Performance Analysis of Wireless Sensor Networks using Elliptical Curves Cryptography

Ms. Reena S. Satpute
M. Tech. 4th sem. (C.S.E.)
B.D.C.O.E., Sevagram
Pin Code-442001.

Prof. R. S. Mangrulkar
Associate Professor & HOD
B.D.C.O.E., Sevagram
Pin Code-442001.

Prof. A. N. Thakare
Assistant Professor
B.D.C.O.E. Sevagram
Pin Code-442001.

***Abstract*--Wireless sensor networks consist of autonomous sensor nodes attached to one or more base stations. As Wireless sensor networks continues to grow, they become vulnerable to attacks and hence the need for effective security mechanisms. Identification of suitable cryptography for wireless sensor networks is an important challenge due to limitation of energy, computation capability and storage resources of the sensor nodes. Symmetric based cryptographic schemes do not scale well when the number of sensor nodes increases. Hence public key based schemes are widely used. To keep away from various vulnerable attacks, we have introduced Elliptic Curve Cryptography, which takes less memory, reduces the computation time, provides great security and flawlessly suitable for low power devices like mobile nodes.The goal of this paper is to provide security to the wireless sensor network using elliptical curves cryptography.**

Keywords: Wireless Sensor networks, Elliptical Curves Cryptography, Wireless Sensor node

1. INTRODUCTION

Wireless sensor networks are becoming very popular now a day as they offer economically feasible and real-time monitoring solutions. While establishing the Wireless Sensor Network, the sensor nodes can be easily deployed in the unreceptive environments and thus they are broadly used in the diversity of real-time applications such as environment control, military surveillance, forest detection, harmful gas monitoring, intelligent transportations etc.[1] Also they are providing economical solutions in a host of diverse industries such as in case of electric utilities WSNs use for remote voltage monitoring, museums use WSNs for humidity monitoring and control, health care providers use WSNs for patient monitoring and notification etc. A wireless network is constituted by a number of nodes communicating wirelessly over the limited frequency and bandwidth. Sensor networks are depends on the dense deployment and co-ordination to execute their tasks. When the exact locality of a particular event is unidentified, this method of distributed sensing allows for closer placement to the happenings than would be achieved with a single sensor. A wireless sensor network consists of a discrete group of independent, low cost nodes with limited memory and computation power. More explicitly, sensor nodes cooperatively monitor the area and sense significant amounts of data which will get aggregated and then forwarded to their respective cluster head and then finally to the base stations. As wireless communication technology has advanced, the deployment of Wireless Sensor Networks has become more common [1].Wireless communication is good for sensor networks because of the reasons:

- It reduces the cost of infrastructure
- It allows the sensor networks to be deployed in the prohibited areas also
- It allows a greater range of applications than fixed location sensor networks

In order to design a completely secure wireless sensor networks, security must be integrated to every node of the system. The reason is that a component implemented without any security could be easily become a point of attack. It indicates that a security must permeate through every aspects of design of wireless sensor networks. Wireless sensor networks (WSNs) are subject to various attacks because of the vulnerable environment, limited recourse, and open communication channel [2][3]. To protect WSNs from such vulnerabilities, we have implemented the concept of elliptical curves cryptography. Wireless networking has witnessed a strong interest in the recent past due to the applications in mobile and personal communications. Wireless network architectures can be categorized into infrastructure wireless network architectures and ad hoc wireless network architectures. Sometimes wireless networks are extended from existing wired networks [1]. As per the research studies, Wireless sensor networks are becoming very popular now a day as they offer economically feasible and real-time monitoring solutions. While establishing the Wireless Sensor Network, the sensor nodes can be easily deployed in the unreceptive environments.

1.1. Framework of Wireless Sensor Networks

The ubiquitous nature of communication networks has covered the way for the development of wireless and internet applications, making communication possible all over the world. With the explosion of networks and the huge amount of data transmitted along, securing the data content is becoming more and more important [4, 5]. Wireless sensor networks are broadly used in the diversity of real-time applications such as environment control, military surveillance, forest detection, harmful gas monitoring, intelligent transportations etc.

.

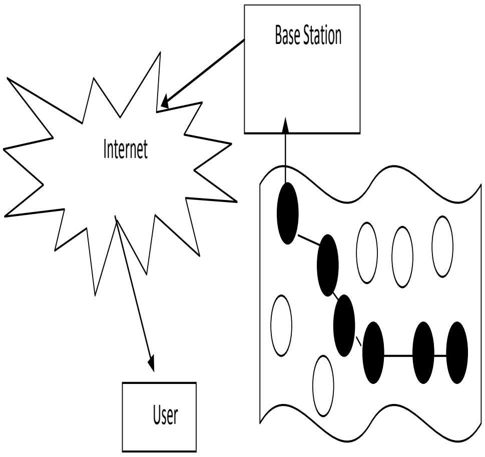

Fig. 1) Framework of Wireless Sensor Network

Above figure shows the architecture of WSN which provides economical solutions in a host of diverse industries such as in case of electric utilities WSNs use for remote voltage monitoring, museums use WSNs for humidity monitoring and control, health care providers use WSNs for patient monitoring and notification etc. Wireless communication is good for sensor networks as they offers the facilities as, it reduces the cost of infrastructure, allows the sensor networks to be deployed in the prohibited areas [6]. A wireless sensor network is deployed in the unreceptive environments and over large environmental regions. It is set up by a number of nodes cooperating wirelessly over the restricted frequency and bandwidth [7].

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed to monitor and affect the environment [1]. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security.

1.2. Security Requirements in Wireless Sensor Network

The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. The security requirements in WSN include:

1. Confidentiality: Confidentiality is hiding the information from unauthorized access. In many applications, nodes communicate highly sensitive data. A sensor network should not leak sensor reading to neighbouring networks. Simple method to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers possess, hence achieving confidentiality [2].

2. Integrity - Integrity defines the reliability of the data and refers to the capability to authenticate that a message has not been corrupted with, altered or changed while on the network[2][3].

3. Authentication - Authentication ensures the dependability of the message by recognizing its basis. By authenticating other nodes, cluster heads, and base stations before yielding some degree of resource, or revealing information [3].

4. Availability - Availability defines the services of assets offered by the network, or by a single sensor node must be available whenever it is required [2].

1.3. CRYPTOGRAPHY

Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. But as the sensor nodes are limited in their computational and memory capabilities, the well-known traditional cryptographic techniques cannot be simply transferred to WSNs without adapting them.

There are basically two types of cryptography:

1. Symmetric Cryptography

Symmetric encryption (also called as secret-key cryptography) uses a single secret key for both encryption and decryption.[8,9] This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are used to achieve the security requirements, several researchers have focused on evaluating crypto graphical algorithms in WSNs and proposing energy efficient ciphers.[10,11] Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. Examples are AES, DES etc. [11]

2. Asymmetric Cryptography

Asymmetric encryption (also called public-key cryptography) uses two related keys (public and private) for data encryption and decryption, and takes away the security risk of key sharing. The private key is never exposed [13, 14]. A message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key [15]. Likewise, a message that is encrypted by using the private key can only be decrypted by using the matching public key. Examples are RSA, ECC etc.

Public key Cryptography was omitted from the use in WSN because of its great consumption of energy and bandwidth which was very crucial in sensor network. But, now a day a sensor become powerful in terms of CPU and memory power so, recently there has been a change in the research community from symmetric key cryptography to public key cryptography. Also symmetric key does not scale well as the number of nodes grows.

1.3.1. RSA CRYPTOGRAPHY

RSA is a method to implement a public key cryptosystem whose security is based on the difficulty of factoring large prime numbers was proposed in [20]. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Through this technique it is possible to encrypt data and create digital signatures. It was so successful that today *RSA* public key algorithm is the most widely used in the world [16].

Algorithm:

Key generation:

1. Choose two distinct prime numbers, p and q.
2. Compute modulus n= pq
3. Compute phi, φ =$(p-1)(q-1)$

Where, φ is Function.

4. Select public exponent e
5. Compute private exponent

$d = e - 1 \, mod \, \varphi$

6. Public key is$\{n, e\}$, private key is d

Encryption: c = me (mod n).
Decryption: m = cd (mod n).

1.3.2. ECC CRYPTOGRAPHY

Elliptic Curve Cryptography was first projected by victor Miller and independently by Neal Koblitz in the mid-1980s and has evolved into a mature public-key cryptosystem. Compared to its traditional counterparts, ECC offers the equal level of security using much smaller keys [17, 18]. This result in faster computations and reserves in memory, power and bandwidth those are especially important in constrained environments. More significantly, the advantage of ECC over its competitor's increases, as the security needs increase in excess of time [21]. ECC operates over a group of points on an elliptic curve defined over a finite field [6].

Algorithm:

1. At first we will take a curve in the form

$y2 = x3 + ax + b$

Where, a and b are curve parameters

2. Choose a prime number.
3. Using point adding and point doubling we compute the points on the curve.
4. Select a generating point out of those points whose order should be large.
5. Take a random number less than order of generating point as a private number for each entity. This will be a secret key.
6. Generate its public key by multiplying the generating number with the secret number and will publish the point.

Encryption :

The first task in this system is to encode the plaintext message m to be sent as an x-y point Pm. It will be the point Pm that will be encrypted as a cipher text and subsequently decrypted. As with the key exchange system, an encryption and decryption system requires a point G and an elliptic group Ep (a, b) as parameters.

1. Each user A selects a private key nA and generates a public key

$PA = nAXG$

2. To encrypt and send a message Pm to B, A chooses a random positive integer x and produces the cipher text Cm consisting to the pair of points
3. Cm = { $xG, Pm + xPB$ }. (A uses B's public key PB to encrypt the message.)

Decryption

To decrypt the cipher text, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$Pm + xPB - nB(xG)$

$Pm + xBG - nB(xG)$

Pm, which is the original message or plaintext.

2. RELATED WORK

In Wireless Sensor Network, large number of nodes that are deployed densely in close proximity to the phenomenon to be monitored. Each of these nodes gathers data and its purpose is to route this information back to a sink. Cryptography is the vital encryption method used in security implementation basically for data communications. There are two types of cryptographic methods namely asymmetric and symmetric. The drawbacks are like it requires more computation power and more memory than symmetric key cryptographic approach. Since it provides the more security it is widely used such as RSA and Elliptic Curves Cryptography algorithms.

A. Liu and P. Ning described the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered [19]. Particularly, ECC is highlighted as suitable technique for WSN which provides a good trade-off between key size and security. Liu and Ning [17] also emphasize that ECC is one of the most efficient types of public key cryptography in WSNs. The steps of design, implementation and evaluation of TinyECC, a configurable and flexible library for ECC operations in WSNs, are presented [22].

Arazi, B., Elhanany, L. Arazi [20] described the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered.

Particularly, ECC is highlighted as suitable technique for WSN which provides a good trade-off between key size and security. The security issues by analysing the use of symmetric cryptography in contrast with public-key cryptography [23, 24]. The author also discussed the important role of elliptic curve cryptography in this field. An identity based key agreement protocol based on the technique of elliptic curve cryptography (ECC) between users of different networks with independent private key generations (PKGs). Elliptic curves are used to obtain more computational efficiency [25].

3. PROPOSED WORK FLOW

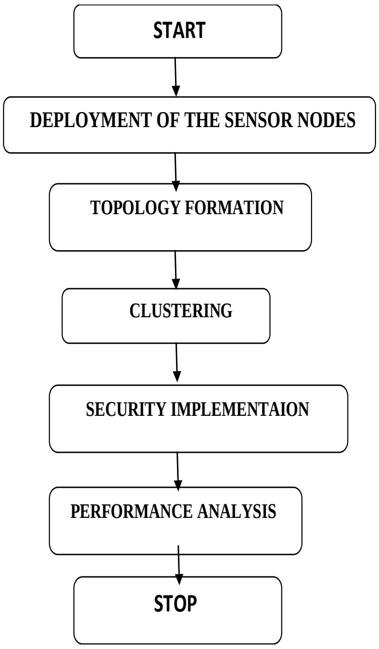

Fig. 2) Work flow

The proposed methodology has implemented to provide the security in the wireless sensor network using elliptical curves cryptography. We have implemented the project using NS2 platform. Network Simulator-2, NS2 is Network simulator is the part of software that predicts the performance of the network without a real network being there. It is a vital simulation tool for networks which contains, Lists of events and executes one event after another; Single thread of control so no blocking or race conditions, Otcl adds object orientation to TCL, Transport layer protocols like TCP and UDP as a Traffic Agent. As we know for the simulation it offers various benefits like:

- Provides a graphic interface
- Compatible with many platforms

The project has gone through the following phases:

1. Deployment of the Sensor Nodes: In this, we have created the wireless sensor nodes which are randomly generated.

2. Topology Formation: These nodes are scattered randomly and have formed the structure, we can call it as topology.

3. Clustering: After deployment of random nodes, we have created clusters of the nodes. The wireless sensor network is energy sensitive. Therefore, we adopt the maximum energy cluster head (MECH) protocol for our network architecture [1]. The MECH is an LEACH-like protocol (LEACH: low energy adaptive clustering hierarchy) [2] which divides the network into clusters. We have used the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol which will create the clusters and the node with the highest energy has been elected as a cluster head for that particular cluster. In our project we have formed four clusters. The four cluster heads (CH) are represented by the yellow colour and their respective sensor nodes are represented by four different colours. Here we have assumed:
i) All sensor nodes are dynamic.
ii) Each sensor has a unique ID assigned by the base station.
iii) Each sensor has the same capabilities in energy, computation, radio range, and so forth.
(iv) If a node is compromised, all of the key things in the node are revealed [7].
(v) Each sensor is in, and only in, one cluster.
(vi) The BS can communicate with all sensors in the network.

The clustering phenomenon plays an important role in not just organization of the network, but can dramatically affect network performance [8]. There are several key limitations in WSNs, that clustering schemes must consider.

• ***Network Lifetime:*** The energy limitation on nodes results in a limited network lifetime for nodes in a network. Proper clustering should attempt to reduce the energy usage, and hereby increase network lifetime.

• ***Energy Limitation:*** Not like wired designs, wireless sensor nodes are ”off-grid”, meaning that they have limited energy storage and the efficient use of this energy will be vital in determining the range of suitable applications for be considered as proper clustering can reduce the overall energy usage in a network.

• ***Limited Abilities:*** The small physical size and small amount of stored energy in a sensor node limits many of the abilities of nodes in terms of processing and communication abilities. A good clustering algorithm should make use of shared resources within an organizational structure, while taking into account the limitation on individual node abilities [8].

• ***Application Dependency****:* Often a given application will heavily rely on cluster organization. When designing a clustering algorithm, application robustness must be considered as a good clustering algorithm should be able to adapt to a variety of application requirements.

4. Security Implementation: For security implementation in wireless sensor network, we have used elliptical curve cryptography. After deployment and clustering of the wireless sensor network, we have implemented the security among the each node to be communicated. Each sensor node will have routing table. Each sensor node is having their id and some relevant information like their public key which has been used in the process of encrypting the data or message to be transmitted.

The private keys are randomly generated which are used to decrypt the message at the receiver side.

Consider the standard elliptic curve equation as,

$$y2 = x3 + ax + b$$

Ex:

E = $y2 = x3 + 4x + 20$, defined over F29 with the constants where,

a = 4 and *b* = 20 which have been checked to satisfy that *E* is an elliptic curve.

The 37 randomly generated points in *E* (*F*29) are as following:

{O, (0, 7), (0, 22), (1, 5), (1, 24), (2, 6), (2, 23), (3, 1), (3, 28), (4, 10), (4, 19), (5, 7), (5, 22), (6, 12), (6, 17), (8, 10), (8, 19), (10, 4), (10,25), (13, 6), (13, 23), (14, 6), (14, 23), (15, 2), (15, 27), (16, 2), (16, 27), (17, 10), (17, 19), (19, 13), (19, 16), (20, 3), (20, 26), (24, 7), (24, 22), (27, 2), (27, 27)}.

These points can be represented on the elliptical curve are as follows:

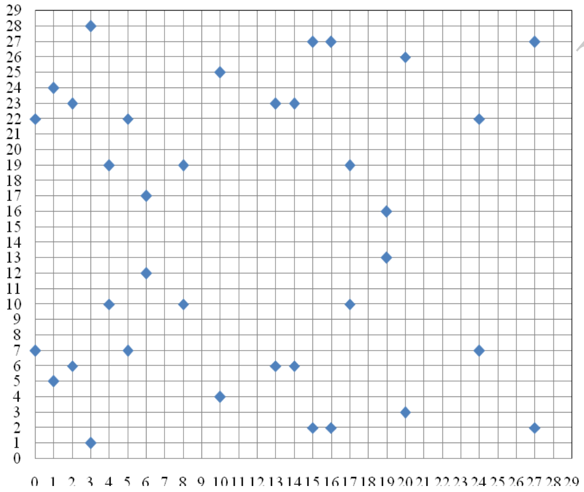

Fig. 3): Elliptic Curve Point Representation

Consider the points,

1).The point (x=1, y=5) in *E* (*F*29) satisfies the equation elliptic curve as:

*y*2 mod *p* = x3 + 4*x* + 20 mod *p*

25 mod 29 = 1 + 4 + 20 mod 29

25 = 25 this satisfies the equation of EC

2) The point (x=3, y=1) in E (F29) satisfies the equation elliptic curve as:

y2 mod p = x3 + 4x + 20 mod p

1 mod 29 = 27 + 12+ 20 mod 29

1 = 1 this satisfies the equation of EC

3) The point (x=15, y=2) in E (F29) satisfies the equation elliptic curve as:

y2 mod p = x3 + 4x + 20 mod p

4 mod 29 = 3375 + 60+ 20 mod 29

4=4, this satisfies the equation of EC

4. SIMULATION RESULT USING NS2

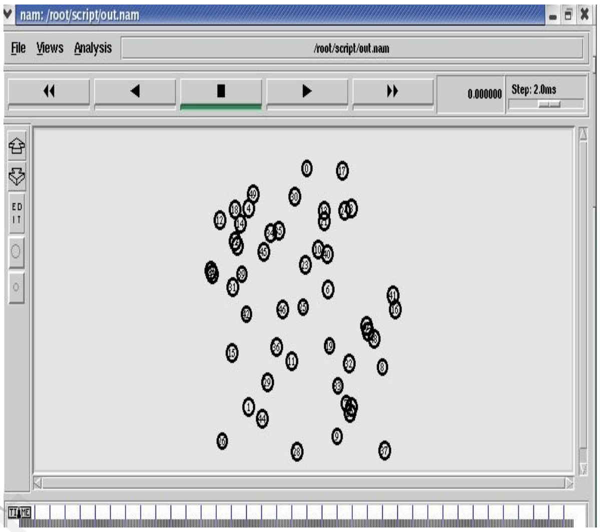

Fig. 4) : Node Creation

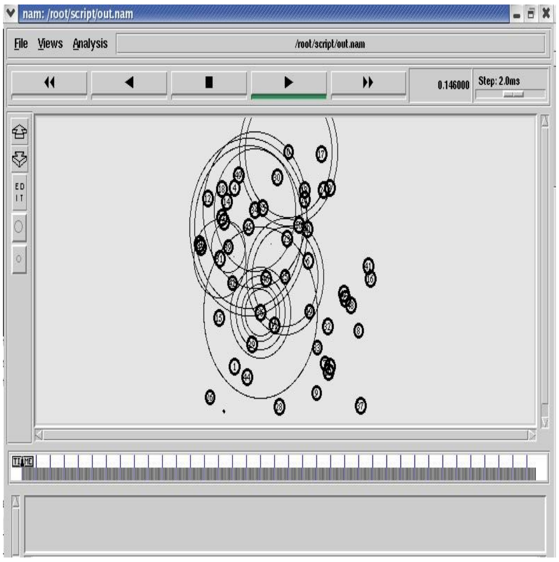

Fig. 5): Transmission range of sensor nodes

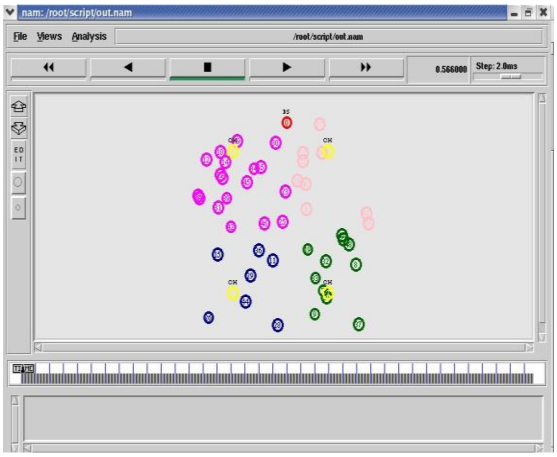

Fig. 6): Formation of Clusters along with Base Station(BS),Cluster heads(CH) &Sensor nodes(SN)

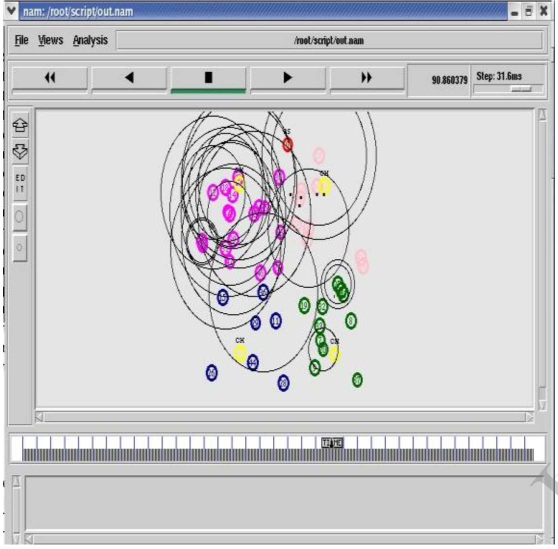

Fig. 7): Packet drops from the sensor nodes

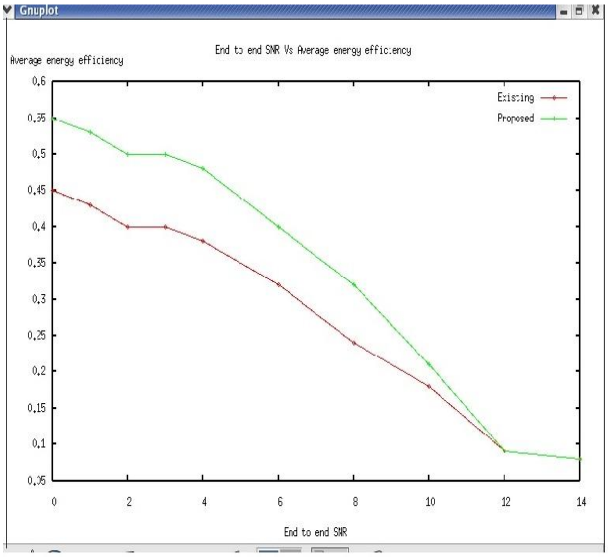

Fig. 8): S-N ratio Vs Average Energy efficiency

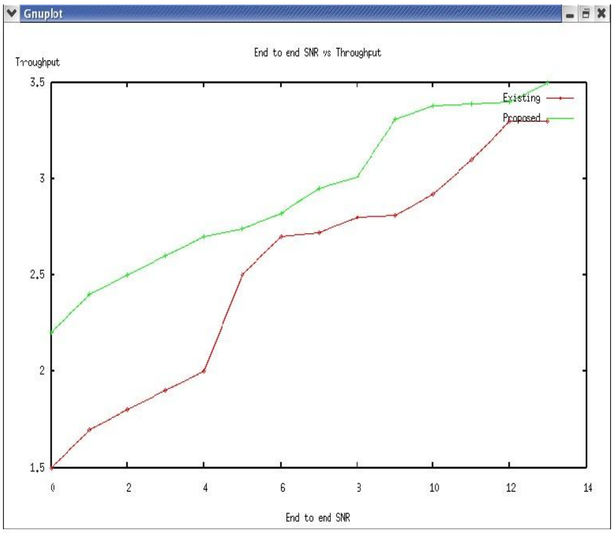

Fig.9):Graph of Signal to Noise ratio Vs throughput

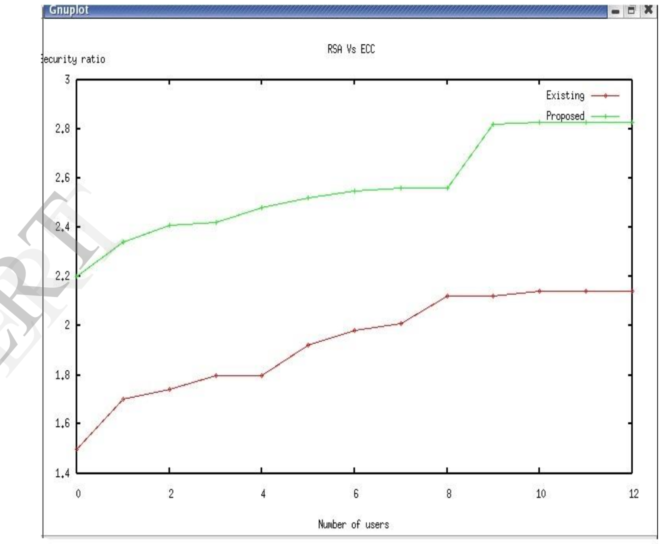

Fig. 10): Graph of Number of nodes Vs Security ratio using RSA and ECC

From the Fig. 4), we have created approximately 50 random generated wireless nodes. Fig. 5) shows, the transmission range of nodes. In Fig. 6) shows that have formed their cluster including their member nodes. Node ‘0’ at the top is acting as a base station or sink node(BS) shown by red colour and 4 cluster heads are shown by yellow colour and remaining nodes for the respective nodes are acting as a cluster members for their respective cluster heads.. All nodes in the wireless sensor networks are at last sensor nodes but depending upon their responsibilities they have been classified as base station (BS), cluster head (CH) and member nodes.

Fig. 7) shows the packet drop scenario. Fig. 8) represents the graph plotted against Signal to Noise ration Vs Average Energy efficiency considering the implemented methodology. Fig. 9) represents the graph plotted against Signal to Noise ration Vs throughput and Fig. 10) represents the graph plotted against Number of nodes Vs

Security ratio using RSA and ECC for the implemented methodology.

5. COMPARISION OF RSA AND ECC

The comparison between the ECC and RSA are represented in the following table:

Table 2. Comparison of RSA and ECC

Sr. No.	Parameters	RSA	ECC
1.	Key Size	Large	Small
2.	Security	Weak	Strong
3.	Key Generation	Fast	Slow
4.	Encryption	Fast	Slow
5.	Decryption	Slow	Fast
6.	Power Usage	High	Low
7.	Throughput	Average	High
8.	Response Time	Average	High
9.	Latency	High	Low
10.	Protocol Performance	Average	Best

6. CONCLUSION

In wireless sensor networks, the energy limitations of nodes play a crucial role in designing any protocol for implementation. The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide security, one is cryptography.

Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches. In this project, we have studied two schemes ECC and RSA. At the analysis, it is found that ECC is more advantageous compared to RSA, due to low memory usage, low CPU consumption and shorter key size compared to RSA.

Though, the operations in RSA are comparatively faster than ECC. In RSA key generation and encryption are faster whereas decryption is slower. On the other hand in ECC key generation and encryption are slower whereas the decryption is faster. From this conclusion RSA is faster but it is said that security wise ECC is stronger than RSA.

REFERENCES

[1] Wenbo Shi and Peng Gong, “A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography” in proceedings of Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, vol-730831, 1-7 , 2013.

[2] Yiying Zhang, Chunying Wu, Jiping Cao “A secret sharing based key management in hierarchical wireless sensor” proceedings in International journal of Distributed sensor network, vol. no, 406061, pp.1-7, 2013.

[3] Mohammad, Sabzinejad Farash and Mohammad Ahmadin Attari, “An ID-Based Key Agreement Protocol Based on ECC Among Users of Separate Networks” in proceedings of 9th International ISC Conference on Information Security and cryptology, p. no.31-37 , 2012

[4] Kamrul Islam, Weiming Shen, “Security and Privacy Considerations for Wireless Sensor Networks in Smart Home Environments”, in proceedings of the IEEE 16th International Conference on Computer Supported Cooperative Work in Design, vol no. 978 pp. 626-630, 2012

[5]. K. Akkaya, “, A review on routing protocols for wireless sensor networks” *in proceedings of Ad Hoc Networks*, PP. 325-349 vol. 3, 2005.

[6] Eleni Klaoudatou, Elisavet Konstantinou, “A Survey on Cluster-Based Group Key Agreement protocols for WSNs” in proceedings of IEEE Communications Surveys & Tutorials, Vol. 13, pp-33, Third Quarter 2011

[7] M. Younis, “A survey on routing protocols for wireless sensor networks*” in proceedings of IEEE Communications Magazine for wireless* Networks, 32-34. 2005

[8] .M. Healy, T. Newe,”.*Power management in operating systems for wireless sensor nodes”, in Proc. of the IEEE Sensor Applications Symposium*, pp.1-6. 2007,

[9] I. F. Akyildiz, W. Su, Y. Sankara Subramanian, and E. Cayirci. A survey on sensor networks. *In proceedings of IEEE Communications Magazine*, 40(8):102–114, August 2002.

[10]. Ning P, Wang R”, An efficient scheme for authenticating public keys in sensor networks”, *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, USA, pp. 58-67, 2005

[11]. Goodman J and Chandrakasan P ,”An Energy Efficient Reconfigurable Public Key Cryptography Processor”, *in proceedings of IEEE journal of solid state circuits*, pp. 1808-1820, November 2001.

[12]. S. Bandyopadhyay and E. J. Coyle, “An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks,” *proceedings in of IEEE INFOCOM*, vol. no. 4. Pp. 250-255, April 2003.

[13] A. Mainwaring et al., “Wireless Sensor Networks for Habitat Monitoring,” *Proceedings of the 1st ACM International Workshop on WSN*, 2002.

[14] M. Chatterjee, S. K. Das, and D. Turgut, “WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks Clustering Computing”, *proceedings in Elsevier* vol. 5, pp. 193–204, 2002.

[15] M. Ye, C. Li, G. Chen, and J. Wu, EECS: An Energy Efficient Clustering Scheme in Wireless Sensor Networks, *proceedings in National Laboratory of Novel Software Technology*,pp 350-354,vol.4 2008

[16] O. Younis and S. Fahmy, “HEED: A Hybrid Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks,” *proceedings in IEEE Transactions on Mobile Computing*, vol. 3, no. 4, Oct-Dec 2004.

[17] W. R. Heinrelman. A. Chandrakasan, “Energy-Efficient Communication protocol for Wireless Micro sensors.” *in proceedings of Elsevier journal* vol 4. pp.4 -7 January 2000.

[18]. B. Arazi, I. Elhanany, O. Arazi, and H. Qi, “Revisiting public-key cryptography for wireless sensor networks” *proceedings in wireless sensor. Technology Soc. Journal.*, vol. 4. Pp-569-572, 2009

[19]. A. Liu and P. Ning, TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks, *in Proc. of the International Conference on Information Processing in Sensor Networks* (IPSN ’08), St. Louis, MO, 2008, 245–256.

[20] Arazi,B.,Elhanany,L.,Arazi,O.,Qi,H.,:Revising public–key cryptography for wireless sensor networks *in proceedings of IEEE Computer*, PP. 103-105. Vol. 67, 2005

[21] T. Claveirole and Y. Viniotis, “Secured wireless sensor against aggregator comprimise” in proceedings of *IEEE Trans.on Sensor network*, vol. no.4, pp. 28– 38, Aug. 2009

[22] Y. Zhang, W.C. Yank, “Tree-based Dynamic key management in hierarchical WSN”, in Proceedings of the *IEEE International conference on Sensor Network Protocols, Applications*, vol. 4, page no. 52-68, 2008

[23] M. Luk, G. Mezzour, “MiniSec: A secure sensor networks communication architecture” in proceedings of the *1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2007

[24] Peng Changgen, Li Xiang, “Threshold Signcryption Scheme Based on Elliptic Curve Cryptosystem and Verifiable Secret Sharing” in proceedings of *IEEE conference on sensor networks*, page no.1136-1139, 2005

[25] S. Zhu, S. Setia, “The efficient security mechanisms for large-scale distributed sensor network” in *proceedings IEEE Trans.on Sensor network*, vol. 6, no. 4, pp. 528–538, Aug. 2005