Received: November 21, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Optimal Lightweight Cryptographic Approach for WSN and its Energy Consumption Analysis

Shailendra Singh Gaur[1*] **Amar Kumar Mohapatra[2]** **Brijesh Kochar[1]**

[1] *Bhagwan Parshuram Institute of Technology, India*
[2] *Indira Gandhi Delhi Technical University for Woman, India*
* Corresponding author's Email: shailendra.gaur08@gmail.com

Abstract: Wireless Sensor Network has various security issues like authentication of sensor nodes and its power consumption. Therefore, we are focusing on evaluation and optimization of power consumption in wireless sensor networks using light weight cryptographic techniques. This research paper studies the certificateless cryptographic algorithms and hence develops an optimal algorithm for the same. The proposed algorithm is more efficient and secured by eliminating the concept of digital signature to make the light weight cryptographic algorithm using PKC and IBE. The simulation result shows that the proposed algorithm can achieve approximately 5-20% reduction of energy consumption with same level of security.

Keywords: WSN, Cryptography, CLAE, Clustering, Energy consumption.

1. Introduction

Wireless networks are used in many applications and they are a faster and an inexpensive manner of data transfer and data retrieval [1]. The nodes are virtually connected amongst each other through a gateway that provides such wireless connectivity. A group of nodes in a network is known as cluster. A master of all the clusters is selected and that node is known as cluster head. Clustering is the method of grouping a set of nodes in such a manner that the nodes in the same group resemble each other rather than resembling to other nodes in other groups.

For an analyst, a crucial step is to calculate and keep a check on the optimality of every algorithm. Network security is the security provided to a network, so that is protected from unauthorized users and malicious access. Nowadays, when everything is done on a virtual and digital platform, like the internet, it is very important to provide security so as to avoid the dark sides. The most common manner of providing security is assigning a unique username and setting a strong password. A network security system depends upon tiers of protection which include a myriad of security software, in addition to hardware and other equipments. Each such layers implements different security policies and algorithms. Network security helps in protecting confidential information from illegitimate use. It targets various threats and stops them from penetrating the system.

There are many crucial information varies from normal to confidential in different agencies, organizations and institutions etc. This information is stored on a server and is retrieved through the network all over the world by different users and therefore needs security from mischievous users. Globalization of business, extended enterprise and the need for distributed Information System demands the network security. Network security is the fundamental defense to protect the collective enterprise. The activities of hackers like malicious attacks on the network are also increasing day by day.

Cryptography and security in WSN and other ad-hoc network has been increased. Network security is provided by employing the techniques like generation of keys for encryption and decryption to make the data secured and authenticated. Asymmetric key cryptography is broadly divided into RSA, Elliptic Curve Cryptography and Threshold Cryptography. These cryptographic algorithms are employed to the specific Wireless Sensor Network [2].

1.1 Cryptography

Cryptography is a technique of providing security, integrity and confidentiality to a piece of information being shared between different clients and servers. The main techniques used in cryptography are encryption, decryption and hashing [3]. Therefore, this involves key exchange problem. The sender's public key is used for encryption and the receiver's private key is used for decryption. The pioneer of the asymmetric algorithm was RSA or Rivest Shamir Aldeman algorithm. The algorithm provides a method to ensure integrity of the data. The reason that this algorithm became widely popular is that either of the public and the private keys can be used to encrypt a message and the key opposite to it can be used for decryption. It is one of the most reliable alternatives to implement asymmetric key cryptography. It generates keys with the help of elliptical curve equation, which makes the keys stronger and less vulnerable. It is widely being used for mobile applications. But, generally these techniques deal with one to one sender receiver relationship.

Although, in practical applications, information is exchanged between a number of senders and receivers, the motivation of multiple senders and receivers system was imbibed into threshold cryptography. Threshold cryptography ensures better security and availability of data in real time events [4]. With the current advancements in the system, a check on energy consumption is always a priority. For the researchers, the primary objective is to analyze energy, so that it can be judiciously utilized in the future. Because of the various diversities and dynamics, energy consumption in sensor networks has increased.

1.2 WSN-wireless sensor network

A very complex distributed system which consists of base stations and wireless sensor nodes is known as Wireless sensor network where sensor processor, memory, RF transceiver, peripherals and power supply completes each sensor node. An intelligent environment can be created by WSN by collecting real-time data [5]. WSN is fault tolerant, self-organizing sensing technique which can deploy rapidly and thus proves to be a deserving military applicant.

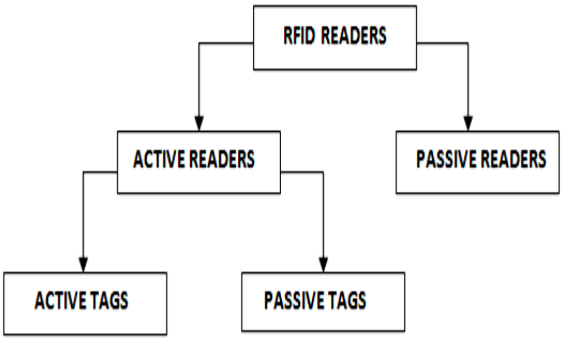

Figure. 1 RFID Architecture

Single node failure can prostrate entire system due to difficult charging and recharging process of batteries. There are three types of routing protocols under WSN, namely, data centric, location based and hierarchical protocols. Radio transmitters can only communicate with least proximate nodes due to limited range in order to conserve energy. Alterations can be done in networks by changing the membership of devices [6].

Applications of WSN: Mechanical stresses of bridges is monitored by the use of WSNs and therefore used in disaster management procedure. Secondly, gaining information about enemy movements, detecting explosions etc. can be done by the use of WSNs.

1.3 RFID-radio frequency identifiers

The process of identifying and tracking items wirelessly is done by the means of radio frequency identifiers (RFID) systems. RFID systems are small in size, cost efficient and attached with the items that need to be tracked. Due to the presence of low-power transmitters in RFID, they prove to be unreliable and the message data can be easily attacked in transit. Standard architecture of RFID readers is shown in Fig.1.

Applications of RFID: Since there exists no line-of-sight requirements, RFID systems are ideal for fast check outs and inventory controls.

1.4 Elliptic curve cryptography

In Elliptic Curve Cryptography [7], we can take any two points on a curve, add them together to achieve the third point to make the authenticated data. It was proposed by Victor Miller and Neal Koblitz. The operations performed on ECC are addition, multiplication and the use of Finite Fields.

ECC is defined by:

$$y2 + mxy + ny = x3 + ox2 + px + q \tag{1}$$

Here the real numbers are m, n, o, p and q.

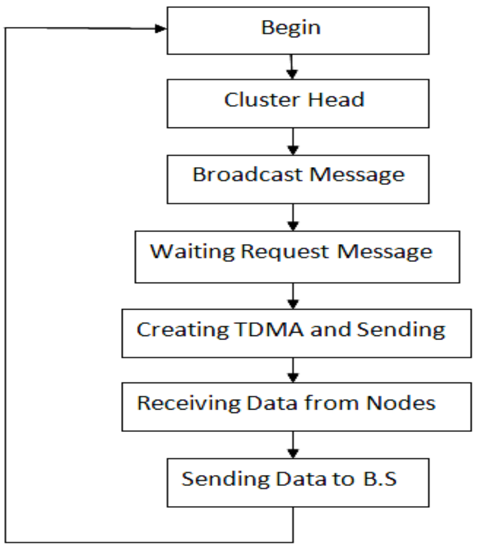

Figure. 2 LEACH protocol

1.5 Threshold cryptography

This technique does not depend on one node for transmitting of messages and the process of encryption and decryption is done by sharing of keys among number of users without knowing the partial key [8].

The threshold schemes involve key generation, encryption and decryption, share generation, verification and combining of algorithm.

1.6 LEACH algorithm

LEACH is a clustering algorithm where , cluster head is selected and the process is based on random selection of nodes. LEACH does not give any guarantee of Cluster Head formation and do not follow the layer concept.

There are two type of phases, Setup Phase and Steady Phase.

1) Setup Phase: In this phase, Cluster Head is selected. According to signal Strength, cluster head is selected among cluster node.
2) Steady phase: In this phase, data signal is transmitted from cluster head to base station after being aggregated from cluster nodes.

1.7 HEED algorithm

Hybrid Energy-Efficient Distributed (HEED) clustering is a clustering technique that selects the different cluster head on the basis of distributed energy among others sensors node. This method increases the life time of network by distributing the energy consumption of nodes. HEED is better than LEACH in terms of energy consumption of nodes and works correctly when cluster nodes are not synchronized properly. This technique also provides the confirm connectivity among sensor nodes. Hence, we can say that HEED is a novel clustering approach for Wireless Sensor Network.

1.8 Comparison of LEACH and HEED

On the basis of various parameters like number of rounds executed for nodes, the life time of sensor nodes and the consumption of energy, the comparison of LEECH and HEED is given below:

2. Related works

2.1 Types of certificate-less cryptographic algorithms

2.1.1. CLAE (Certificate-less Authenticated Encryption)

CLAE [9] is an asymmetric encryption algorithm that provides ultra security and simplicity to share the secret keys with anyone, anywhere over the internet.

In this approach, there is no need for checking or storing certificates by recipients and securely storing the secret keys used to cipher the emails. It provides end-to-end security without relying on S/MIME or TLS/SSL that leads to both authenticity and confidentiality to every message. It is useful in stopping email phishing attacks.

In CLAE architecture, it is difficult to break the important data and it is protected by Key Generation Centre and the generation of Private Key.

Certificate-Less Authentication Encryption is based on ID based authentication encryption technique where Identity String Issues the public key and the trusted centre is chosen by recipients to Identity itself.

Table 1. Comparison of clustering techniques; LEACH and HEED

S.No.	PARAMETER	LEACH	HEED
1	NO. OF ROUNDS FOR FIRST NODE DEAD	498	1459
2	NO. OF ROUNDS FOR HALF NODES ALIVE	676	2068
3	AVERAGE LIFETIME	Longer than LEACH-C	Moderate
4	PERCENTAGE ENERGY CONSERVATION EFFICIENCY	40.7	17.5

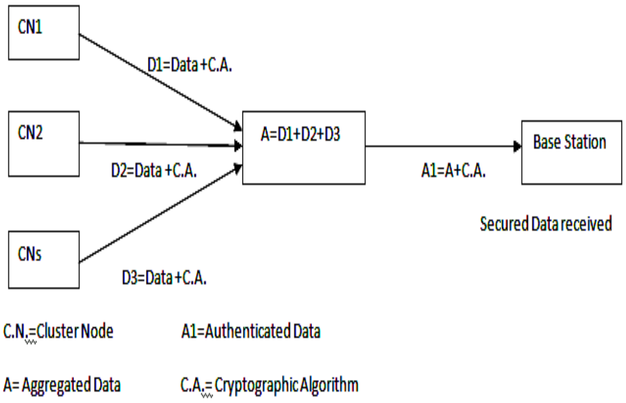

Figure. 3 Certificateless clustering

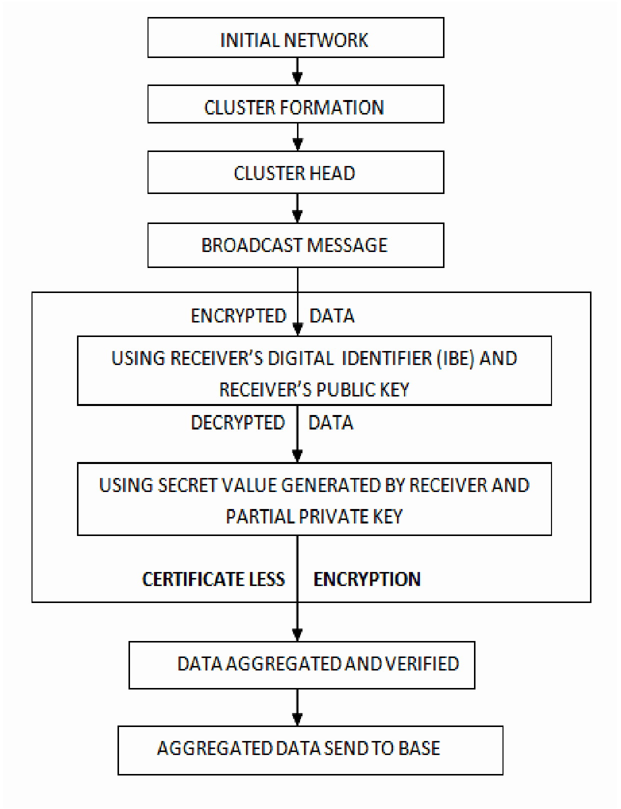
INITIAL NETWORK
CLUSTER FORMATION
CLUSTER HEAD
BROADCAST MESSAGE
ENCRYPTED DATA
USING RECEIVER'S DIGITAL IDENTIFIER (IBE) AND RECEIVER'S PUBLIC KEY
DECRYPTED DATA
USING SECRET VALUE GENERATED BY RECEIVER AND PARTIAL PRIVATE KEY
CERTIFICATE LESS ENCRYPTION
DATA AGGREGATED AND VERIFIED
AGGREGATED DATA SEND TO BASE

Figure. 4 Certificateless security in WSN

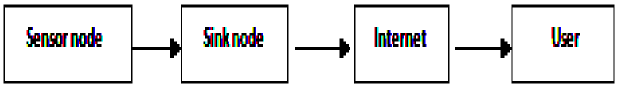

Figure. 5 Architecture of WSN.

2.1.2. ID based certificate-less scheme using bilinear pairing

In this algorithm, there is no need to carry public key of recipients just their identity and no pre-enrollment is needed. This technique proves good in mobile phone calling and prove efficient and practical for electronic voting.

2.1.3. RSA based certificate less cryptography

This type of technique facilitates with a public encryption key which actually differs from decryption key. This technique is most efficient one for encryption and the use of data space is variable. This technique is widely used in secure data transmission and hybrid encryption. Digital signatures are also efficiently implemented using RSA technique.

2.1.4. CL-PKC- based communication for P2P network

This model supplies partial keys to entities. Each user has two keys: public and private. It is also known as asymmetric cryptography. It solves the key-escrow problem and also provides explicit certification. This technique is used in most of the e-business organizations implement CL-PKC cryptography and biometric systems with identity revocation are implemented by the use of this technique.

2.2 Clustering in WSN

Wireless Sensor Network (WSN) protocols commonly use symmetric cryptographic algorithms because they consume less energy and CPU than asymmetric ones. But in case of battlefield it is crucial to secure communication despite of energy saving. So exploring the various cryptographic algorithms in order to exploit them in Wireless Sensor Network is the main objective which will provide out of box robust and secure protocols.

LEACH Algorithm: 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 [10]

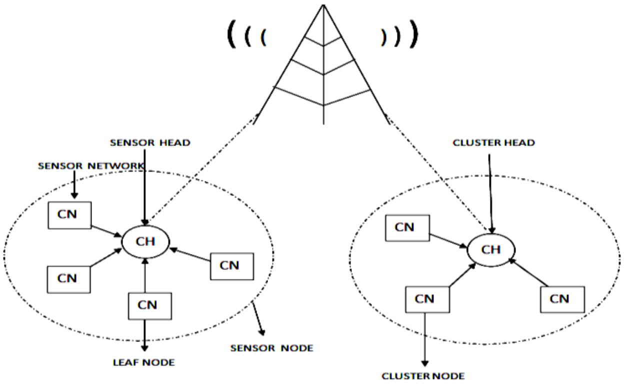

Figure. 6 Clustered WSN using LEACH protocol

Table 2. Comparison of certificate and certificateless algorithm.

PARAMETER	**CERTIFICATE CRYPTOLOGY**	**CERTIFICATE-LESS CRYPTOLOGY**
PROPOSER	Gentry	Al-Riyami and Paterson
CERTIFICATION	This system gives users both implicit and explicit certification	No certification is Required
ACCESS TO USER PRIVATE KEY	Key generation centre has the access to user's private Key	Key generating centre does not have the access to user's private key
ID BASIS	Based on identity	Not Identity-Based
KEY AUTHENTICATION	Public Keys are not authenticated	Public keys are not authenticated
KEY-ESCROW PROBLEM	Problem exists due to basis on identity	Problem is eliminated
PARTIAL KEY	No involvement of partial keys	Partial private keys are maintained

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.
2) Steady phase: In this phase, all the aggregated data received from sensor nodes is transmitted from cluster head to Base Station or sink. In WSN, we need to consider the distance of sensor node from cluster head and to base station. The data is transmitted from source node to destination node through central gateway known as sink or base station.

2.3 Comparison of certificate and certificate-less cryptographic

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 uses 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 [11].

3. Algorithm based on certificate-less encryption techniques and WSN

Certificate less Authentication Encryption (CLAE): It 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 [12].

Identity based encryption (IBE) is used to provide authentication and flexible delivery of secret key.[13] 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.

3.1 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 [14].

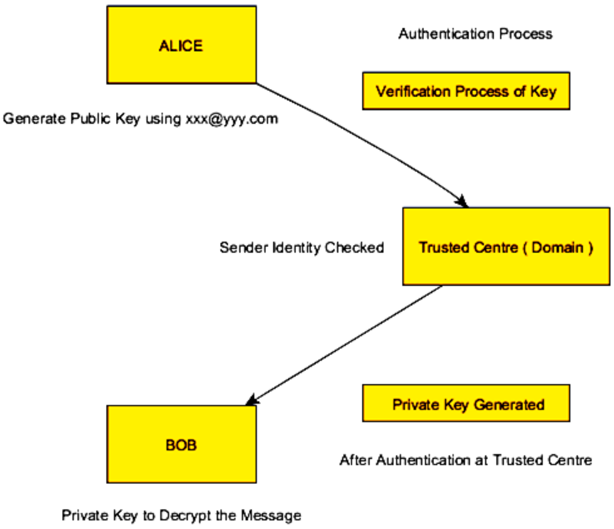
ALICE
Authentication Process
Verification Process of Key
Generate Public Key using xxx@yyy.com
Sender Identity Checked
Trusted Centre (Domain)
Private Key Generated
BOB
After Authentication at Trusted Centre
Private Key to Decrypt the Message

Figure. 7 Certificate-less encryption technique

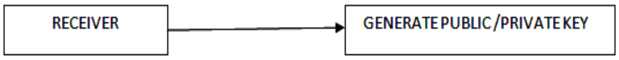

Figure. 8 Working of PKI

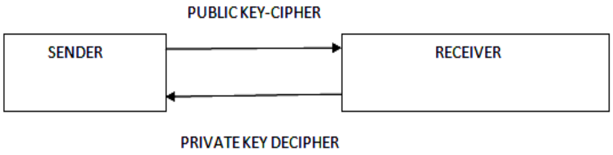

Figure. 9 PKC-retreiving secret key

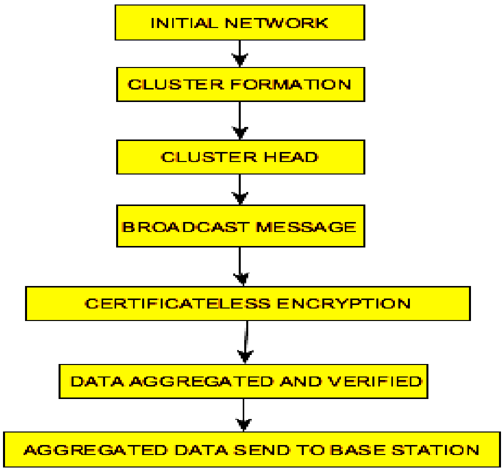
INITIAL NETWORK
CLUSTER FORMATION
CLUSTER HEAD
BROADCAST MESSAGE
CERTIFICATELESS ENCRYPTION
DATA AGGREGATED AND VERIFIED
AGGREGATED DATA SEND TO BASE STATION

Figure. 10 LEACH and CLAE

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 [15].

In Fig. 7, we are interfacing the LEACH algorithm with Public Key Cryptography and Identity based Encryption for Authentication to secure the Secret Key.

4. Energy-model for LEACH algorithm

Various parameters like modulation, rate of data transmission, distance and modulation etc. affects the power consumption in WSN. The energy consumption of WSN nodes can be reduced using different methodologies [16, 17].

Total energy consumed for transmitting and receiving the data of 1 kbit is :

For Transmitting:

$$E_{TX}(k,d) = E_{elec} \times k \times E_{amp} \times K \times d^{r} \tag{2}$$

For Receiving:

$$E_{RX}(k) = E_{elec} \times K \tag{3}$$

E_{elec} = Total Energy consumed in transmitting and receiving of data.

E_{amp} = Energy consumed during signal amplification.

The distance between the nodes is directly proportional to radio signal [18]. If the distance is sort, then r=2 and if the distance is long, then r=4.

5. Implementation

5.1 Cluster formation

Out of 50m × 50m region space, we have deployed 50 to 150 nodes in a given space measured in meters. We have been observed that, when the number of nodes N is 50, the first node dead at 950 i.e. the number of rounds.

Case 1. When the Number of Nodes is 50 and Cluster Head is 5, the first Cluster Head dead at 2750.

Case 2. When the Number of Nodes is 150 and Cluster Head is 15, the first Cluster Head dead at 1750.

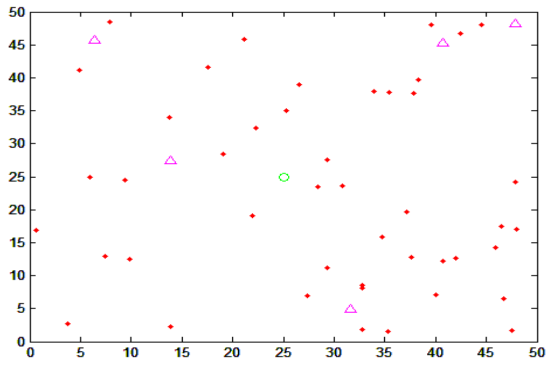

Figure. 11 Cluster formation: Number of nodes vs. Cluster Head, when N=50.

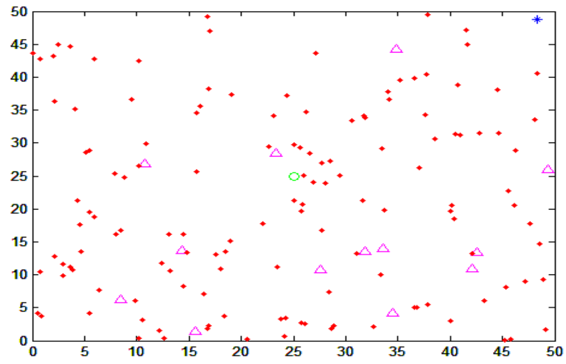

Figure. 12 Cluster formation : Number of nodes vs. Cluster Head, when N=150.

Table 3. Cluster formation in WSN

Number of Nodes	Total Cluster Head	First Node Dead	All Nodes Dead	First Cluster Head Dead	All Cluster Head Dead
50	5	950	1600	2750	5700
75	7	920	1780	1980	4400
100	9	1000	1680	1990	6800
125	13	935	1600	1620	3880
150	15	989	1700	1750	4580

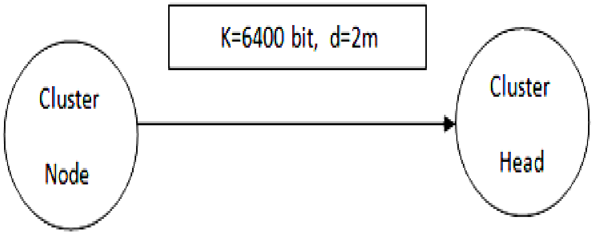

Figure. 13 Data signals transferred.

Table 4. Energy consumption of nodes

No. of Nodes	Total Cluster Head	First Node Dead (Rounds)	Energy consumed in Transmitting, ETX	Energy consumed in Receiving, ERX
50	5	950	.00032J	.00000032J
75	7	970	.00048J	.00000048J
100	9	1000	.00064J	.00000064J
125	13	1026	.00080J	.00000080J
150	15	1062	.00096J	.00000096J

The formation of cluster head and the energy consumption of dead cluster head is mentioned in the table given below [19]. Here, we are analyzing the consumption of energy during dead cluster head and all cluster head dead.

5.2 Energy consumption analysis

Parameters Used for Energy Consumption:
When the number of round is: 9000

Eelec=50pj/bit (Consumption of energy per bit)
Efs= 10pj/bit (Amplification factor)
Eamp=.0010pj/bit (Signal Amplification).

6. Analysis

It has been observed that, with the increase of sensor nodes in a cluster from 50 to 150, the intensity of dying of all cluster head will be decreases in a given number of rounds i.e. 9000. Table 2 represents the results from simulation that with the increase of number of nodes, the total cluster head will slightly increase.

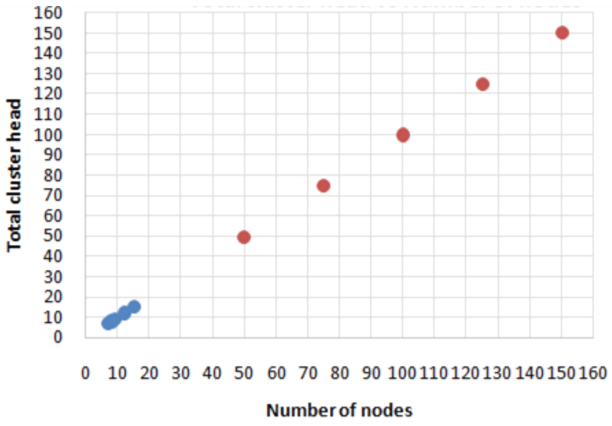

Figure. 14 Clustered WSN

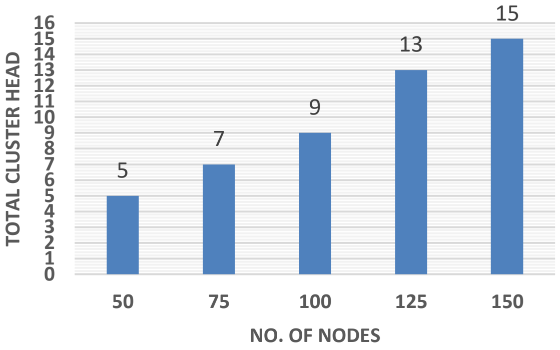

Figure. 15 Cluster head formation

It is observed that the energy used for secure sending and receiving the data signal is directly proportional to the number of nodes and the total cluster head used. For example, if we have 50 nodes and 5 Cluster head, the energy utilized for secured transmission *(Etx)* and reception *(Erx)* of data signal is 0.00032J and 0.00000032J.

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.

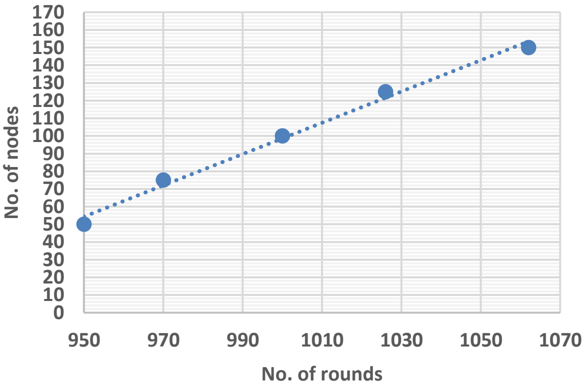

Figure. 16 Energy consumption analysis

Table 5. Number of shares and threshold

No. of Shares	Shares Generated	Index of Share
1	1027	1027
2	1064	1064
3	1121	Nil
4	1198	1198
5	1295	1295
6	1412	Nil

Table 6. Comparison of algorithm based on threshold cryptographic algorithm and the proposed algorithm

Algorithms	Share Generated	Level of Encryption	Splitting of shares
Threshold Cryptography	1027 1064 1121 1198	Single level of Encryption	Lagrange Interpolation
Proposed Algorithm			
ECC based Threshold Cryptography in WSN	20 38 64 98	Double level of Encryption	Shamir Secret Sharing algorithm
Certificateless Cryptographic algorithm	Share is not Generated. It is based on Trusted Centre	Double level of Encryption	Comprises of PKC and IBE

Figs. 14 to 16 represents the results from simulation that has been carried out between number of nodes and first cluster head dead at 9000 number of rounds. The simulation results are mentioned in Table 2 and Table 3.

6.1 Comparative analysis of proposed algorithm with existing algorithms in WSN

Input parameters:

Secret message: 1010, No. Of shares: 6 and Threshold value: 3

In Threshold cryptography algorithm, only single level of encryption is followed. In encryption method, number of shares are generated whereas Threshold(t) of shares are selected for decryption [20, 21].

In the given algorithm, the attackers cannot break the identity of the user. Secondly, this algorithm is a light weight cryptographic algorithm because we are not using digital Signature for the verification of Public key required for security. Thus, the proposed algorithm is secured and light weight cryptography than the previous algorithms mentioned in comparison of power utilization and efficiency of WSN. The proposed encryption scheme achieves lower reduction of energy, higher performance of WSN and secured transmission of data.

7. Conclusion

The proposed work aims at reducing the energy consumption of sensor nodes using certificateless encryption. Instead of using Digital Signature, we used Trusted Centre for the generation of Private Key. Secondly, it comprises of Public Key Cryptography and ID based encryption technique. In certificateless encryption technique, the protection of public/ private key and the Digital Signature for the identification of false public key for an identity of a user is not required . In this technique, we are free from storing the certificate and that was the major issue in the digital signature. Minimizing the energy consumption in WSNs and its design issues has become an important issue of research. It is concluded that the total energy consumed by sensor node for sending and receiving of data signal depends upon the total sensor nodes and cluster head used.

As future work we will compare our algorithm with some other certificate and certificateless encryption techniques along with energy consumption. The research in this field is still continuing and will lead to better results in the future.

References

[1] A. K. Sharma and Manpreet, "*Cryptographic Hash Key Algorithm to Mitigate Wormhole Attacks and Lure Catch Algorithm to Block the Attackers*", International Journal of Computer Engineering and Technology, Vol. 7, No. 3, pp. 108–117, 2016.

[2] S. S. Gaur, A.K. Mohapatra, and R. Roges, "*An Efficient Certificateless Authentication Encryption for WSN Based on Clustering Algorithm*", *International Journal of Applied Engineering Research*, Vol. 12, No. 14, pp. 4184-4190, 2017.

[3] C. Alippi, G. Anastasi, M. D. Francesco, and M. Roveri, "An adaptive sampling algorithm for effective energy management in wireless sensor networks with energy-hungry sensors", *IEEE Transactions on Instrumentation and Measurement*, Vol. 59, No. 2, pp. 335-344, 2010.

[4] H. Dey and R. Datta, "Monitoring threshold cryptography based wireless sensor networks with projective plane", In: *Proc. of the 2012 5th*

International Conference on Computers and Devices for Communication, pp. 1-4, 2012.

[5] M. H. Au, J. Chen, J. K. Liu, Y. Mu, D. S. Wong, and G. Yang, "Malicious KGC attacks in certificateless cryptography", In: *Proc. of the 2nd ACM symposium on Information, computer and communications security*, pp. 302-311, 2007.

[6] H. Patel and V. Shah, "A Review on Energy consumption and conservation techniques for Sensor nodes in WSN", In: *Proc. of the 2016 International Conference on Signal Processing, Communication, Power and Embedded System*, pp. 594-599, 2016.

[7] N. Hiremani and T.G. Basavaraju, "An Efficient Routing Protocol Adopting Enhanced Cluster Formation Technique Accompanied by Fuzzy Logic for Maximizing Lifetime of WSN", *International Journal of Intelligent Engineering and Systems*, Vol. 9, No. 4, pp 185-194, 2016.

[8] L. H. Ying, S. S. Tzuo, T. W. Guey, and B. S. P. Lin, "Toward Data Confidentiality via Integrating Hybrid Encryption Schemes and Hadoop Distributed File System," In: *Proc. 26th International Conf. on Advanced Information Networking and Applications*, pp. 740-747, 2012.

[9] Q. Phong, E. Oswald, and P. Q. Nguyen "Advances in Cryptology-EUROCRYPT 2014", In: *Proc. of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Vol. 8441, pp. 1-10, 2014.

[10] S.K Saroj, S. Kumar, S. K. Chauhan, A. K. Sharma, and S. Vats, "Threshold cryptography-based data security in cloud computing", In: *Proc. of the 2015 IEEE International Conference on Computational Intelligence & Communication Technology*, pp. 202-207, 2015.

[11] U. Somani, K. Lakhani, and M. Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", In: *Proc. of the 1st International Conf. on Parallel Distributed and Grid Computing*, pp211-216, 2010.

[12] W. Ye, J. Heidemann and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks", In: Proc. of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, pp. 1567-1576, 2002.

[13] M. N. Kumar, D. S. Rao, and D. Sravanthi, "A Novel Approach for Cheating Prevention through Visual Cryptographic Analysis", *International Journal of Computer Science and Engineering Survey*, Vol.2, No.4, pp-123-131, 2011.

[14] S. S. Gaur, A.K. Mohapatra, and S. Masood "Design of an optimized noval cryptographic algorithm and comparative analysis with the existing cryptographic algorithms", *International Journal of Control Theory and Applications*, Vol. 9, No. 34, pp 503-514, 2016.

[15] A.S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks", In: *Proc. of the Third IEEE International Conference on Pervasive Computing and Communications*, pp. 324-328, 2005.

[16] Y. Jitarwal, Yashpal, P. K. Mangal, and S. K. Suman, "Enhancement of elgamal digital signature based on RSA & symmetric key", *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, Vol. 5, No. 5, pp 693-696, 2015.

[17] R. Cramer, I. Damgård, and J. B. Nielsen, "Multiparty computation from threshold homomorphic encryption", In: *Proc. of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 280-300, 2001.

[18] A. I. Hamed and S. E. ElKhamy, "New low complexity key exchange and encryption protocols for wireless sensor networks clusters based on elliptic curve cryptography", In: *Proc. of the Radio Science Conference*, pp. 1-13, 2009.

[19] P. K. K. Vijay, M. K. Banga, U. R. Vinayakamurthi, and B. M. Thippeswamy, "Zone based Energy Efficient Mobile Data Collector in Wireless Sensor Networks", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.6, pp. 284-292, 2017.

[20] J. Singh, V. Kumar, and R. Kumar, "An RSA Based Certificateless Signature Scheme for Wireless Sensor Networks", In: *Proc. of the 2015 International Conference on Green Computing and Internet of Things*, pp- 443-447, 2015.

[21] 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, 2014.