Energy Saving Techniques for Wireless Sensor Networks using Data Compression and Routing Protocols

1Spoorthi Ganesh, 2Shubha G. N.
1PG Student, Department of ECE, D B I T, Bengaluru, INDIA
2Assistant Professor, Department of ECE, D B I T, Bengaluru, INDIA

Abstract- Wireless Sensor Networks (WSN) has emerged as one of the most exciting fields in Computer Science research over decades. Processors with on-board sensors are said to be nearing the size of a dust. Applications of WSN include military surveillance, habitat monitoring, structural monitoring and medical and health etc. Efficient utilization of energy and security has been a core area of research in wireless sensor networks. Sensor nodes used in a network are battery operated having low power capabilities. Batteries of these nodes cannot be recharged frequently in the field setting, so energy optimization becomes paramount in increasing the battery-life and, consequently, the network lifetime. To design a secure sensor network, that has low energy consumption, is a challenging issue. There are many methods to optimize power in WSN. In this project, compression and encryption techniques are used for optimizing power in WSN. Here optimization means reducing the amount of energy consumption. If the input data is large then automatically the transmitters and receivers will take more amount of energy. So here by reducing the data size by compression and by sending an encrypted version for the compression. At the receiving end by reconstructing and decryption of the data, we are able to recover the complete data. Then comparing the result with different techniques.

Keywords- Sensor nodes, Routing, Compression, Encryption.

I. INTRODUCTION
A wireless sensor are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. They are widely used in Military and national security application, Environment monitoring, Medical application. Wireless sensor networks (WSN) are collection of autonomous network of sensors placed at different geographical locations. These sensors are mainly used to monitor and measure the physical and environmental parameters and transmit the data of the same. These Wireless Sensor networks are gaining popularity because they can perform the job in the places which is out of reach of humans. Wireless sensor networks are a class of ad-hoc networks where resource-constrained sensor nodes are deployed for some kind of monitoring or control function. Fig.1 shows the data communication in WSN. A typical configuration of sensor nodes comprises one or more sensing units, one processor, memory, a communication component and a power source. Such sensors will then be used to perform measurements of some physical magnitude from the surrounding environment [1].

![Fig.1 Data communication in WSN](image-url)
transmission are more challenging due to the huge amount of information to be handled when compared to scalar data. Sensor is used to sense and track in the military, collect the data during disaster management, finding the fire in the forest, find the defect in the manufacturing process, monitoring the temperature of the building and many more applications like monitoring, tracking, detecting, collecting or reporting. The medical and military solutions require more security than other solutions. The military application uses sensor data for enemy tracking and targeting and medical solutions store the individual medical related information.

Secure data transmission deals with preventing the interception, injection and alteration of malicious data during the course of transmission. Security in WSNs is not easy compared with conventional desktop computers; severe challenges meet these sensor nodes. The sensor node which deployed in a hostile environment has limitation in processing power, storage, channel bandwidth and computational energy, prone to failure and the network topology changes frequently. We attempt to overcome these challenges, due to importance of security. Sensor networks are used sometime in very sensitive applications such as healthcare and military [2]. With this in mind we must address the security concerns from the beginning of network design. Sensor networks pose unique security challenges because of their inherent limitations in communication and computing abilities. Deployment of sensor networks in an unattended environment makes them vulnerable to potential attacks. Attackers can compromise the network to accept malicious nodes as legitimate nodes. Hardware and software improvements will address these issues at some extend but comprehensive security requires development of countermeasures such as secure key management, lightweight encryption techniques; secure routing protocols and malicious node detection mechanism.

II. ROUTING AND ENERGY ESTIMATION
Routing of data it is done by LEACH (Low energy adaptive clustering hierarchy) protocol and MG LEACH (Multigroup leach). Both LEACH and MG LEACH use single Hop transmission. LEACH is a cluster cased routing protocol, which uses distributed cluster formation. LEACH randomly selects the cluster head based on the energy of the sensor node. This is to form the sensor node based on the received signal strength and use cluster head as the routers to the base station. In LEACH, the cluster head gets the compressed data from the input sensor nodes. From cluster head it is passed to the base station. From base station it is transmitted to the other cluster head and then to the receiving node.

MG LEACH is similar to that of LEACH routing protocol. It is using same redundant nodes present in the system that locate in the same region for enhancing lifetime of the whole network. After routing of data the next important step is to calculate energy for transmission of data. Here we use first order radio model for wireless sensor networks. Here we have taken some assumptions for these networks. All sensors are within the wireless communication range when they communicate with each other or with the base station. Sensors should have homogeneous sensing, computing and communication capabilities. Base station is located in the center of the sensor networks and it has infinity energy. Thus, to transmit a k-bit message a distance d, the energy consumed is:

\[ E_u(k,d) = k \cdot E_{elec} + K \cdot E_{amp} \cdot d^2 ... 1.1 \]

Where \( E_u \) is energy consumed for transmission, \( E_{elec} \) is transmission and receiving energy and \( E_{amp} \) is amplifier energy. After calculation of energy we compare the energy consumed by different combination of encryption and compression techniques. Key management is central for most modern cryptography algorithms. The main goal of key management is to establish a key exchange between sensor nodes and between nodes and base stations, safely and reliably. Such schemes should support the addition and revocation of nodes in the network, and they must be extremely light due to the restrictions of memory, processing and energy resources in wireless sensor networks. Most WSN key management protocols are based on symmetric encryption, and there are two possible classifications for establishing keys between nodes: by network structure or by probability.

Some of the considerations for calculating energy are as shown below:

- **Parameter Value**
  - Initial energy of each node: 1 J
  - Transmission and Receiving energy: 50n J/bit Amplifier energy: 0.0013pJ/bit/m²
- **Type of distribution Random**, Energy level for node to be alive: 0.009 J.

III. PROPOSED METHODOLOGY
Large systems are always decomposed into subsystems that provide some related set of services. The initial design process of identifying these subsystems and establishing a framework for subsystem control and communication is called Architecture design and the output of this design...
process is a description of the software architecture. The architectural design procedure is a basic framework for the system. It contains many major modules of the scheme and also the communication between the components. In the following subsections we delve into the design aspects and the sub systems involved in this software package are shown in Fig.2.

![Fig.2 Architecture of the proposed system](image)

In this approach the focus is on the energy efficiency of secure communication in wireless sensor networks. Elliptic curve cryptography (ECC) is an approach to base on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography to provide equivalent security. Elliptical curve cryptography that can be used to create faster, smaller and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. According to some researchers, ECC can yield a level of security. ECC helps to establish equivalent security with lower computing power and battery resource usage; it is becoming widely used for mobile applications.

Compression Techniques Applied in Wireless Sensor Network: After encryption the following
Compression techniques are applied to the input. Compression means reducing the size of data so that it can save space while storing data and consume less energy while transmitting. Here lossless compression techniques are used. The lossless compression used are Huffman coding and Arithmetic coding.

Huffman Coding is a lossless compression developed by David Huffman. It is an entropy encoding algorithm which uses variable length code table for encoding a source symbol. The variable length code has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. It uses a specific method for choosing presentation for each symbol, resulting in prefix code. The Huffman coding can be constructed on two ideas: In an optimum code, the symbols that occur more frequently should have shorter code words and the two symbols that occur least frequently will have same length.

Arithmetic coding (AC) is a special kind of entropy coding. Unlike Huffman coding, arithmetic coding doesn’t use a discrete number of bits for each symbol to compress. It reaches for every source almost the optimum compression in the sense of the Shannon theorem and is well suitable for adaptive models. The biggest drawback of the arithmetic coding is its low speed since of several needed multiplications and divisions for each symbol. The main idea behind arithmetic coding is to assign to each symbol an interval. Starting with the interval (0...1), each interval is divided in several subintervals, which sizes are proportional to the current probability of the corresponding symbols of the alphabet. The subinterval from the coded symbol is then taken as the interval for the next symbol. The output is the interval of the last symbol. Implementations write bits of this interval sequence as soon as they are certain.

IV. RESULTS AND DISCUSSIONS
As mentioned earlier, before transmission of data to the networks it is encrypted using ECC and then using different compression techniques it is compressed. And then routing of data is done by LEACH protocol. Then energy is calculated for each combination and compared.

A. Encryption and Compression Results
As ECC is employed, after encryption also the data size remains in same so encryption here is just for a security purpose. As after encryption the data remains the same. The energy consumption mainly depends on the size of data and distance between the nodes. As the data size is decreased the energy consumed will be less for wireless sensor network. For lesser data values the comparison between Huffman and arithmetic coding is shown in Fig 4.1.

For lossless compression the energy required for computing is more compared to lossy compressed data, the energy required is less? Since here lossless compression techniques are used, comparatively Arithmetic coding has computationally lesser compressed ratio than Huffman coding shown in Fig 4.1 and Fig 4.2 here.

B. Routing Protocol Results
The LEACH Network is made up of nodes, among them cluster-heads are formed for each round. The
The job of the cluster-head is to collect data from their surrounding nodes and pass it on to the base station. LEACH is dynamic because the job of cluster-head rotates, using the leach protocol increases the life time of the network. By using MG LEACH, since groups are made and only one cluster head for each group, the nodes can evenly transfer data to the cluster heads, hence the higher performance can be achieved.

C. Main Comparison between Different Techniques

In this article, the system lifetime is characterized as the time from the earliest point at the beginning of the activity to the time once the last hub passed on. The system life is isolated into stable period and precarious period in wireless sensor networks. Stable period for the most part means the time from the earliest starting point to the time when the primary hub is dead, the precarious period is the state at the time from the failure of first hub to the end. For the better the execution of the system, the stable period must be more extended. In LEACH Protocol, Arbitrarily distributed nodes and unevenly selecting the group heads causes some bunch heads kick the nodes prior due to the low energy or the long distance to base station. Deployment of nodes in LEACH and MGLEACH Routing Protocol is shown in Fig 4.3 and Fig 4.4.

Optional cluster heads are set for these groups to be in charge of the correspondence with regular nodes; this adjusts the energy heap of group heads and keeps away from sudden passing of these cluster heads, so the steady time of system lifetime will be delayed. Fig 4.5 and Fig 4.6 is system lifetime in recreation, reenactment results shows that the system lifetime of the enhanced convention and LEACH Protocol are about the same. This demonstrates the running execution of MGLEACH is greatly improved than that of LEACH Protocol.
From the examination of Fig 4.7, we realize that in the entire running of the system, the Energy utilization of MG LEACH calculation is much lower than that of LEACH Protocol. These outcomes are reliable with the configuration reasons for enhanced calculation. Throughput vs No. of Rounds is shown in Fig 4.8.

Table 4.1 Main Comparison between Different Techniques

<table>
<thead>
<tr>
<th>Combinations</th>
<th>First Node</th>
<th>Half Node</th>
<th>Last Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEACH - HUFFMAN - ECC</td>
<td>32</td>
<td>278</td>
<td>613</td>
</tr>
<tr>
<td>LEACH - ARITHMETIC - ECC</td>
<td>32</td>
<td>277</td>
<td>606</td>
</tr>
<tr>
<td>MGLEACH - HUFFMAN - ECC</td>
<td>132</td>
<td>366</td>
<td>1305</td>
</tr>
<tr>
<td>MGLEACH - ARITHMETIC - ECC</td>
<td>135</td>
<td>365</td>
<td>797</td>
</tr>
</tbody>
</table>

V CONCLUSIONS
In this project encryption is done so that the data will be more secured and to optimize energy various compression techniques and LEACH protocol has been applied. Here lossless compression is done. We can see that more number of nodes is alive when the data is compressed. By these methods we can increase the life time of sensor nodes in wireless sensor network. There are many more issues to be resolved around energy management. By solving those we can reduce energy consumption of sensor nodes in wireless sensor networks. Particularly in the design of energy efficient protocol and its implementation has a significant scope.

REFERENCES


