient, secure and user privacy-preserving search protocol for peer-to-peer networks", Book Chapter in: Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence, Bessis, N. et al. (eds.), pp. 279-320, Springer, Heidelberg, Germany, January 2013.