Evaluation of Performance of Ciphers for Routing Protocols in Distributed Sensor Networks

Suresha
Reva Institution of Technology and Management
Kattigena halli, Yelahanka
Bangalore 560064

Nalini N.
Nitte Meenakshi Institute of Technology
Govindapura, Yelahanka
Bangalore 56006

ABSTRACT
With recent advances in communication technologies, Distributed Sensor Networks (DSNs) are widely deployed for many applications such as military, bank transactions and healthcare. These sensor nodes are equipped with lesser memory, limited battery power, little computation capability, small range of communication and then need a secured and efficient routing algorithm to forward incoming packets. In this paper, two routing algorithms viz., FLAT and HIERARCHICAL are compared with respect to energy consumption and security features in transmission of data from a source to a destination and for providing security services like confidentiality. The ciphers considered for performance analysis are symmetric (RC5), and asymmetric (ElGamal, RSA and ECC) algorithms.

Keywords

1. INTRODUCTION
A DSN comprises 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 aids in generating early warning of natural disasters. These applications often demand continuous monitoring of physical phenomena for extended period 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 which sense and communicate information.

1.1 Information Routing Issues in DSN
A processing node receives a bulk of data from the sensors at a fixed rate. After some amount of processing, this information is sent to a few or to all nodes within the network, depending on the problem solving technique. It is imperative that information is routed to the destination nodes in an efficient manner since the data generation is repetitive. Generally, data is transmitted to the destination nodes in packets.

Some of the requirements of information routing in DSN are as follows.
1. It is desirable to collect the entire information generated by a sensor in to one single packet.
2. In most of DSN applications, the sensor data will be generated and transmitted within the span of one sensing cycle. Since data exchange is almost continuous, routing protocols should be designed such that an explicit acknowledgement is not used for each packet. This saves enormous traffic on the network considering both the size of DSN and also energy constraints.
3. By not using acknowledged messages, it is necessary to ensure that the substantial 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, life time of sensor network 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. These protocols can be classified into three categories Flat, Hierarchical and Location based routing protocols. The flat routing protocols are simple, robust and suitable for small networks, whereas hierarchical protocols need to select and manage clusters, they are complex and suitable for large scale networks. In flat and hierarchical routing protocols, we have selected the Directed Diffusion (DD) and Low Energy Adaptive Cluster Hierarchy (LEACH) protocols for our analysis.

1.2 Directed Diffusion Protocol
DD, developed by Intanagonwiwat et al.[7], is a data-centric protocol. It consists of several elements-interests, data messages, gradients, and reinforcements. An interest message is a query or an interrogation which specifies what a user wants. Each interest contains a description of a sensing task that is supported by a sensor network to acquire data. Typically, data in sensor networks is either collected or processed information of a physical phenomenon. Such data can be an event, which is a short description of the sensed phenomenon. In DD, attribute value network as an interest for named data. This dissemination sets up gradients within the network designed to draw events. Specifically, a gradient is a direction state created in each node that receives an interest. The direction of the gradient is always toward the nearest node from where the interest is received. Events start flowing toward the originators of interests along multiple gradient paths. An important features of Directed Diffusion are interests, data propagation and aggregation which are determined by localized interactions (message exchanges between neighbors or nodes within some vicinity).

1.3 LEACH Protocol
LEACH is a completely distributed, clustering and the most popular of hierarchical routing protocol for DSN. It requires 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 only sensing. This means that creation of clusters and assigning special tasks to Cluster-Head (CH)s can greatly contribute to overall system scalability, life time, and energy efficiency. Communication
protocols used for data transmission TDMA, CSMA-MAC and CDMA. One complete cycle of operation of LEACH protocol is depicted in Figure 1.

![Figure 1 One cycle of operation of LEACH](image)

**1.4 Cryptosystems**

A cryptosystem is a package of all procedures, protocols, cryptographic algorithms and instructions used for encoding and decoding of messages using cryptography, which is an indispensable tool for protecting information in computer systems. There are a number of cryptographic primitives such as

- Basic building blocks - such as block ciphers, stream ciphers, and hash functions.
- Ciphers - they may either have one key for both encryption and decryption, in which case they are called shared key, they are also known as secret key or symmetric key, or they can have separate keys for encryption and decryption, in which case they’re called public key or asymmetric key.
- A digital signature scheme - it is a special type of asymmetric crypto primitive.

There are two types of algorithms, symmetric and asymmetric. The advantage of symmetric algorithm is good performance. This system is preferred when large data is to be encrypted. It uses single key for both encryption and decryption. Integral to the design of an asymmetric algorithm is the utilization of a one way trapdoor function. It has to be computationally infeasible for an adversary to retrieve the private key from the published public key of the algorithm. Asymmetric algorithms use different keys for encryption and decryption respectively. Public key is used for encryption and its related private key is used for decryption. The critical feature of asymmetric algorithm is the key pair - public key and private key. An important property of this key pair is that one of the keys cannot be obtained from the other. An asymmetric algorithms are suitable for encrypting small messages. We have selected asymmetric algorithms such as ElGamal, Elliptic Curve Cryptography (ECC) and RSA and symmetric algorithm RC5 for our analysis.

**2. RELATED WORK**

1. Routing of information from a source to a sink in DSN is an important parameter to be considered in the analysis of its energy consumption. An efficient routing algorithm is one which consumes less energy and selects the shortest path between the source and the sink. Important requirements of information routing in DSN are number of packets, reliable

routing, energy consumed and life of the network, as explained by S.S. Iyengar et al[1].

2. The Directed Diffusion protocol’s working analogy, propagation gradients and reinforced path established are explained by Zaho et al[2] and they also provide information that is used for estimation of energy consumed for the data transmission from a node to a sink (Base Station). In this paper the design problems of reinforced path for minimum delay or maximum number of packets received during a certain period of time are discussed.

3. One of the most preferred energy efficient routing protocols of DSN is the LEACH protocol. It was developed by W. R.Heinzelman et al[8]. This paper explains in detail cluster formation, cluster head selection for the first round, the procedure to be followed for the next rounds, and communication protocols used for data transmission such as TDMA, CSMA-MAC and CDMA. They also provide information about the amount of energy saved by using LEACH protocol.

4. Ali Akkaya et al [9] describes ElGamal, an asymmetric algorithm along with its advantages. ElGamal 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.

5. ECC is most preferred asymmetric algorithm. It provides a better security service for a small key size. ECC can be implemented with smaller parameters for the better level of security against the best known attacks, which leads to improved performance in wireless sensor area as explained by Lauter, K et al [5]. For elliptic curves, the group operation is written as the addition instead of multiplication, and in that case exponentiation, it is more appropriately referred to as scalar multiplication. For efficient implementation of ECC, it is important for the point multiplication algorithm and the underlying field arithmetic to be efficient. There are different methods for efficient implementation, point multiplication and field arithmetic.

6. The most commonly used asymmetric algorithm is the RSA algorithm, it is based on the factorization of large number. This algorithm cannot only be used for both data encryption and authentication. It is a safe algorithm and is easy to be implemented, as described by Yi Xiaolin et al[16].

7. RC stands for “Rivest Cipher”, RC5 is a block cipher notable for its simplicity. It was invented by Ron Rivest and analyzed by RSA laboratories. It has variable word size, variable number of rounds and variable secret key length. The distinguished feature of RC5 is its heavy use of data-dependent rotations - rotations are random variables dependent on the input data, and they are not predetermined values as said by Ali, A [17].

In the paper [1] communication issues of DSNs are discussed in detail. The authors also present distributed algorithm with the assumption of no-node/link failures. Energy required for transmission of data is not estimated in this paper. In [2] DD protocol is described in detail. The average energy required for data transmission is estimated and the concept of path-reinforcement is explained, which is used for energy calculations. The paper [8] is the original paper on LEACH protocol which is based on clusters, which minimizes global energy by distributing the load to all the nodes at different points in time. The authors describe radio model first and then make energy analysis of routing protocols for both radio model and LEACH. The advantages of LEACH protocol are also explained. In the presentation [9] basic terminology of
cryptography is explained. Symmetric and asymmetric cryptographic algorithms are also described. Also fundamentals of ElGamal and ECC systems are described in detail. The paper [16] deals with the history of RSA keys generation and characteristics, the modular mathematics and the basic principles of RSA algorithm. The RSA authentication based design of the trusted communication system is also explained. The authors also mention that with the provisioning of RSA authentication, the speed of the message transmission will be affected. Here also the amount of energy required for provisioning of security services is not estimated. In [17] the basics of RC5 algorithm are explained in detail. In this paper also energy required for the provisioning of security services using RC5 encryption algorithm is not estimated. In our work, we have estimated the energy required for the provisioning of security services (confidentiality) using RC5, ElGamal, RSA and ECC symmetric and asymmetric algorithms.

Rest of the paper is organized as follows. Motivation is described in section 3, section 4 explains the Security performance model, Section 5 provides Simulation details, Evaluation of performance analysis is discussed in section 6 and final conclusion and future scope are given in section 7.

3. MOTIVATION

With the advancement of technology, the size of the memory present in sensor nodes has increased from 8KB to 32MB. For example, XM2110CA IRIS mote and IPR2400 Imote2 have the memory power of 8KB [21] and 32MB [22], respectively. Since asymmetric encryption algorithms are more complex, significantly more secure and use, more computationally expensive algorithms with Mathematical relations, we are motivated to use asymmetric encryption algorithms to provide confidentiality to routing protocols of DSNs and evaluate their performance with symmetric encryption algorithm.

4. SECURITY PERFORMANCE MODEL

In a DSN, energy and security are two key considerations. Security is prominent entity for communications in various applications like military, healthcare, bank transactions etc. [12]. We are modeling systems to estimate the energy required for routing the information by using flat (DD) and hierarchical protocols (LEACH) routing protocols, and provision of security involves incurring additional inc of energy. We have made the model to determine the energy required to provide security service for these routing protocols by using symmetric and asymmetric crypto systems such as RC5, ElGamal, ECC and RSA.

4.1 Directed Diffusion protocol

In the Directed Diffusion protocol, a area is divided into 3 zones, namely inner zone, intermediate zone and peripheral zone and the base station is located at the center of the area. Once the network is set, we check all the hundred nodes to see which of the nodes sensed data falls in-between the specified temperature range. Only the nodes falling in this range will transmit data to the base station using multi-hop strategy. If data has to be sent by a node in the peripheral area to the base station, it first finds the nearest node in the intermediate zone and passes the data to it. This intermediate node then finds a nearest node in the inner zone and finally data will be transmitted to the base station [10].

4.2 LEACH protocol

LEACH protocol uses a distributed cluster formation technique, which enables self-organization of large number of nodes. There are two types of nodes: cluster head and sensing nodes. The sensing nodes are organized into clusters, which promote one node as the cluster head. All sensing nodes transmit their data to their respective cluster heads, which further routes it to the remote sink node [6]. LEACH uses cluster head rotation for even distribution of energy load among all the nodes within a cluster. Nodes forward their data to the sink through the cluster heads [10].

During the cluster formation, a node declares itself, randomly as a cluster head in the beginning itself with a certain probability. And then the principle of cluster head selection is carried out as follows: each node randomly generates a number between 0 and 1, if the number is lower than a threshold, it will be a cluster head, or it is an ordinary node. The threshold is calculated by the formula:

\[
T(n) = \begin{cases} 
\frac{P}{1 - p \cdot \left\lfloor \frac{m \text{ mod} (1 / p) \right\rfloor}, & n \in G \\
0, & \text{otherwise}
\end{cases}
\]

- \( T(n) \) is the threshold value.
- \( P \) describes desired percentage of Cluster i.e., 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 within each cluster, the cluster head broadcasts a message containing its ID to all the nodes in the respective cluster. 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 sensing nodes of the cluster send the data during the allotted time slot to the cluster head. Intra cluster collisions are avoided/removed by using TDMA protocol. 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 complete data transmission from the nodes to the base station is said to be a one cycle or one round.

4.3 ElGamal algorithm

ElGamal algorithm is designed by Taher ElGamal in1985. Security of ElGamal algorithm depends on the difficulty of computing discrete logarithms in a large prime modulus. ElGamal algorithm is vulnerable to chosen cipher text attacks. The security of this system depends on the key size.

The ElGamal encryption-decryption scheme is one of the most popular and widely used public-key cryptosystems. It is described in the setting of the multiplicative group \( Z_p \) of the field \( Z_p = a,1,2,3, \ldots, p-1 \), the field of integers modulo a prime integer \( p \). The multiplicative group \( Z_p^* \) is a cyclic group generated by some generator \( a \neq 1 \) whose order is equal to \( p-1 \). That is, every element of \( Z_p \) is a power of \( a \). Note that \( Z_p \) is a...
complete residue system modulo p and Z is a reduced residue system modulo p.

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 ≤ d ≤ p-2.
Select e1 to be prime root of p
e2 ≡ e1^d mod p
Public_key ← (e1, e2, p)
Private_key ← d
Return Public_key and Private_key
}

ElGamal Encryption(e1, e2, p, P)
{
Select random number r in the group G=Zp, x>
P is the plain Text.
C1 ← e1^r mod p       // C1 and C2 are Cipher texts
C2 ← (P x e2^r) mod p
return // C1 and C2
}

ElGamal Decryption
{
P ← [C2 (C1)^-y]^-1 mod p
return P
}

4.4 Elliptic Curve Cryptography algorithm

Elliptic Curve Cryptography (ECC) is based on the theory of elliptic curves. Key size in ECC is the logarithm of the number of points on the chosen prime sub group of points on the elliptic curve. The small key size in ECC provides greater security. For faster cryptographic operations and reliability, ECC can be implemented in hardware chips also. ECC is better than other public key algorithms. It offers same security with smaller key size and consumes lesser 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 Y2= X3+aX+b together with a single element 1, called the point at infinity. If 4a3+27b^2=0, then the equation has three distinct roots (which may be real or complex numbers). Then elliptic curve is called non-singular and If 4a3+27b^2 ≠ 0, then it is called singular elliptic curve. An example of the elliptic curve is shown in Figure 2.

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 on modulo p and it is best implemented in software. For a binary curve GF(2m) the variables and coefficients all take on values in GF(2n) and calculations are performed over GF(2n) and it is best implemented in hardware. The points on the Elliptic Curve are determined using following Pseudopodia.

Elliptic curve points (p, a, b) // p is the modulus
{
x ← 0
while (x < p)
   Y2 ← (x^3+ax+b) mod p
   If (y^2 is a perfect square in Zp) 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, e1(x1, y1)
Choose an Integer d
Calculate e2 (x2, y2) = d X e1(x1, y1)
Public key ← [ E(a,b) , e1(x1, y1), e2 (x2, y2) ]
Private_key ← d

ECC Encryption
P is the plain Text.
Choose random number r
C1 ← r X e1(x1, y1)
C2 ← r + P X e2 (x2, y2)

ECC Decryption
P = C2 (d X C1) ,     The minus sign here means adding with the inverse.
P, C1, C2, e1 and e2 are all points on the curve GF(p)

4.5 RSA Algorithm Model

RSA is an asymmetric encryption algorithm developed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. It is the most widely-used public key algorithm in the world. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factorizing a large integer. An RSA cryptosystem includes three basic stages: key generation, data encryption and data decryption. It utilizes a public key for encrypting plain texts and a private key for decrypting cipher texts. A key pair must be generated before each encryption or decryption process[14].

The basics of RSA algorithm are as follows.
Key Generation

The steps for generating an N-bit key pair are as follows.

1. Generation of two distinct (N/2)-bit random prime numbers, p and q;
2. Computation of $M = p^q - 1$ and $\Phi(M) = (p-1)(q-1)$, where $M$ is the modulus and $\Phi()$ is the Euler’s phi function.
3. Selection of an integer e, which satisfies the conditions $1 < e < \Phi(M)$ and $e$ is relatively prime to $\Phi(M)$ (i.e., $gcd(e, \Phi(M)) = 1$, where $gcd$ is greatest common divisor).
4. Determining d, which is the modular inverse of e modulo $\Phi(M)$ (i.e., $d = e^{-1} \mod \Phi(M)$).

The pair {e, M} is the public key pair that consists of the public exponent e and the modulus M. The pair {d, M} is the private key including the private exponent d and the modulus M. Finding two large random primes p and q is the most time consuming step which roughly determines the total time required for generating an RSA key pair.

Encryption

A plaintext $LE \in Z_{M^t}$ is encrypted to the cipher text $C \in Z_{M^c}$ using the public exponent e and modulus M as $C = L^e \mod M$, where $Z\in$ is a set of nonnegative integers less than M.

Decryption

A cipher text $C \in Z_{M^c}$ for a given plaintext $L \in Z_{M^t}$ is decrypted using the private exponent d and modulus M as $L = C^d \mod M$.

4.6 RC5 Algorithm

The RC5 symmetric encryption algorithm is a new block cipher designed by Ron Rivest in 1994. It has a variable number of rounds and a variable secret key length. It also has an advantage that, it can be implemented in memory limited platforms like microcontrollers. The novel creature of RC5 is the heavy use of data-dependent rotations. Security of RC5 relies on the rotation operation. It performs encryption on block of plain text to produce block of cipher text. For an encryption process two parties have to agree on a key and number of rotations, which are kept secret. Block diagram of RC5 is shown in Figure 3.

In Key expansion, the secret key is expanded to generate the sub keys. These sub keys are stored in S array. For generating sub keys first part key K is copied to array L [0, 1, ..., c-1]. For generating L, where c = b/u (words) where $u = w/8$. An array S is generated with help of two magic constants Pw and Qw.

The number of sub keys in array S depends upon the number of rotation i.e. number of sub keys = 2(r+1). Sub keys are stored in S array as S[1, ..., 2(r+1)].

Initially array S is generated without the use of a secret key K, as follow:

$$S[0] = Pw$$

for i = 1 to t-1
$$S[i] = S[i-1] + Qw$$
where $t=2(r+1)$

Now as the secret key K is copied in to array L, array S will be mixed with array L as follow.

$$X = S[i] = S[i] + X + Y \ll 3$$
$$Y = L[i] = L[i] + X + Y \ll (X+Y)$$

For i = (i+1)mod t
j = (j+1)mod c

Here $\ll$ means left shift. This key expansion gives a final array S containing 2(r+1) sub keys. Since these sub keys will be used for encryption and decryption. Key expansion is done at both the end of communication.

Encryption

In encryption a block of plaintext is divided into two halves (words) A and B. A contains first w bits of plaintext and B contains next w bits of plaintext. These A and B are XORed, rotated and added with sub key in one round. The encryption algorithm is described as below,

A = first half (w bits)
B = second half (w bits)

$A = A + S[0]$
$B = B + S[1]$

For i = 1 to r do

$A = ((A \oplus B) \ll i) + S[2i]$  
$B = ((B \oplus A) \ll i) + S[2i+1]$.

After completing all the rounds, final A and B are taken as block of cipher text.

Decryption

In RC5 decryption steps are absolutely in reverse order of encryption steps. It divides block of cipher text into two A and B, and followed as follow:

for i = r down to 1
5. SIMULATION

The proposed Model is simulated using C programming language. A network with hundred nodes deployed over a 1000X1000 m$^2$ area is considered and the base station is fixed at the center of the network\[10][11].

The assumptions made are:

- Deployment of the nodes is as shown in Figure 4.
- All nodes considered here are homogeneous in nature having a battery power of 5 Joules.
- The size of the packet is 3 bytes. A byte each for source address, destination address and data.
- Source nodes are situated anywhere in the specified area and the destination is the base station located at the center of the area.
- Nodes will sense the temperature in the range 30 - 40 degree celsius (Measuring temperature as an example).
- A node is said to be dead if its battery power goes below 500 mJoules.
- Each operation in the node consumes considerable amount of energy. For the energy computation, we have considered a small low-power sensor Mica2 developed by UC Berkeley. This device consists of a 7.3 MHz AT-mega 128L processor, 128KB code memory, 512 KB EEPROM, 4KB of data memory and a chip con CC1000 radio capable of transmitting range approximately 300m \[19\]. From the data sheet of CC1000[20] we have the following values as shown in Table 1.

<table>
<thead>
<tr>
<th>Supply Voltage</th>
<th>Current Consumption</th>
<th>Transmit Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Transmit mode</td>
<td>Receive mode</td>
</tr>
<tr>
<td>3V</td>
<td>26.7mA</td>
<td>9.6mA</td>
</tr>
</tbody>
</table>

Energy consumptions for various operations are:

Transmission of data-81 mJoules, data reception-30 mJoules and 10 mJoules for internal processing.

6. EVALUATION OF PERFORMANCE

The performance of Directed Diffusion protocol and LEACH protocol with respect to energy is analyzed for 8 rounds of communications and the results are shown in Figure 5. It shows that the energy consumed is more in Directed Diffusion protocol than LEACH Protocol. Hence the life of a network is less with Directed Diffusion protocol than LEACH protocol. Energy consumption increases gradually as the rounds increase because of multi hopping.

Figure 5 Energy consumed for 8 rounds.

The Figure 6. shows the number of dead nodes for 8 rounds for DD protocol and Figure 7 displays the number of dead nodes for 20 rounds for LEACH protocol. The dead nodes in LEACH protocol are lesser because of cluster formation and change of CH selection at the end of each round. In DD the Dead nodes are more because of flooding and due to the presence of least energy node on their path. The above graphs indicate 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 6 The number of Dead Nodes for 8 rounds

Figure 7 The number of Dead Nodes for 20 rounds
The Comparison of LEACH and DD Protocols are shown in Table-2. The results shows that LEACH protocol consumes less energy compared with DD protocol and hence lifetime of the network increases with LEACH protocol. In DD at the end of 9th round, the energy of all the nodes with in the inner zone will be dead. Nodes in the intermediate and periphery zones will not be able to communicate to base station and hence no life remains in the network.

Table-2 Comparison of Directed Diffusion and LEACH protocols

<table>
<thead>
<tr>
<th>Description</th>
<th>LEACH Protocol</th>
<th>Directed Diffusion Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Energy Dissipation</td>
<td>14910 mjoules</td>
<td>253241 mjoules</td>
</tr>
<tr>
<td>No. of Dead nodes of After 5 rounds</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>No. of Dead nodes of After 10 rounds</td>
<td>0</td>
<td>26</td>
</tr>
<tr>
<td>No. of Dead nodes of After 15 rounds</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>No. of Dead nodes of After 20 rounds</td>
<td>9</td>
<td>-</td>
</tr>
</tbody>
</table>

Fig 8 shows the graph of DD protocol (without security) and with RC5, ElGamal, RSA and ECC algorithms. In this graph energy consumed is gradually increasing linearly as the number of rounds increase. Energy required for provision of security using asymmetric algorithms such as for ElGamal is 262962 mjoules, for RSA 263981 mjoules and for ECC 276319 mjoules, symmetric algorithm such as RC5 is 260861 mjoules and without security (normal) is 253241 mjoules on DD protocol at the end of first round. The graph indicates that ElGamal requires less energy for the provision of security compared to ECC and RSA asymmetric algorithms and RC5 requires still lesser energy compared to asymmetric algorithms.

Energy consumption of the LEACH protocol (without security) and with symmetric and asymmetric algorithms, ElGamal, RSA and ECC is shown in Fig 9. From the graph, at the end of first round energy consumed by RC5 is 19714 mjoules, ElGamal is 24760 mjoules, RSA is 28826 mjoules, ECC is 31759 mjoules and without security (normal) is 14910 mjoules.

The results of the implementation of symmetric and asymmetric algorithms such as RC5, ElGamal, RSA and ECC to DD and LEACH protocols shows that energy required to provide security is marginally more with respect to that without security. But with security the data will be more secure.

7. CONCLUSIONS AND FUTURE SCOPE.

In this paper, the comparison of two routing protocols, DD and LEACH protocols are performed with respect to energy consumption and then the energy required for the provision of security service, confidentiality, using ElGamal, RSA, LEACH and RC5 crypto systems is estimated using C programming language. It is found that ECC consumes marginally more energy compared to RSA and ElGamal asymmetric algorithms. Since, ECC offers better security features and can withstand attacks when compared to other algorithms, it is feasible to use ECC in DSNs with an additional consumption of very few mjoules of energy. Symmetric algorithm like RC5 requires less energy for the provision of security when compared to asymmetric algorithms. As a future work, the above simulations can be simulated using a suitable network simulator and energy required for providing security to routing protocols can be compared.

8. REFERENCES


