International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 14 (2017) pp. 4184-4190

An Efficient Certificateless Authentication Encryption for WSN Based on Clustering Algorithm

Shailendra Singh Gaur
Department of I.T.
BPIT, GGSIP-University
Delhi, India.

Orcid Id: 0000000202840447

Dr. A.K. Mohapatra
Department of I.T.
IGDTUW
Delhi, India.

Rashmi Roges
Department of E.C.E.
BPIT, GGSIP-University
Delhi, India.

Id: 0000000296257315

Abstract

Authentication of Sensor nodes is a major security issues in WSN. Lack of authentication yields security attacks like man in middle attack, wormhole attack etc. One of the way of achieving authentication is the use of Digital Signature. Certificateless Signature scheme is an important key parameter for improving the performance of WSN. However, the energy constraints in WSN demands Certificateless Authentication schemes. The proposed scheme is more efficient by eliminating the need of certificate authority centers. The simulation result of proposed algorithm and technique can approximately achieve 6-15% reduction of energy dissipation and provide secured transmission using certificateless algorithm.

Keywords: WSN; Clustering; Leach protocol; Cryptography; Certificateless encryption; CLAE; Matlab Simulation.

INTRODUCTION

Wireless Sensor Network are used in many application and provides a contribution in the field of ubiquitous computing like mobile communication and portable navigation devices. Security is important to make the network secured and authenticated. Number of sensor nodes in WSN are deployed very close to each other. The central nodes communicates with a base station that received the aggregated data from the sensor nodes and communicates with the user [1].

Wireless identification and tracking of items are enabled by Radio Frequency Identifiers (RFID) systems using transponders consisting of Wireless RF transceiver and Unique Identifier installed on items. These devices are enabled by ultra-low-power technology like Wireless Sensor Network and Radio Frequency Identifier required to make the data secured using ECC and Threshold Cryptographic techniques. WSN belongs to low power consuming devices with tiny sensor nodes that make the ubiquitous computing[2].

Low Power Adaptive Clustering Hierarchy (LEACH)[3] is an algorithm designed and used in Wireless Sensor Network to manage the cluster head node in the process of data communication between the base station. There are important data and sensitive information that must be protected in WSN. Therefore, the proposed algorithm provides an important factor in terms of privacy and authentication. Certificateless Authentication Encryption reduces the additional packages of checking digital signatures and eliminates fishing attacks and spanner.

In the clustering process, the WSN nodes are divided into groups where each group has Cluster Head or Central Node that aggregate all the data linked to sensor nodes and lastly provided to Base Station [4]. Each node sense and process the data and finally the collectively data send to Base Station. Hence, using this technique the power consumption is reduced in Wireless Sensor Network. The four stages of clustering are: Selection of first node, Cluster formation, radio establishment and finally scheduling mechanism. Smart devices are used for accessing emails and important transactions like online banking and payments. Security is very important for Internet banking used in mobile and other devices to stop the malware. Security of devices is a major challenge for seamless interconnectivity to provide various services to users. This paper discussed the various security concerns and their challenges to provide security to devices. Therefore, the security of devices is discussed and analyzed.

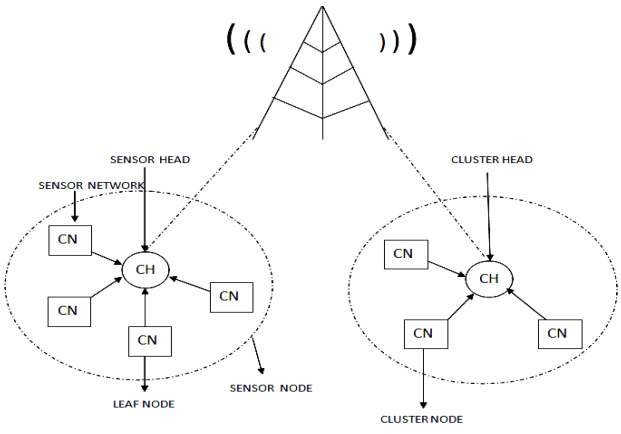

Figure 1: Clustered WSN using LEACH protocol

CERTIFICATE AND CERTIFICATELESS CRYPTOGRAPHIC ALGORITHM:

Certificateless cryptography was first introduced by AI-Riyami and Paterson in 2003[14]. This signature scheme does not require a necessary certificate to bind the signer identity and the public key. Using third party, we can easily manage the generation and distribution of user's private key. In this paper we are proposing a certificateless scheme based on ID based and PKC. Using Certificate Encryption for security, such as Advanced Encryption Standard, we uses a long string of characters like 32 characters or 256 bits in secret key to encrypt the sensitive data and we can easily guess all 256 bits to find an AES 256 secret key. To protect the secret key, asymmetric encryption algorithm knows as Certificate less Authentication Encryption (CLAE) is proposed[5]. The person who has the private key can retrieve the secret key protected by an algorithm. CLAE is the solution to securely share secrets in widely decentralized system for ubiquitous computing like mobiles and tablets.

A. Cryptographic and clustering techniques:

1) Elliptic Curve Cryptography:

ECC was first proposed by Neal Koblitz and Victor Miller in 1985. Elliptic Curve Cryptography is a technique based on finite fields. Elliptic Curve performs operation on any two points on a curve and gets a result after adding it. It is used to make the integrated and authenticated data. ECC was used for devices where power consumption is very less. The affine coordinate and the projective coordinate are the two coordinates used for the ECC over GF (2n)[6]. The scalar multiplication, the addition of point, and the finite field are the three levels provided by ECC.

The equation of ECC is defined by:

$$y2 + mxy + ny = x3 + ox2 + px + q \qquad (1)$$

Here the values of m, n, o, p and q are represented as real numbers. Using small bit key size in ECC has many advantages like smaller RAM and ROM with proper storage of data.

2) Threshold Cryptography:

This technique based on sharing of a key among number of users involved in encryption and decryption depends not only on one node for transmitting of message. Threshold cryptography share the key in such a way that each individual point performs a calculation without knowing its partial message or key.

This technique provides confidentiality, integrity and verification of data against malicious nodes without sharing its secret key[7]. It is based on distributed architecture where nodes are required for encryption and decryption of a message. The threshold schemes involves key generation, encryption and decryption, share generation, verification and combining of algorithm.

3) LEACH Algorithm:

LEACH algorithm as a basic clustering algorithm is mostly used in WSNs. In this algorithm, cluster head is selected and the process is based on random selection. LEACH protocol has many advantages like energy efficiency and data aggregation etc. This protocol will randomly select the cluster head nodes and thus provide the most optimal cluster number. Due to less number of clusters, the network will not follow the concept of layer but this protocol does not provide any guarantee for the formation of cluster heads [8].

LEACH is based on distributed cluster based protocol. High Energy Cluster Head position is selected from randomized rotation from cluster nodes and the energy is distributed among the sensor nodes of network. The LEACH protocol is operated by two phases i.e. the setup and steady phase.

1) Setup Phase: Cluster Head (CHs) is selected among Cluster Nodes. Each Sensor Nodes selects two numbers 0 and 1 randomly. Cluster head is selected when the number 0 and 1 is less than threshold value. Each node decides to join which cluster node according to signal strength.

2) Steady phase: In this phase, all the aggregated data received from sensor nodes is transmitted from cluster head to Base Station or sink.

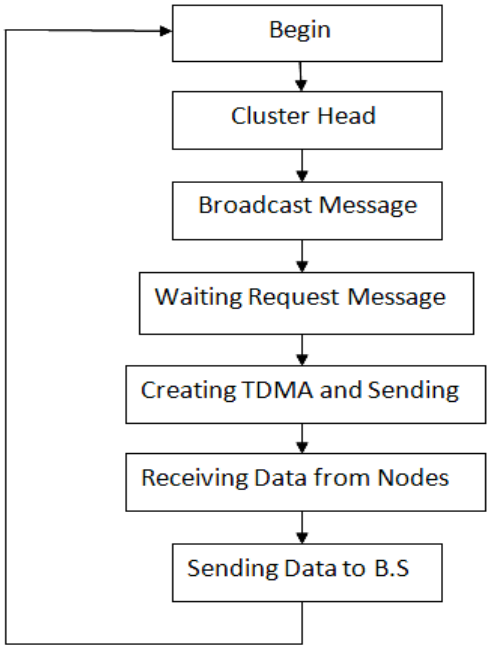

Figure 2: LEACH Protocol in WSN

RELATED WORK

A) Wireless Sensor Network and Clustering:

Transmission of secured data in WSN is a critical issue because this wireless sensor network consist of various sensor nodes as distributed devices.

Therefore, clustering techniques is used to improve the performance of WSN. Hence, LEACH is one of the clustering technique to achieve this goal.

In this paper, we are proposing a certificate-less encryption technique and energy efficient LEACH algorithm to provide security to the network. This algorithm for improved and secured network not only gives the secured transmission but also the utilization of energy is reduced in Wireless Sensor Networks.

B) Clustering in WSN:

The computation and sensing is the major issues of the Wireless Sensor Network in wireless communication. WSN comprises of large number of sensor nodes which can detect and process the data in a periodic manner. The performance of wireless sensor network relies on power, energy consumption and the sensor nodes life.

The purpose of our work is the optimization of energy consumption in WSN using proposed certificateless security techniques along with clustering techniques of WSN.[9]

In WSN we need to consider the distance of sensor node from cluster head and base station. The data is transmitted from source node to destination node through central gateway known as sink or base station. Transmission based on clustering in WSN (CWSN) is used to reduce the consumption of bandwidth and increases the scalability of the sensor nodes.

C) Algorithm based on certificateless encryption:

Certificatless Authentication Encryption (CLAE):

CLAE is mainly comprises of Public Key Cryptography (PKC) and Identity Based Encryption (IBE) for secured sharing of secret keys. PKC is used to cipher the secret key and sharing over an insecure channel. The third party known as certificate or centre authority generates the keys within a PKC. Identity based encryption (IBE) is used to provide authentication and flexible delivery of secret key. Here, the public key is generated by itself using any identity like email_id, mobile number and device number etc. CLAE is used in many applications like email services, banking sector, secured sharing of files etc. It shares the secured secret keys in decentralized systems for mobile communication, tablets etc.

D) Public Key Cryptography:

The information of Public Key can be used by anyone who wishes to cipher the secret key and share it over an insure channel. Two Sets, Public Key and Private Key are used in PKC. Both cipher and secret key is protected by Public Key before it is transmitting over an internet. [10]

Private Key is used by the recipient to decipher the ciphering mechanism and retrieve the secret key. Only the recipient who is aware of the private key can retrieve the secret key and access the confidential data.

E) Identity Based Encryption:

In Identity based encryption, we verify the identity of the recipients and issues the corresponding public key certificates. The sender can locally generate the public key certificates using a known Identity of the intended recipients such as email address. The self-generated public key is then used to cipher the secret key and protect it for distribution over the Internet. Suppose, if a public key is generated for xxx@company.com, the owner of the email address has to verify itself to the trusted authority, such as www.security.com, before the sender can receive a private key that allows it to decipher the ciphered secret key and access the confidential data.

Public parameter is verified by the sender in CLAE method before encrypted message is allowed to transmit. This technique allows the sender to verify the trusted center before the encrypted message is to be transmitted. CLAE can use the trusted center and the identity of the recipient.

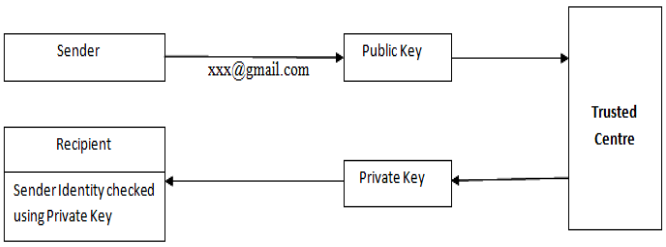

Figure 3: CLAE based encryption and decryption.

For example, the sender can use xxx@gmail.com to generate the public key and force the user to verify itself to www.yyydomain.com to receive the private key corresponding to the xxx@gmail.com identity. Authentication of the sender is initiated into the deciphering process, that is the sender identity can be checked locally using the private key received from the trusted authority. This will ensures that the sender is indeed a legitimate user, whose identity has been verified with the trusted center.

PROPOSED ALGORITHM

In CLAE architecture, the identity of the user is protected by the private key and the hackers cannot break the confidential message being transmitted using Key Generation Centre.

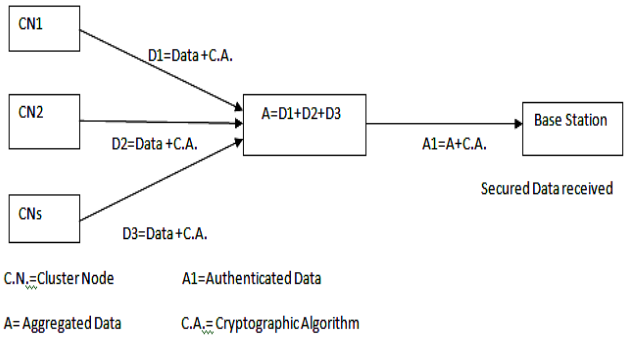

Figure 4: Certificateless security in clustering

[17][18] Certificate-Less Authentication Encryption is a ID based authentication encryption where public key is generated by identity strings and sender has to choose the trusted center to which the recipients has to identify itself.[11]. This technique allows the sender to verify the public parameter before the message to be encrypted and also ensured that the message has not been tempered.

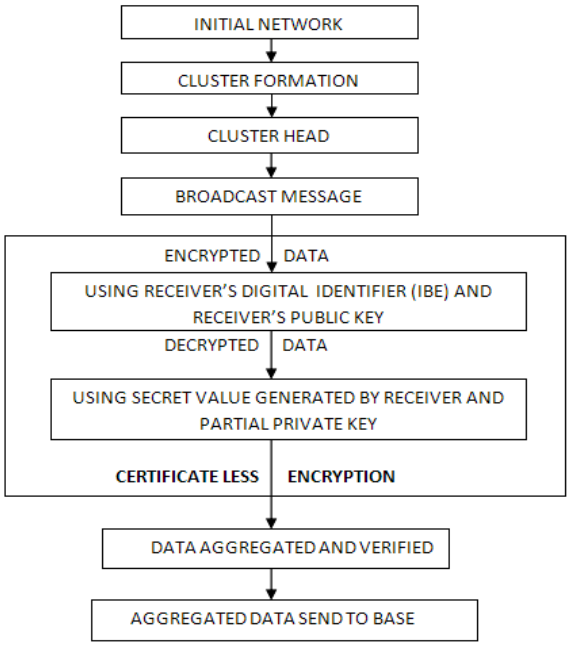

Figure 5: Proposed algorithm of certificateless security in WSN

SIMULATION RESULTS AND ANALYSIS

In this scheme, we consider the different parameters and its comparison in the first cluster head dead and the number of rounds used. On the basis of nodes being deployed, we assumed some parameters related to node features.

Table I. Simulation environment parameters for LEACH implementation.

Different parameters of Leach Implementation				
S_ No	**Field Dimensions**	**Number Of Nodes**	**Energy Model**	**Number of Rounds**
1	**Xm=50, Ym=50**	**N=50**	**Eelec=50pj/bit Efs=10pj/bit Emp=.0010pj/bit Eda=5pj/bit**	**9000**
2		**N=75**		
3		**N=100**		
4		**N=120**		
5		**N=150**		

A total of 50 to 150 nodes were deployed within a 50m × 50m space region measured in meters. We obsorved that when N=50, the first node dead at 950 number of rounds.

Table II. Implementation of LEACH in Matlab

S-No	Number of Nodes	Total Cluster Head	First Node Dead	All Nodes Dead	First Cluster Head Dead	All Cluster Head Dead
1	**50**	**5**	**950**	**1600**	**2750**	**5700**
2	**75**	**7**	**920**	**1780**	**1980**	**4400**
3	**100**	**9**	**1000**	**1680**	**1990**	**6800**
4	**125**	**13**	**935**	**1600**	**1620**	**3880**
5	**150**	**15**	**989**	**1700**	**1750**	**4580**

Case 1: When N=50 and Cluster Head is 5.

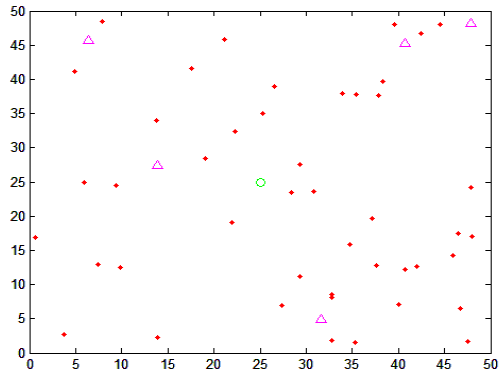

Figure 6: The first Cluster Head dead at 2750.

Case 2: When N=75 and Cluster Head is 7.

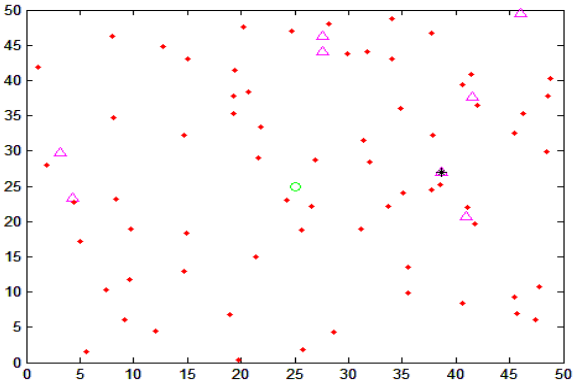

Figure 7: The first Cluster Head dead at 2980

Case 3: When N=100 and Cluster Head is 9.

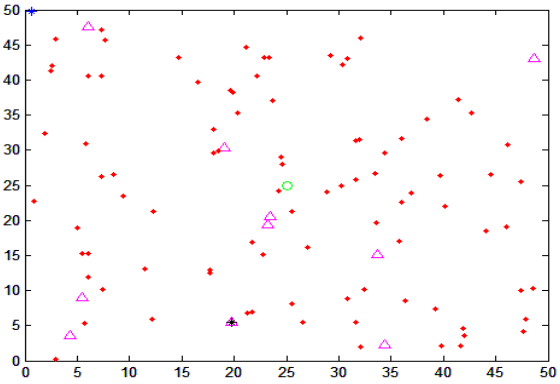

Figure 8: The first Cluster Head dead at 2990

Case 8: When N=125 and Cluster Head is 13.

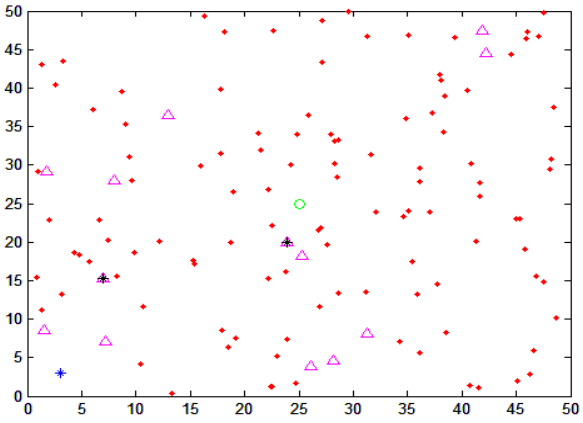

Figure 9: The first Cluster Head dead at 1620

Case 5: When N=150 and Cluster Head is 15

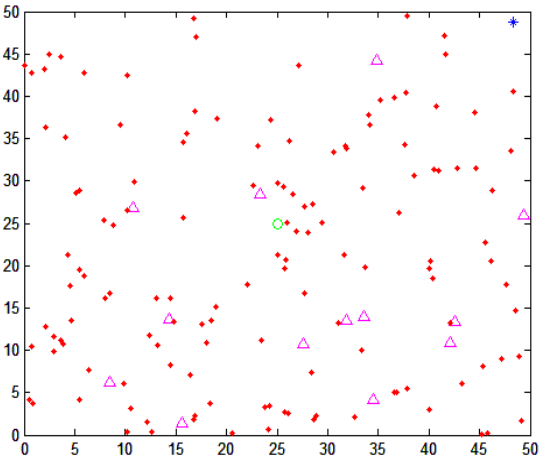

Figure 10: The first Cluster Head dead at 1750

Figure 6 to 10 represents the results from simulation that has been carried out between number of nodes and first cluster head dead at 2750 number of rounds. The simulation parameters are listed in Table 2 and Table 3.

Table III. Data delivered and received using certificate less algorithm

Number of Cluster Head	Data Delivered (Data Signal)	Energy Dissipation	Certificateless Algorithm Public Key	Certificateless Algorithm Private Key	Data Received (Data Signal)
3	61223	Full Energy	5	8	61223
5	71233	Slightly Less	6	1	71233
9	190,22522	Loss of Energy	4	3	190,22522

Trusted Centre

SECURITY DISCUSSION

Using proposed algorithm, we do not require a Digital Signature for the identification of false public key for an identity of a user. Secondly, without knowing the private key of the concerned identity the attackers cannot break the transmitted message. There is no need of digital signature to verify the public key required for security. Lastly, the proposed algorithm is more secured against malicious attacks created by key generation authority. [12]

In our proposed scheme, we are considering the certificate less encryption scheme and avoid the certificate based algorithm.[16]

The consumption of node energy has been reduced in the proposed scheme by using the certificate less encryption algorithm. The results show that the increase of number of nodes from 50 to 150 and cluster heads in LEACH protocol, the first cluster head dead was found to be 2750 to 1750 rounds.

Thus, the proposed algorithm is better than existing algorithms in terms of power consumption and efficiency of WSN. The proposed encryption scheme achieves lower reduction of energy, higher performance of WSN and secured transmission of data.

CONCLUSION

Using Certificateless encryption technique in WSN, there is no need to protect both the Public Parameters and Private Key generated. Secondly, there is no need for checking or storing certificates by recipients.

The proposed algorithm reduces the administrative work to issuing and revoking public key/private key pairs per request. The proposed algorithm aim at reducing the energy consumption of cluster head. As future work we will compare our algorithm with some other certificate less encryption techniques.

REFERENCES

[1] B. Karthikeyan, M. Veluman, R. Kumar and Srinivasa Rao Inabathini, "Analysis of Data Aggregation in Wireless Sensor Network", IEEE: School of Electronics Engineering, VIT University, Vellore, India, 2015.

[2] Z. Sheng, C.Mahapatra, C. Zhu and V.C.M. Leung, " Recent advances in industrial wireless sensor networks toward efficient management in IoT". IEEE Access, vol. 3,pp. 622-637, May 2015.

[3] Chunyao FU, Zhifang JIANG, Wei WEI and Ang WEI, "An Energy Balanced Algorithm of LEACH Protocol in WSN", International Journal of Computer Science Issues, pp. 354-359, 2013.

[4] B.Brahma Reddy and K.Kishan Rao, "A Modified clustering for LEACH algorithm in WSN", IJACSA, VBIT, India and Vaagdevi College of Engineering, Warangal, India, Vol. 4, No.5, 2013.

[5] P. Gong and P. Li, "Further improvement of a certificate less signature scheme without pairing", International Journal of Communication Systems, vol. 27, pp. 2083-2091, Oct. 2014.

[6] D. He, J. Chen and R. Zhang, "An efficient and provably-secure certificate less signature scheme without bilinear pairings, "International Journal of Communication Systems, vol. 25, pp. 1432-1442, 2012.

[7] Muhammad Hammad Ahmed, Syed Wasi Alam, Nauman Qureshi and Irum Baig," Security for WSN based on Elliptic Curve Cryptography", IEEE, 75-79, 2011.

[8] Haimabati Dey and Raja Datta, "Monitoring Threshold Cryptography based Wireless Sensor Networks with Projective Plane", IEEE: Indian Institute of Technology, Kharagpur, India, 2012.

[9] Qian Liao and Hao Zhu, "An Energy Balanced Clustering Algorithm Based on LEACH Protocol" Proceeding of the 2nd International Conference on System Engineering and Modeling -13, pp. 0072-0077, 2013.

[10] Abdullahi Arabo and Bernardi Pranggono,"Mobile Malware and Smart Device Security: Trends, Challenges and Solutions", IEEE: The Oxford Internet Institute (OII), U.K., 2013.

[11] C. Wang, D. Long and Y. Tang, "An efficient certificateless signature from pairings, International Journal of network Security, vol. 8, no. 1, pp. 96-100, 2009.

[12] M. H. Au, J. Chen, J.K. Liu, Y. Mu, D.S. Wong and G. Yang. "Malicious KGC attack in certificate less cryptography". In Proc. ACM Symposium on Information, Computer and Communications Security. ACM Press, 2007.

[13] Huaiqing Lin and Qian Zhang, "CL-PKC-Based Secure Multicast Communication for P2P Network", 2010 Second International Conference on Network Security, Wireless Communications and Trusted Computing, IEEE, 154-157, 2010.

[14] R.A. Roseline and Dr. P. Sumanthi, "Energy Efficient Routing Protocol and Algorithms for Wireless Sensor Networks-A Survey". Global Journal of Computer Science and Technology, vol. 11, 2011.

[15] S.A. Riyami and K. Paterson, " Certificateless public key cryptography," in Proceedings of Asiacrypt-03, pp 452-473, 2003.

[16] Huaiqing Lin, Yonghong Zhou and Qian Zhang "CL-PKC Based Secure Multicast Communication for P2P Network" Second International Conference on Network Security, Wireless Communications and Trusted Computing, IEEE-2010, pp 154-157

[17] Jitendra Singh, Vimal Kumar and Rakesh Kumar "An RSA Based Certificateless Signature Scheme for

Wireless Sensor Networks" ICGCIoT-2015, IEEE, 2015, pp- 443-447.

[18] Thomas Eisenbarth, Christof Paar, Sandeep Kumar and Leif Uhsadel "A Survey of Lightweight Cryptography Implementations", IEEE Design and Test of Computers, 2007 IEEE, pp-0-11.