International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Design and Implementation of Secure Communication using Elliptic Curve Cryptograph between Wireless Sensor Nodes

Gagana B E, S Usha, Rajesh K S

Abstract: ***Wireless Sensor Networks is an emerging trend and has become gradually popular across wide range. A key distributional protocol is intended to safely provide authentic motes with secret keys system using Elliptic Curve Cryptography functions. The convention is a variation of the Diffie_Hellman convention utilizing Elliptic Curve Cryptography. It's agreement of a key convention that permits pair of gatherings, both having a elliptic open and closed key, to build up a mutual secret key over an uncertain channel. This shared secret key may be either utilized as key or used to determine another key which would then be able to be utilized to subsequent correspondences utilizing a cipher of symmetric key. The use of advanced encryption standard for the encrypt and decrypt of the data also ensures that security is never flawed. Therefore Elliptic curve cryptograph is a best candidate for providing secure communication between Wireless Sensor Networks.***

Keywords **: *Advance encrypt algorithm (AES), cipher text key, Diffie_Hellman convention, elliptic curve cryptographic (ECC), Wireless or remote sensor network (WSN).***

I. INTRODUCTION

Wireless or Remote sensing system is a remote or wireless system including spatially appropriated free gadgets using sensors to gather and scatter information. With rising patterns in innovation, Wireless sensor network (WSNs) have advanced in the course of recent decades. Remote sensor systems are utilized in numerous regions, for example, training; inquire about, business, warehousing, agribusiness, human services, producing, online exchanges, ventures, military and transportation particularly for reconnaissance and observing. In this way, the significance of remote sensor arranges security is critical. In these systems, countless sensor hubs are sent to screen an immense field. The detecting innovation joined with computational power and the remote correspondence includes to its restrictive utilization in the systems administration, dispersed calculations, programming models, information the board and security, and social variables.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Gagana B E*, PG Student Dept of CSE, Rajarajeswari College of Engineering Bangalore, India. Email: gaganaeswara.18@gmail.com
S Usha, Professor and Head, Dept of CSE, Rajarajeswari College of Engineering Bangalore, India. Email: sakthivelusha@gmail.com
Rajesh K S, Associate Professor,Dept of CSE, Rajarajeswari College of Engineering Bangalore, India, Email: rajeshks_hrr@yahoo.com

Since these systems are actualized in remote regions, these systems are defenseless against numerous security dangers which may unfavorably influence the exhibition. This is a basic issue when the WSNs are used in mission basic applications. They are inclined to numerous assaults, for example, refusal of administrations, hub catching, spying and so forth. The difficulties forced on security are very surprising from the conventional system security, because of innate asset and figuring requirements. The following is the wireless or remote sensor system graph.

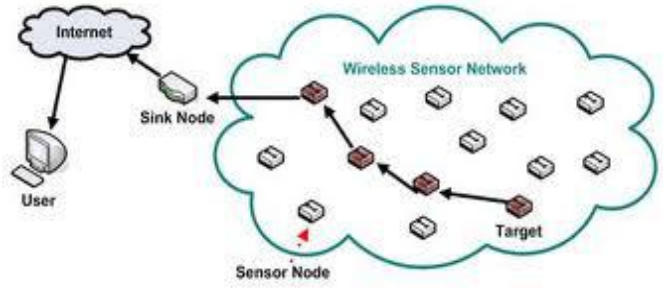

Fig. 1 Wireless sensor network

Wireless or Remote sensor systems depend on the continuous accessibility of the remote medium to interconnect taking an interest hubs. Be that as it may, the open idea of this medium leaves it defenceless against various security dangers. Anybody with a handset can listen in on remote transmissions, infuse false messages or jam real ones. Some regular difficulties towards remote security are:

- •Wireless nature of correspondence
- •Resource requirement
- •Large and thick WSN
- •Lack of physical framework
- •Unknown organize topology before arrangement
- •High danger of physical assault to unattended sensors
- •Adverse and threatening working conditions

The customary security techniques can't be utilized in view of the sensors constrained capacity limit, control utilization and computational complexities. These limitations are because of sensors restricted vitality and physical size of the sensor hub.

Elliptic Curve Cryptography (ECC) has a wonderful history being examined by mathematicians throughout the hundreds of years. Fig 2 demonstrates an elliptic bend. It has been used for caring about the fluctuated scope of issues. It is an open key cryptographic procedure. In open key cryptography, every client has two keys,

open key and private key, to set up a protected correspondence. Open key is made accessible to each one of the individuals who wish to speak with the client; the private key is kept up just by the client and is kept secret.

It has risen as an answer for remote sensor arranges as it provide same security level as of RSA, at the same time, with a littler key-estimate and lesser computational overhead. ECC's quicker estimation, most brief preparing time, lower power and memory utilization is prompting expanding interest.

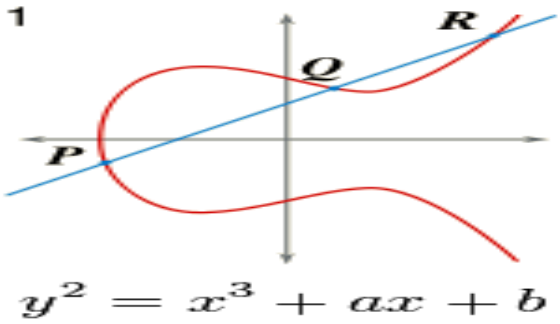

Fig. 2 Elliptic Curve

The more prevalent and generally comprised symmetric encrypt calculation is responsible to be experienced these days is the AES Advance Encrypt Standard. It is established in any event multiple times quicker than triple DES. The highlights of AES are Symmetric key and symmetric square figure, 16-bytedata, 16/24/32-byte keys, Quicker and stronger than Triple-DES, offer individual and arrangement of subtleties, Software executable in C and Java.

It depends on 'substitution_change and arrange'. It includes a development of tasks connected, some of which comprise of replacing contributions by explicit produces (substitutions) and others include reorganizing of bits around (changes). In current day of cryptanalysis, AES is extensively gotten and reinforced in both gear and program design. Also, AES is worked in versatility of length of key, which permits a dimension of 'future-fixing' against headway in the capability to achieve thorough key interests.

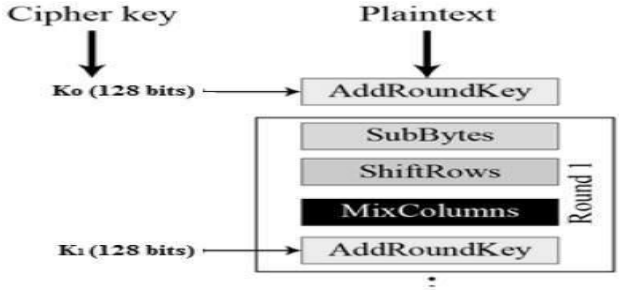

Fig. 3 Advanced Encryption Standard

The undertaking work proposes a safe correspondence calculation which uses elliptic bend cryptography for key foundation process and propelled encryption standard calculation for encryption and unscrambling of information exchanged over the wireless or remote sensor systems.

II. RELATED WORK

A. Wireless Sensor Networks

Now a day Wireless or remote sensor network are very popular as they are offering economically viable and actual monitoring resolutions. While generating the Wireless Sensor Network, the sensor nodes can be easily organized in the rigid environments and thus they are used broadly in the variety of applications such as military surveillance, environment control, harmful gas monitoring, forest detection, intelligent transportations etc. Wireless communication is best for sensor systems as they have the facilities like, it decreases the cost of arrangement, allows the sensor networks to be installed in the restricted areas also. Also Wireless or remote sensor networks comprises of distinct group of low cost, independent nodes with restricted memory and calculation power. Moreover, sensor nodes supportively monitor the area and detect major amounts of data which will be collected, grouped and then forwarded to their respective cluster head and then finally to the base stations.

B. Ellipsometric Cryptography

Ellipsometric or Elliptic curve cryptograph method has evolved as a safety resolution for wireless or remote sensor networks as it deals with same secured level to RSA with smaller size of key and very less execution power. For example, the level of security of 20-byte Ecc is equal to 128-byte Rsa. The Ellipsometric system is based on the theory of finding the random ellipsometry element's isolated logarithm along a visibly known base point. Ellipsometric cryptography, a kind of open key cryptanalysis where each client or the method takes part in the interaction has a couple of keys, an open key and a closed key, and a fixed set of activities linked with the keys to execute the cryptanalysis operations. The open key is recognized by all users in the internet but only the individual user knows the closed key. Point development is vital procedure under Ecc that is distinct over limited field procedures.

C. Advanced Encryption Standard

Advance encrypt algorithm can be uncategorized and must be "able to protect sensitive government data fine into the upcoming generation," according to the NIST announcement of the particular technique for the development of an advance encrypt standard algorithm. That was intentional to be simple to apply in software and hardware and also in limited environments (for example, in plastic money) and offer good resistance against numerous attack methods

Reasons for choosing AES algorithm includes:

- **Security:** Contending calculations must be given outcome to their ability to avoid attacks, compared with different ciphers; however safety quality was to be observed as the utmost important feature in the challenge.
- **Cost:** Planned to be satisfied under a universal, comprehensive and pre-eminence, the applicant calculations were to be evaluated on calculation and memory proficiency.
- **Implementation:** Calculation and usable qualities to be evaluated is incorporated by the adaptability of the calculation; correctness of the calculation to be executed in equipment or program design; and in general, absolute effortlessness of execution.

In [1], the Ecc application implementation is provided in multiple platforms. Ellipsometric or Ecc was discussed and used in multiple platforms based on the works reviewed; criteria of evaluation and a standard related to Ecc. The hardware engineer and software engineer working on development of Ellipsometry are provided with the relative study and survey of topic and useful reference. The conclusion is that the technologies and the performance of the technologies correspondingly employed by the hardware and the software have made more knowledge about the enhancements of both areas that are need in the today's concept for the user. With the perception of making the execution of software and the hardware cryptography designs unique a scheme called C programming platform is been proposed for this process. Then later it was tested for Ellipsometry system and evaluated under good criteria speed.

In [2], ECC is contemplated and connected on a standard WSN working framework, Tiny OS. Down to earth execution of the Ellipsometry tasks has been executed utilizing Tiny Ecc library. Minor Ecc has been utilized to create custom safety conventions on Tiny OS. The presentation standard of the proposed conventions has additionally been completed. An examination and use of Ellipsometric cryptanalysis for tending to secured and safety needs in remote detector systems have been talked about in this paper. As Elliptical Curve Cryptography devours less energy and power, it seems to be progressively reasonable for asset limitation remote sensor systems. The basic safety and security managements like validation, classification, and sharing of key can be for all intentions and purposes executed in remote sensor systems utilizing Tiny ECC.

Tiny Ecc is a very high library that is configured may also be used for the development of protocol of convention as described in this paper. An enhanced key interchange rule has been developed to overcome the drawback of Ecdh in the term of attack in-between two parties. With an involvement of Ram and Rom the designed protocol can provide protection against the attack between communications of two parties.

In [3], key distribution agreement was proposed to securely give verified bits anonymous structure keys using ecc based cryptanalysis capacity. The designed system encountered the basic necessities for a distribution plan of key that is to be viewed securely and capable in WSNs. A total security plan utilizing ECC calculations was structured in this paper. The scheme encountered the minimum necessities for a key distribution scheme to be considered as secured and efficient.

Further perceptions recommend that the framework is truly steady and could be effectively adjusted to numerous assignments by just including usefulness in the customer applications. A recommendation for upcoming work is progressively thorough testing to observe all weakness and activities that have to be the option to improve the framework. Expelling the humanoid administrator as of the procedure to do the framework increasingly adaptable will likewise be valuable.

In [4], a creating work in a propelled calculation for picture encryption is spoken to. Initial, an adaptable encoding calculations dependent on AES, RSA and elliptic-bends techniques for content scrambling is been modified. Second, the reconciliation these calculations to scramble compacted pictures is been done. At last a reasonable correlation between the three utmost renowned encoded calculations: Aes, Rsa and elliptic bends is been given.

In this paper, a product use of all the three well known encrypt calculations, Ecc, Rsa and Aes, in picture encoding is portrayed. The three popular encrypting calculations are portrayed have been assessed them as far as encoding speed, security and safety level, scrambled JPEG or PNG picture measure, age of key, throughput and time. The age of key for every encoding calculation is utilized to figure pixel of picture at a source side. As per our table outcome examination appears that Ecc calculation, encoding is the safe and secured calculation. It is seen that the quantity of the Ecc is the best contrasted with the Rsa and Aes crypt-framework calculation.

III. SYSTEM ARCHITECTURE

The framework design is a theoretical model which gives a comprehensive perspective on the framework. It gives auxiliary, conduct and a lot more perspectives on the framework. It portrays their properties and the connection between them. It includes distinguishing the parts, which include remotely obvious segments, their properties, conduct with different segments. The engineering configuration procedure is for the most part worried about foundation of structure for any framework.

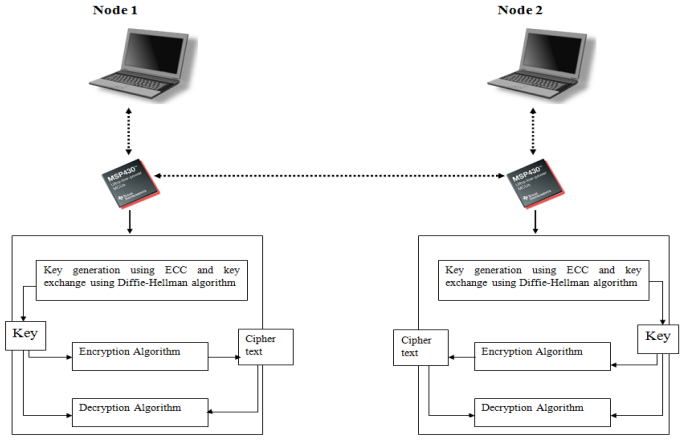

Fig. 4 System Architecture

The fig 4 demonstrates the framework engineering of the proposed work. It comprises of two remote hubs having a protected correspondence. The framework comprises of two remote sensors, one at every hub. The sensor utilized here is MSP430 sensor. The MSP430 sensor is installed with Contiki working framework, a little OS. There are three modules inside every sensor hub. When the hub requires sending information to other hub, the key is being built up utilizing the key Elliptic bend cryptography and keys are traded utilizing Diffie-Hellman calculation. The key is given to the encryption module which changes over the plain content to a figure content. This figure content can be transmitted to the proposed collector hub. At the less than desirable end, the unscrambling module takes the figure message and disentangles it with assistance of the key.

The functioning of the components is described as follows:

A. Key Generation and Exchange

This module portrays the foundation of key for secure correspondence. The system utilized here to produce key is ECC. ECC Elliptic Curve Cryptograph is a methodology to manage open key cryptography subject to the logarithmic structure of elliptic twists around restricted fields. It includes the accompanying advances:

- Define a Curve.
- Generate open private Key pair utilizing that bend, for both sender and beneficiary.
- Generate a Shared mystery key from the key pair.

Key trade is finished utilizing Diffie-Hellman calculation. Both the clients touch base at a typical point on the bend. This regular point is the mutual key utilized for the correspondence.

Fig 5 gives the functional flow of key generation and exchange.

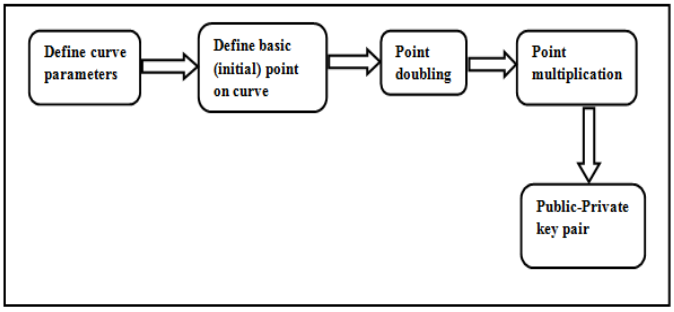

Fig. 5 Key Generation and Exchange

B. Encryption Module

The procedure utilized for encryption is Advanced Encryption Standards (AES). The square figure is of fixed size over a variable key size. The key of size 128-bits is utilized. Since 128-bits key is utilized the amount of sequences used to create figure content is 10. Each round includes of four tasks:

- Substitute bytes
- Shift columns
- Mix segment
- Add round key

The fig 6 demonstrates the control flow of encryption module.

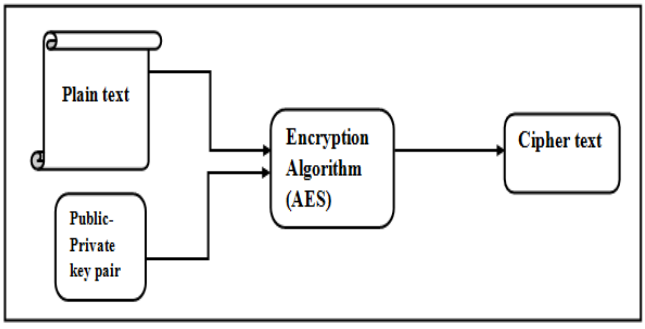

Fig. 6 Encryption Module

C. Decryption Module

This module executes the reverse process of encrypt module. It uses the similar key, which was used for encryption to decipher the data. It also has 10 rounds of procedure for the 128-bit key. Each round contains the below four operations:

- Inverse substitute bytes
- Inverse shift rows
- Inverse mix column
- Inverse round add key

The fig 7 demonstrates control flow of decryption module.

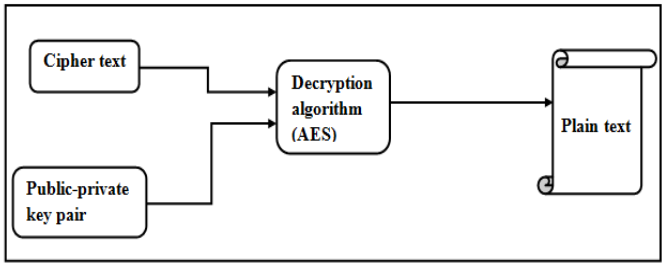

Fig. 7 Decryption Module

IV. RESULT

Fig. 8 represents the simulation control. The sensor motes are configured on the simulation screen, and the simulation is run. The user can monitor the actions using the below window.

Fig. 8 Simulation Control

The Fig 9 represents the key generation at mote1. The mote1 is named Alice, and the key generation occurs by using ECC. After computing public key both the communicating parties arrive at a common shared key used for encryption.

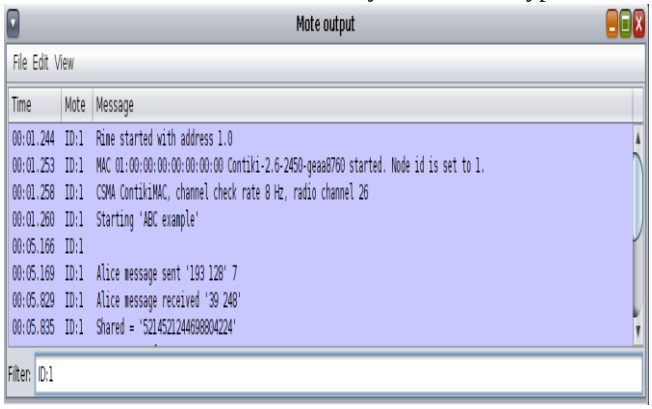

Fig. 9 Key generation at Mote 1 (Alice)

The Fig 10 represents the encryption at mote1. The text message is encoded using the shared common key. The encoded message is directed to the receiver.

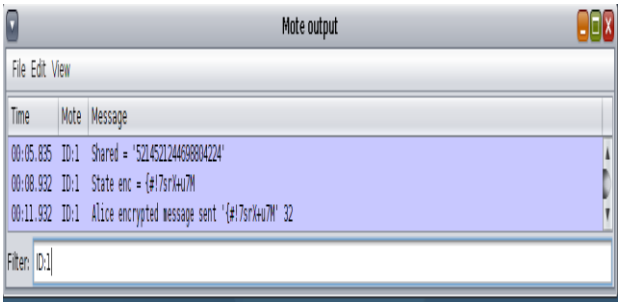

Fig. 10 Encryption at Mote1

Fig 11 represents the decryption at the receiving mote. This mote is named Bob. The encrypted message received from Alice is decrypted by using the shared common key.

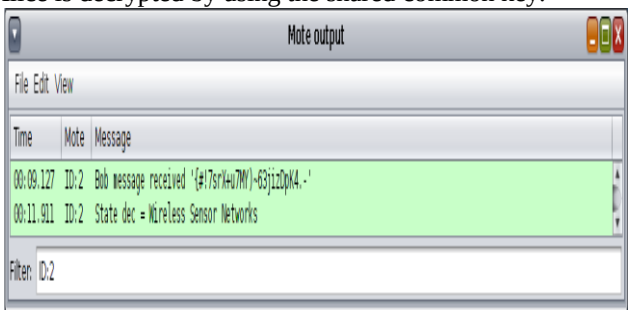

Fig. 11 Decryption at receiving mote (Bob)

Fig 12 provides the complete cryptographic scenario taking place between the communicating parties. It shows the transmission of encrypted message and then receiving it and decoding at the receiver.

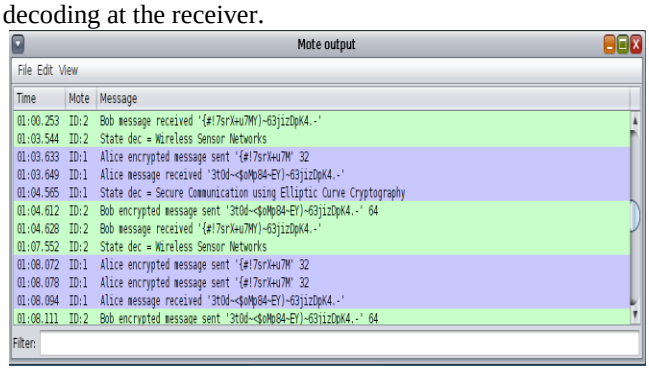

Fig 12 Cryptographic scenario at both ends

Fig 13 represents the simulation screen. It demonstrates the communication amongst the nodes of sensor. The simulation demonstrates the communications using the lines to represent the data flow.

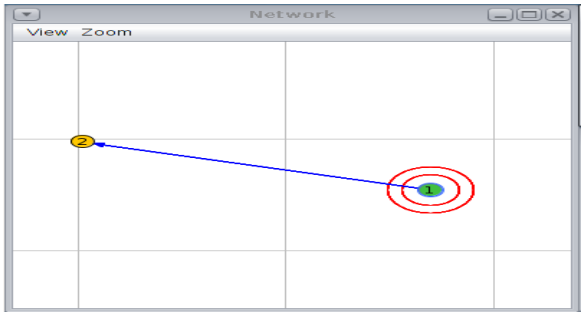

Fig. 13 Communication between the sensor nodes

V. CONCLUSION

Extended use of wireless or remote sensors has given growth to numerous security issues. Due to their resource constrains, traditional cryptographic methods have proven to be overwhelming. The key size and the computational time are the major issues of concern in wireless sensors.

To reduce the key size and optimize the complexity of calculations; we use ECC with Diffie_Hellman exchange of key algorithm. The ECDH protocol developed along with Advanced Encryption Standard provides effective security. The trapdoor function of ECC guarantees the security which cannot be easily compromised upon. The reduced key size helps to overcome the resource constrains and the overhead imposed on the functioning of wireless sensors.

VI. ENHANCEMENT

This application securely transmits text messages and other real time data such as temperature, gyroscope etc. It attempts to overcome the major limitations of wireless or remote sensor nodes. Increase in the memory size of the sensors for faster computations and increase in key size of ECC would prove to be an effective replacement in the near future.

REFERENCES

1. NejmeddineAlimi, YounesLahbib, Mohsen Machhout And RachedTourkiOn Elliptic Curve Cryptography Implementations And Evaluation 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing.
2. NajmusSaqib and UmmerIqbal Security in Wireless Sensor Networks using ECC 2016 IEEE International Conference on Advances in Computer Applications.
3. J. Louw, G. Niezen , T.D. Ramotsoela and A.M. Abu-Mahfouz A Key Distribution Scheme using Elliptic Curve Cryptography in Wireless Sensor Networks 2016 IEEE.
4. AsmaChaouch, BelgacemBouallegue and OuniBouraoui Software Application for Simulation-Based AES, RSA and Elliptic-Curve Algorithms 2nd International Conference on Advanced Technologies for Signal and Image Processing 2016.
5. Darrel Hankerson, Scott Vanstone ,AlfredMenezes, Guide To Elliptic Curve Cryptography, ©Springer-Verlag New York, Inc 2004
6. SudipMisra, Isaac Zhang and Subhas Chandra Misra Guide to wireless sensor networks, ©Springer-Verlag New York, Inc 2009
7. Joan Daemen, Vincent Rijmen, The Design Of Rijndael- Advanced Encryption Standard, ©Springer - Verlag Berlin Heidelberg 2002
8. Ian F. Blake, GadielSeroussi, and Nigel P. Elliptic Curves in Cryptography .Smart London Mathematical Society Lecture Note Series Cambridge University Press, Cambridge, 1999
9. Raghavendra CS, Krishna M, Sivalingam, TaiebZnati. Wireless Sensor Networks ©Springer US 2004
10. On Elliptic Curve Cryptography implementations and evaluation: http://ieeexplore.ieee.org/document/7523058/
11. A key distribution scheme using elliptic curve cryptography in wireless sensor http://ieeexplore.ieee.org/document/7819342/
12. EllipticCurveCryptography: https://en.wikipedia.org/wiki/Elliptic_curve_cryptography
13. Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks: https://link.springer.com/chapter/10.1007/11964254_3/
14. EllipticCurveDiffie-Hellman: https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman
15. Results of Asymmetric Performance testing (RSA) https://people.cs.uct.ac.za/~pbrittan/privacy_brittan_petzer/results_shelley.html
16. Elliptic curve cryptography http://doi.ieeecomputersociety.org/
17. Design of Secure Group Key Agreement Protocol using Elliptic Curve Cryptography: http://ieeexplore.ieee.org/document/7045305/
18. A. Kumar and G.P. Hancke, "Energy Efficient Environment Monitoring System Based on the IEEE 802.15.4 Standard for Low Cost Requirements.," IEEE Sensors Journal, vol. 14, no. 8, pp. 2557-2566
19. Gura,N., Patel,A., Wander,A.S, Eberle,H. and Chang Shantz,S. “Comparing elliptic curve cryptography and RSA on 8-bit CPUs”. Cryptographic Hardware and Embedded Systems, vol. 3156, pp. 119–132. Springer ,2004
20. Levis,P., and Gay.D, TinyOS Programming. Cambridge University Press, 2009

21. Adrian Perrig, John Stankovic, David Wagner ,"Security in wireless sensor networks" Communications of the ACM June 2004 vol 47,no. 6, pp53-57.
22. Gura,N., Patel, A., et .al 2004 " Comparing Elliptic Curve Cryptography and RSA on 8 bit CPU," Workshop on cryptographic hardware and embedded systems.
23. Gura,N., Patel,A., Wander,A.S, Eberle,H. and Chang Shantz,S.,2004 "Comparing elliptic curve cryptography and RSA on 8-bit CPUs". Cryptographic Hardware and Embedded Systems, vol. 3156, pp. 119–132. Springer.
24. D. S. Kumar, C. Suneetha, and A. Chandrasekhar, "Encryption of data using elliptic curve over finite fields," arXiv preprint arXiv:1202.1895, 2012.