Performance Analysis of Security in FLAT and HIERARCHICAL Routing Protocols for Distributed Sensor Networks

Suresha
REVA Institute of Technology and Management
Kattigenhalli,Yelahanka,
Bangalore 560 064, Karnataka.

Dr. Nalini .N
NITTE Meenakshi Institute of Technology
6429, Yelahanka, Bangalore 560064,
Karnataka.

ABSTRACT
Distributed Sensor Networks (DSNs) are an emerging technology, recently finding extensive application in scientific and military surveillance. DSNs operate under severe energy constraints and are largely characterized by short range a multi-hop data transmission, which drives the need for energy-efficient routing schemes in such networks. In this paper, the comparisons of FLAT and HIERARCHICAL protocols have been made with respect to Energy Dissipation for transmission of data and also with and without security features for the routing protocols. The proposed model estimates the energy required for providing security features for the routing protocols.

Keywords
Routing Protocols, Security, Directed Diffusion, LEACH, ECC, Elgamal.

1. INTRODUCTION
A Distributed Sensor network (DSN) comprises a multitude of tiny nodes, collaborating in their sensing, processing and communication process to accomplish high-level application tasks. DSNs provide persistent, unattended monitoring of natural and man-made phenomena in applications such as homeland security, law enforcement, military reconnaissance, space exploration, environmental monitoring, and early warning of natural disasters. These applications often demand continuous monitoring of physical phenomena for extended periods of time without the possibility of replenishing the energy supply at each node.Thus the effectiveness of a DSN depends on its efficiency in using the limited energy supply.
A typical sensor network (for monitoring applications) consists of hundreds of tiny, short-range, energy constrained, wireless sensors deployed densely in the target area to sense and communicate information.

1.1 Information Routing Issues in DSN
A processing node receives a bulk of data from the sensor it is associated with at regular intervals, generally at a fixed rate. After some amount of processing at the node, this information has to be sent to some or all other nodes in the network, depending on the problem solving technique. It is imperative that the information is routed to the destination nodes in an efficient manner since the data generation is repetitive. Generally, data are transmitted to the destination nodes in packets. Some of the requirements in information routing in DSN are as follows.

1) It is desirable to have the entire information generated by a sensor, in one packet.
2) In most of the DSN applications, the sensor data will be generated and transmitted in each sensing cycle. Since the data exchange is almost continuous, the routing protocols should be designed such that an explicit ACKNOWLEDGE is not used for each packet. This saves enormous traffic on the network considering the size of DSN and also Energy.
3) By not using acknowledge messages, it is necessary to see that much data is not lost and hence it is necessary to route the packets within a maximum allowable time with minimum distance.
4) DSN is envisaged to operate under hostile environments. It is therefore necessary to employ reliable point to-point routing protocols.
Therefore, sensor network lifetime is a primary concern in sensor network design. In order to enhance the network life time for a particular application, many routing protocols have been devised. Those protocols can be categorized into three classes: Flat, Hierarchical and Location based routing protocols.The flat routing protocols are simple and robust and suitable for small networks and hierarchical protocols need to selectand manage clusters, they are complex and suitable for large scale networks. In flat routing and hierarchical routing protocols, we have selected the Directed Diffusion and LEACH protocols for the Analysis.

1.2 Directed Diffusion protocol
Directed diffusion (DD), developed by Intanagonwiwat et al. [7], is a classic data-centric routing protocol. Directed diffusion consists of several elements: interests, data messages, gradients, and reinforcements. An interestmessage isa query or an interrogation which specifies what a user wants.Each interest contains a description of a sensing task that is supportedby a sensor network for acquiring data. Typically, datain sensor networks is the collected or processed information ofa physical phenomenon. Such data can be an event, which is ashort description of the sensed phenomenon. In directed diffusion,data is namedusing attribute-value pairs. A sensing task(or a subtask thereof) is disseminated throughout the sensor networkas an interestfor named data. This dissemination sets upgradients within the network designed to “draw” events (i.e. data matching the interest). Specifically, a gradientis directionstate created in each node that receives an interest. The gradientdirection is set toward the neighboring node from which the interestis received. Events start flowing toward the originators ofinterests along multiple gradient paths.An important feature of directed diffusion is that interest and data propagation and aggregation are determined by

localized interactions(message exchanges between neighbors or nodes within some vicinity).

1.3 LEACH protocol

Low-Energy Adaptive Clustering Hierarchy (LEACH) is completely distributed, clustering and the most popular hierarchical routing protocol for DistributedSensor Networks, requiring no control information from the base station. In LEACH, higher energy nodes can be used to process and send the information while lower energy nodes can be used to perform the sensing. This means that creation of Clusters and assigning special tasks to cluster-heads can greatly contribute to overall system scalability, lifetime, and energy efficiency.

1.4Cryptosystems

Cryptography is the art or science of keeping messagessecret. Cryptosystems are classified in to Symmetric and Asymmetric.

Symmetric cryptosystems use same secret keyto encrypt plaintext and decrypt cipher text. This means both sender and receiver must have same secret key for the cryptosystem. This presents two difficulties. One is how to distribute secrete keys privately. The other is how to manage large number of secrete keys. The advantage of symmetric cryptosystems is good performance for enciphering and deciphering, enabling them to encrypt large messages.

Integral to the design of an asymmetric cryptosystem isthe utilization of a one way trapdoor function. It has tobe computationally infeasible for an adversary to retrievethe private key from the published public values ofthe cryptosystem. On the other hand, for the user it has tobe computationally feasible to compute the process involvingthe function.The asymmetric cryptosystems use different keys for encryption and decryption respectively. One of the keys (the public key) isused for encryption, andits corresponding private key must beused for decryption. The critical featureof asymmetric cryptography is this key pair-public key and private key.The fact that one of the keyscannot be obtained from the other. The asymmetric cryptosystems are suitable for encrypting small messages. We have selected ElGamal and Elliptic Curve Cryptography (ECC) crypto systems for Analysis.

1.4.1ElGamal CryptoSystem

Elgamal crypto system is designed by Taher Elgamal in 1985.Difficulty of computing Security of the ElGamal crypto system depends on the(presumed) discrete logsin alarge prime modulus**.**Elgamal Cryptosystem is vulnerable to chosen ciphertext attacks**.**The security of this system depends on how big the key size is.

1.4.2 Elliptic Curve Cryptography

ECC is based on theory of elliptic curves. The principal attraction of ECC is, itoffers considerably greater security for a given key size. The smaller key size also makes possible much more compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compact software.

1.5Analysis

Energy is one of the very important resources of any DSNs, the Analysis of the energy dissipation by the routing protocols and security crypto systems gives the various domains to Improve the Performance and to increase the Life cycle of the network.

2. RELATED WORK

The important issues of information routing in DSN given in[1].

The Directed Diffusion protocol's working analogy, propagation gradients and reinforced path established are given in [2]. This information is used for Estimation of Energy Dissipated for the data transmission from a node to sink(Base Station).

One of the most preferred energy efficient routing protocols of DSN is LEACHprotocol. It is developed byW. R.Heinzelman et al[8]. This paper explains in detail about Cluster formation, Cluster Head selection for the first round and the procedure to be followed for the next rounds, and communication protocols used for data transmission such as TDMA, CSMA and CDMA.

ElGamal is an Asymmetric crypto system. The advantages of using Asymmetric crypto systems are 1) supports digital Signatures (Authentication), 2) provides Cryptographic Services such as Confidentiality and Data Integrity and 3) makes it possible to implement Key Exchange, Secrete key Derivation [9].

The key generation, encryption and Decryption algorithms information is provided in [3],[4].

ECC is most preferred Asymmetric Crypto System. It provides better Security Services for a small Key Size. For the same level of security per best currently known attacks, elliptic curve-based systems can be implemented with much smaller parameters, leading to significant performance advantages. Such performance improvements are particularly important in the wireless arena where computing power, memory, and battery life of devices are more constrained[5]. For elliptic curves, the group operation is written as addition instead of multiplication, andin that case exponentiation is more appropriatelyreferred to as scalar multiplication,For efficient implementation of ECC, it is important for the point multiplication algorithmand the underlying field arithmetic to be efficient. There are different methods forefficient implementation point multiplication and field arithmetic suited fordifferent configurations

This paper makes an analysis of the power dissipation of the Directed Diffusion (FLAT) and LEACH(HIERACHICAL) protocols and also estimates the energy required for the provision of security to these protocols by using ElGamal and ECC Crypto systems.

Remainder of the paper is structured as follows. Section 3 describes the Proposed Performance Model. Section 4 presents simulation. Section 5 presents result analysis. Finally, conclusion and Future scope is given in section 6.

3. PROPOSED PERFORMANCE MODEL

In a DSN, energy and security are two key considerations. Although security is the design goal, it is not practical to evaluate a cryptographic scheme by taking the security level as a metric. Although security schemes can be identified to have weaknesses, such flaws are not always evident or easily quantifiable [12].We like to estimate the Energy required for Routing the information for two protocols and also to determine Energy required to provide Security for these Routing protocols.

3.1 Directed Diffusion protocol Model

In Directed Diffusion protocol, the area is divided into 3 zones. Once the network is set, we check all the hundred nodes to see which of the node's sensed data falls in-between the specified

temperature range. The nodes falling in the range only will transmit the data to the base station using multi-hop strategy. If the data has to be sent by a node in the peripheral area, then it first finds the nearest node in the second zone and passes the data to it. This strategy will be used by all the intermediate nodes till the node near-by the base station is reached, this node then sends the data to the base station thus completing the data transmission [10].

3.2 Leach protocol Model

LEACH protocol uses a distributed cluster formation technique, which enables self-organization of large numbers of nodes. There are two categories of nodes: cluster-head (CH) and non-CH nodes. The nodes are organized in clusters, each having one node promoted as the CH. All non-CH nodes transmit their data to their respective CH, which further routes it to the remote sink node or BS (Base Station) [6]. LEACH uses CH rotation to evenly distribute the energy load among all nodes. The nodes forward their data to the sink through the CH. [10].

During the cluster formation, randomly a node elects itself as a cluster-head in the beginning with a certain probability. Afterwards, the principle of cluster-head selection is as follows: each node randomly generates a random number between 0 and 1, if the random number is lower than the threshold, it will be a cluster head, or it is an ordinary node. Threshold is calculated by the formula:

$$T(n) = \begin{cases} \dfrac{P}{1 - P * [r \bmod \left(\frac{1}{P}\right)]}, n \in G \\ 0, Otherwise \end{cases}$$

- T(n) is the threshold value.
- P describes desired percentage of Cluster Heads (e.g. P=0.05) or in simpler words, it is the probability of the other nodes to become cluster head in the current round.
- G is the set of nodes that have not been CHs in the last 1/P rounds.
- r is the current round number.
- n is the node number.

Once the cluster-head is selected in each cluster, the cluster-head broadcasts a message containing its ID to all the nodes in the respective cluster. The nodes then register to the corresponding cluster-head by transmitting a message back to the chosen cluster head using Carrier Sense Multiple Access (CSMA) MAC protocol and Once the cluster head receives all the registrations, it allocates a communication time slot to each member node based on Time Division Multiple Access (TDMA). The member nodes of the cluster send the sensed data to the cluster-head only during the allotted time slot. The main objective of using TDMA is to prevent intra-cluster collisions. After the reception of all the data, the cluster head consolidates the data using Data fusion technique [8,9]. Once the data is fused by the cluster-head, it will be sent to the base station using Code Division Multiple Access (CDMA).

The LEACH protocol on implementation yielded considerably improved results as compared to that of the Directed Diffusionrouting protocol. The complete data transmission from the nodes to the base station is said to be one cycle or one round.

3.3 ElGamal Crypto System Model

ElGamal is based on the discrete logarithms. The ElGamalencryption-decryption scheme is one of the most popular and widely used public-key cryptosystems. It is described in the setting of the multiplicative group Z; of the field Zp = {a, 1,2,3, . . , p-1}, the field of integers modulo a prime integer p. The multiplicative group, Z_p^*, is a cyclic group generated by some generator$\alpha \neq 1$ whose order is equal to p – 1. That is, every elementof Z; is a power of a. Note that Zp is a complete residuesystem modulo p and Z; is a reduced residue system modulop.The key generation, Encryption and Decryption algorithms of ElGamal crypto systems are as follows.

ElGamal_Key Generation
{
Select a prime p
Select d such that $1 \leq d \geq p-2$.
Select e_1 to be prime root of p
$e_2 \leftarrow e_1^d \bmod p$
Public_ key ← (e_1, e_2 , p)
Private_key← d
Return Public_key and Private_key
}

ElGamal_Encryption(e_1, e_2, p, P)
{
Select random number r in the group G=<Zp^*, x>
// P is the plain Text.
$C_1 \leftarrow e_1^r \bmod p$ // C_1 and C_2 are Ciphertexts
$C_2 \leftarrow (P \times e_2^r) \bmod p$
return // C_1 and C_2
}
ElGamal_Decryption
{
$P \leftarrow [C_2 (C_1^d)^{-1}] \bmod p$
return P
}

3.4 Elliptic Curve Crypto system Model

ECC is better than other public key cryptosystems. Itoffers same security with smaller key sizes and consumes less memory.

Let a and b be real numbers. An elliptic curve E over the field of real numbers **R** is the set of points (x,y) with x and y in **R** that satisfy the equation $Y^2 = X^3 + a X + b$together with a single element 1, called the point at infinity.

If $4a^3 + 27b^2 \neq 0$, then the equation has three distinct roots (which may be real or complex numbers). Then corresponding elliptic curve is called non-singular and If $4a^3 + 27b^2 = 0$, then it is called singular elliptic curve. One of the elliptic curves is shown in Figure .1

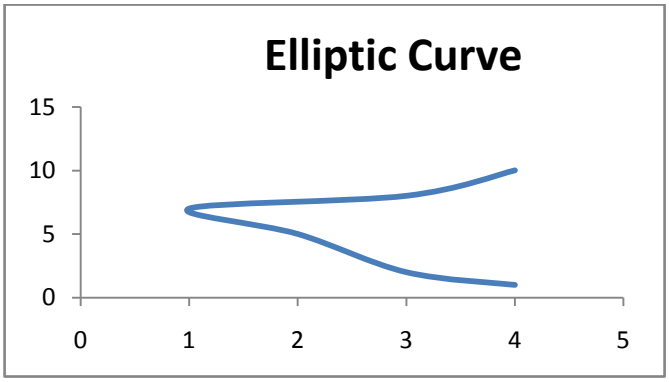

Figure.1 Elliptic Curve

ECC makes use of elliptic curves in which variables and coefficients are all restricted to elements of a finite field. For a prime curve GF(p) over Zp, a cubic is used in which variables and coefficients all take on values in the set of integers from 0 through p-1 and in which calculations are performed modulo p. It is best implemented in software. For a binary curve $GF(2^n)$ the variables and coefficients all take on values in $GF(2^n)$ and calculations are performed over $GF(2^n)$. It is best implemented in hardware.
The points on the Elliptic Curve are determined using following Psudocode.

```
Ellipticcurve_points( p, a , b)   // p is the modulus
{
x←0
while( x<p)
{
Y^2←(x^3+ax+b)mod p
If (y^2 is a perfect square in Z_p) output (x, y) (x, -y)
x←x+1
}
}
```

The key generation, Encryption and Decryption algorithms of ECC works as follows

ECC_Key_generation
Choose E(a,b) with an elliptic curve over GF(p)
Choose a point on the curve, $e_1(x_1, y_1)$
Choose an Integer d
Calculate $e_2(x_2, y_2) = d \text{ X } e_1(x_1, y_1)$
Public_key ← [E(a,b) , $e_1(x_1, y_1)$, $e_2 (x_2, y_2)$]
Private_key← d

ECC_Encryption
P is the plain Text.
Choose random number r
$C_1 \leftarrow r \text{ X } e_1(x_1, y_1)$
$C_2 \leftarrow P + r \text{ X } e_2 (x_2, y_2)$

ECC_Decryption
$P = C_2 - (d \text{ X } C_1)$
P, C_1, C_2, e_1 and e_2 are all points on the curve GF(p)

4. SIMULATION

The proposed Model is simulated using C language. The Simulation is done by taking all the parameters in to considerations and to the required number of iterations. This section describes the simulation model and simulation procedure.

4.1 Simulation Model

Here we assume a network with hundred nodes deployed over a 1000*1000 area and the base station to be at the centre of the network [11]. The assumptions made are:

- The deployment of the nodes is as shown in Figure 2.
- All the nodes considered here are homogeneous in nature having a battery power of 10000 units.
- The size packet of the packets is 3 bytes.
- The nodes which sense the temperature between 30-40˚ Celsius.
- Each operation in the network consumes considerable amount of energy of the nodes. The energy consumptions for node operations are: transmission of data-200 units, data reception-150 units and 50 units for internal processing.

A node is said to be dead of its battery power goes below 500 units.

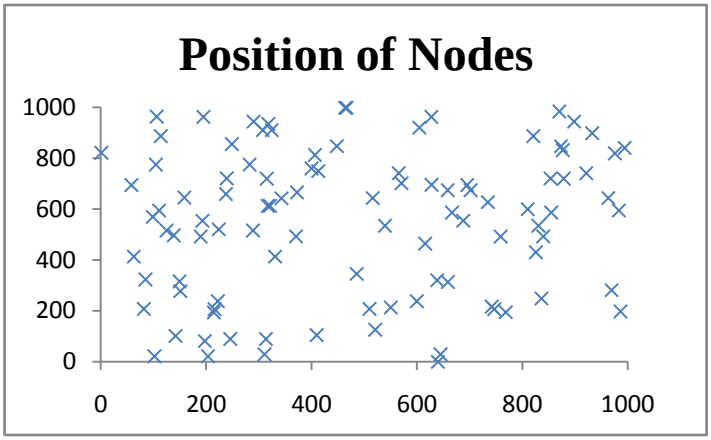

Figure 2: Deployment of Nodes

4.2Simulation procedure

In the first stage the simulation of Directed Diffusion and LEACH routing protocols are done, later security protocols ElGamal and ECC cryptosystems are incorporated onto the routing protocols.

4.2.1 Simulation procedure for the proposed Directed Diffusion and LEACH protocols

Once the network is activated it starts transmitting data to the sink till the network fails. The execution of each iteration is achieved using the following pseudo code.

Begin

- Generate network with 100 of nodes.
- Calculate the Energy Dissipation for Data transmission from a node to Sink at the end of each round
- Compute the number of Dead nodes.

End

4.2.2 Simulation procedure forElGamal Crypto system

The ElGamal Crypto system is simulated with the following parameters. p=11, e_1= 2, d = 3, r = 2.

4.2.3 Simulation procedure for ECC Crypto system

The ECC Crypto system is simulated with the following parameters. The elliptic curve is $E_{(1,1)}$ 13. The equation is $y^2 = x^3 + x + 1$. d = 2, r = 2, and $e_1(x_1, y_1) = (1,4)$.

5. RESULTS

Figure 3 shows the graph of total energy dissipated in both LEACH and Directed Diffusion protocols when run for five rounds. It shows that Energy Dissipated is more in Directed Diffusion protocol Compared to LEACH Protocol. Energy Dissipation increases gradually as the rounds increases because of multi hopping.

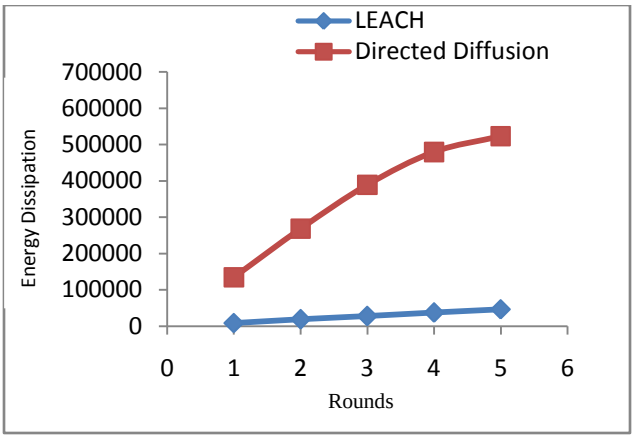

Figure 3Energy Dissipated after 5 rounds.

Figure 4 shows the number of dead nodes after 15 rounds. The Dead nodes in Leach protocol are less because of Cluster formation and Change of Cluster Head Selection at the end of eachround. In Directed Diffusion the Dead nodes are more because of Flooding and the presence of least energy node on the path.From the above graphs, we can definitely say that LEACH distributes the energy impartially among all the nodes consuming less energy and reducing the number of dead nodes, henceforth improving the network lifetime considerably

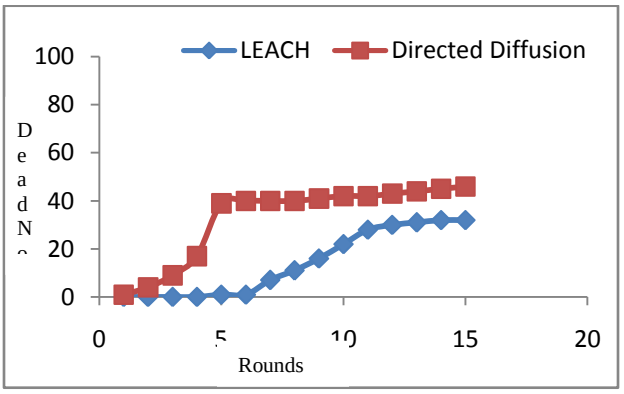

Figure 4 The number of dead nodes after 15 rounds.

The Comparisonof Directed Diffusion and LEACH Protocols are shown in Table-1. The results show that LEACH achieves 10x reduction in energy compared with Directed Diffusion and lifetime of the network increases approximately by 10 rounds.

Table 1: Comparison of Directed Diffusion and Leach Protocols

		Leach Protocol	Directed Diffusion
Total Energy Dissipation		46500 units	523050 units
No.of deadnodes	After 5rounds	1	39
	After10rounds	22	42
	After15 rounds	32	46

Figure 5 shows the graph of Directed Diffusion protocol (without security) and with ElGamal and ECC Crypto systems. In this graph the Energy Dissipation is gradually increasing linearly up to 3 rounds in all the cases and later the slight deviation in the Normal graph is because of randomly sensed data. The energy required for provision of security using ElGamal crypto system is 107100units and for ECC crypto system 129850units at the end of 1 round.

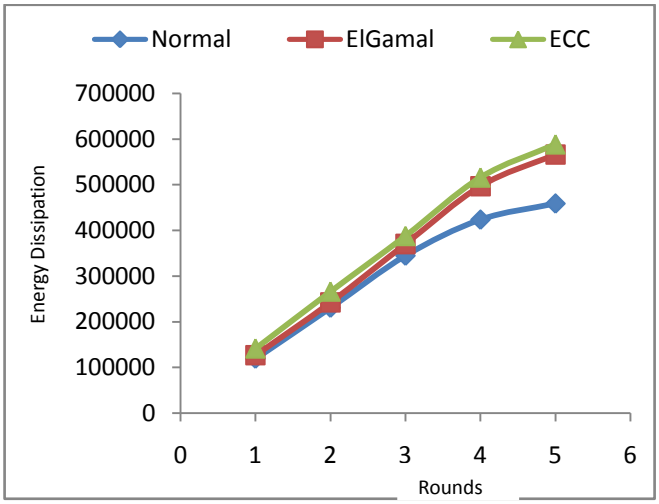

Figure.5 Energy Dissipation of Directed Diffusion protocol and with ElGamal and ECC

Figure 6 shows the graph of Leach protocol (without security) and with ElGamal and ECC Crypto systems. Here in all the three cases the Energy Dissipation varies linearly with the number of rounds. The energy required for provision of security using ElGamal crypto system is 12200units and for ECC crypto system 16900units at the end of 1 round.

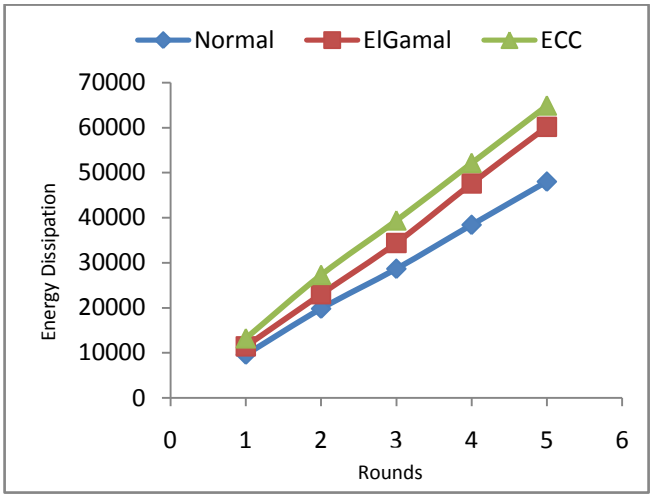

Figure. 6 Energy Dissipation of Leach protocol and with ElGamal and ECC

The results of the implementation of ElGamal and ECC crypto systems to Directed Diffusion and Leach protocols shows that,

Energy required to provide Security is marginally more. But the data will be more secured.

6. CONCLUSION AND FUTURE SCOPE.

Over the last five years, elliptic curve cryptography has moved from being an interesting theoretical alternative to a cutting edge technology adopted by an increasing number of companies. There are two reasons for this new development: one is that ECC is no longer new, and has withstood a generation of attacks; second, in the growing wireless industry, its advantages over RSA have made it an attractive security alternative. Wireless devices are rapidly becoming more dependent on security features such as the ability to do secure email, secure Web browsing, and virtual private networking to corporate networks, and ECC allows more efficient implementation of all of these features. In Future, research should focus on reduction in energy dissipation for ECC crypto systems which can be incorporated for tiny wireless devices [13].

7. ACKNOWLEDGEMENT

This work was supported in part by AICTE, New Delhi, Vide F. No. 8023/BOR/RID/RPS-16/2008-09 dated October, 30, 2008.

8. REFERENCES

[1] Iyengar, S.S.; Sharma, M.B.; Kashyap, R.L.; , "Information routing and reliability issues in distributed sensor networks," *Signal Processing, IEEE Transactions on* , vol.40, no.12, pp.3012-3021, Dec 1992.

[2] Zhao, Shousheng; Yu, Fengqi; Zhao, Baohua; , "An Energy Efficient Directed Diffusion Routing Protocol," *Computational Intelligence and Security, 2007 International Conference on* , vol., no., pp.1067-1072, 15-19 Dec. 2007

[3] Cryptography & Network Security, Behrouz A. forouzan, The McGraw-Hill Companies, Edition 2007.

[4] Cryptography and Network Security, Principles and Practices, William Stallings, Eastern Economy Edition, Fourth edition.

[5] Lauter, K, "The advantages of elliptic curve cryptography for wireless security," *Wireless Communications, IEEE* , vol.11, no.1, pp. 62- 67, Feb 2004

[6] ZhiyongPeng; Xiaojuan Li; "The improvement and simulation of LEACH protocol for WSNs," *Software Engineering and Service Sciences (ICSESS), 2010 IEEE International Conference on* , vol., no., pp.500-503, 16-18 July 2010.

[7] Intanagonwiwat, C.; Govindan, R.; Estrin, D.; Heidemann, J.; Silva, F.; "Directed diffusion for wireless sensor networking," *Networking, IEEE/ACM Transactions on* , vol.11, no.1, pp. 2- 16, Feb 2003.

[8] W. R.Heinzelman, A. Chandrakasan, and H. Balakrishnan,Energy-efficientcommunication protocols for wireless micro sensor networks", Proc. *Hawaii Int.Conf. Systems Sciences*, pp. 3005 - 3014, 2000.

[9] CmpE526 Operating System and Network Security Spring 2005 available at: http://www.cmpe.boun.edu.tr/courses/cmpe526/spring2005/ Cmpe526-20050324-AliAkkaya-PublicKeyCryptography.pdf

[10] Nishanth T.S, Rajesh A.N.K.S, Aditya Bharadwaj B N, Nikhil Chakravarthi M S, Dr.Nalini, Suresha, Mylara Reddy. C." Implementation and Comparison of LEACH and NON-LEACH Protocols in Wireless Sensor Networks"**,** *IC-CANA 2011,International Conference, NAMA Institute of Technology, Nitte*, 8-9 Jan 2011.

[11] Jing Chen; Hong Shen; , "MELEACH-L: More Energy-Efficient LEACH for Large-Scale WSNs," *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1-4, 12-14 Oct. 2008.

[12] Xueying Zhang; Heys, H.M.; Cheng Li; , "An Analysis of Link Layer Encryption Schemes in Wireless Sensor Networks," *Communications (ICC), 2010 IEEE International Conference on* , vol., no., pp.1-6, 23-27 May 2010.