Enhancing Data Transmission and Protection in Wireless Sensor Node- A Review

Prajwali wamanrao Gawande [1], Prof. Vijay Bagdi [2]

[1] Department of Computer Science and Engineering Abha Gaikwad Pati College of Engineering Nagpur, *Maharashtra, India*

[2] Department of Computer Science and Engineering Abha Gaikwad Pati College of Engineering Nagpur, *Maharashtra, India*

---***---

Abstract-A wireless sensor network (WSN) have many different spatially distributed independent Sensors to observe physical or environmental conditions, such as sound, temperature, pressure, etc. and to pass their data to a main location through the network. Adittional Traffic is created with manegment requests and responses and the data issuing from the network's actual sensing application. Sending and processing the data together, rather than individually can reduce the system's energy. As the processing of data in WSN consumes more energy. So the data is being transmitted without processing it. By applying various cryptographic techniques we can transmit the data securely over WSN. In this paper we discuss the problem with wireless sensor network and have proposed the technique for increasing the efficiency of a node as well as for transmitting the data securely.

Keyword: - WSN, RC-6, LEACH

1. INTRODUCTION

Each sensor node has a constraint energy capacity in wireless sensor network, so energy-efficient mechanism is important. Sending packets from the source node to the destination node should be at highest priority than rather sensing the event. A typical node (Berkeley node) in [13] have a configuration of 8-bit CPU(4MHz), 128KB flash,4KB RAM and Transmission range of 100 Feet. The nodes in WSN are made of electronic devices that are able to sense, compute and transmit data from physical environments. These sensor nodes have limited energy resources. So, to extend the lifetime of network, energy resources for wireless sensor networks should be managed wisely.

1.1Efficiency of node:-

In wireless communications, energy wastage shortens the networks lifetime.

Following are the 4 reasons of energy wastage.

1) Collisions:-

When two nodes transmit at the same time and interfere with each other.

2) Idle listening: -

It happens when the radio is listening to the channel to receive a possible data that is not sent.

3) Overhearing: -

When a sensor node receives packets that are not destined to it.

This is the dominant factor of energy wastage, when traffic load is heavy and node density is high.

4) Control: -

Packet overhead for protocols to exchange required information.

Security: -

Basically nature of WSN is to design low power, which forces security mechanisms to fit under very limiting processing and bandwidth constraints, so security to data has been the challenging issue. The security requirements in WSN are the authentication of entity, message, data, especially in data critical applications. It is observed in [12] that due to Sensor Node Constraints and Networking Constraints in WSN's. Most of the protocols [13][14] are based on Symmetric key cryptography.

2. OVERVIEW OF EXISTING METHODS

This section provides review of the existing techniques for important roving energy efficiency of node and provides security to data. Author in [1] has worked on improving the energy efficiency of the node. By considering some parameters.

2.1 By Reducing the Communication Costs Radio:

In most wireless sensor network platforms, one of the key energy consumers is Communication. When the data is not been sent or receive. There are different medium access protocols that allow the radio chip to be put into a low power sleep mode (eg. BMAC, XMAC, and SMAC). Avoiding radio communication saves energy. The conclusions for this observation for a management system were discussed.

1) The management data was sent first, followed by the sensing data after a gap of four seconds.

2) Sending the management data and the sensing data together in a single packet

2.2 Different Degrees of Co-operative Behavior:

Either the management framework or the application has to wait for the next packet to be sent, if packets are to be shared between the sensor network application and the management framework. As decided that there should be no delay for messages sent by the application. In this paper [2] Author has focused that during idle listening energy wastage should be reduced.

Toughest task is co-coordinating the awake schedule of both sender and receiver. They have designed Neighborhood-based Power Management (NPM), an energy-efficient hybrid MAC protocol that balances synchronization and signaling overhead. In which a sender knows exactly when a receiver is awake either through a priori knowledge of or by synchronizing the wakeup schedules. Thus, senders and receivers wake up at the same time, transmit their data, and then go back to sleep.

2.3 Signaling Mechanisms:-

[2]All nodes in NPM periodically get active then they poll the channel for activity to receive incoming data messages. Due to the imperfect (out-of-date) synchronization information available to the nodes, NPM must use preambles before the actual data Messages, to signal the receivers that they must stay active until the data messages are received.

In this paper [3] Author has worked on Security of data in WSN. Identity-based attacks are considered the first step in an intruder's attempt to launch a variety of attacks, including denial of service (DOS), session hijacking, man-in-the-middle, data modification, and sniffing. Following are the two proposed techniques:

Software-based fingerprinting:-Off-the-shelf wireless Devices and existing software ca be used for recording and extracting Software-based fingerprinting. Specifically, by putting the wireless card in monitor mode and using TCP dump or wire shark, all frames sent over the air can be sniffed. Therefore, the frame/beacon interval, frame size, and source and destination addresses of a frame can be easily obtained.

Hardware-based fingerprinting:- It is the reflection of defects/unique design of the hardware on the transmitted wave forms. This signature scheme uses the inherent hardware imperfections and characteristics. It is hard to spoof the signature by using off-the shelf wireless devices.

In this paper [4] DES algorithm has been used to encrypt and decrypt data.

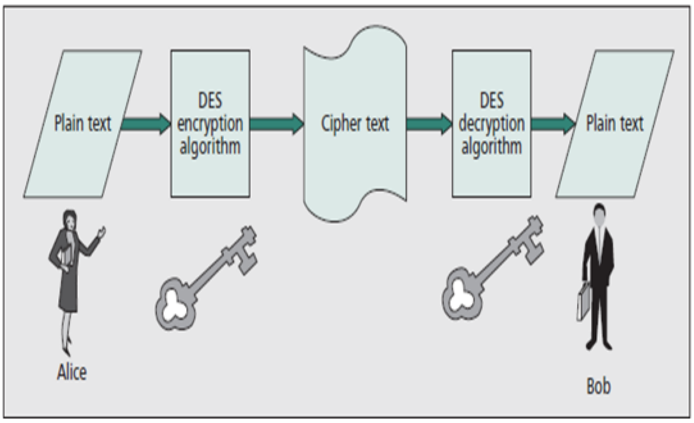

Fig1:-The symmetric data encryption/decryption algorithm has been widely used in networks.

In fig 1:- Alice sends an encrypted message to Bob with a secret key. Bob may use the secret key to decipher the message. Because this message has been encrypted, even if the message is intercepted, the eavesdropper between Alice and Bob will not have the secret key to decipher the message [4].

In paper [5], author has introduced a scheme that could be used to achieve physical layer security against different attacks. They have classified the existing physical layer security methods into five major Categories: theoretical secure capacity, channel, coding, power, and signal detection approach.

The security services in a WSN should protect the information transmitted over the public channels and the resources from attacks and misbehavior of nodes. They have proposed a protocol based on RSA.

Tiny PK: Watro et al [11] has proposed Tiny PK security scheme. It is used to authenticate the user (external agent). It allows the sensor to share a session key with external agent. The infrastructure requirement for Tiny PK is CA, EA and WSN. CA is a trusted Certification Authority. It is an entity with public and private keys. CA is a trusted entity by all friendly units. EA is an External agent is an entity who tries to communicate with a sensor of WSN. Every node is loaded with CA public key while deploying into the network.

3. PROPOSED METHODOLOGY

Hera we have proposed a methodology to increase efficiency of node and a technique to provide data security.

LEACH Protocol has been used for increasing the Efficiency of node we are using a protocol ie.. LEACH is the earliest proposed single-hop clustering routing protocol in WSN; it can save network energy greatly compared with the non-cluster routing algorithm. In LEACH protocol, all clusters are self-organized, each cluster contains a cluster-head and several non-cluster head nodes, and cluster-head node consumes more energy than non-cluster head nodes. With the purpose of balancing network energy consumption and prolonging the network life cycle, it selects cluster head randomly and each node has an equal chance to be cluster-head [9]. Many other clustering algorithm are proposed based on LEACH, such as TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol)[6] ,PEGASIS(Power Efficient Gathering in Sensor Information Systems)[7] ,HEED(Hybrid Energy-Efficient Distributed Clustering)[8]. The cluster structure update constantly and a single updating process are called a round. Each round cycle consist two stages: set-up phase and steady-state phase,

- Set-up phase is the establishment phase of the cluster:- Each node generates a random number between 0 to 1, and compares this number with the threshold value T(n). If the number < T(n), the node is selected as a cluster-head,
- The threshold T(n0) is set as follow;

$$T(n) = \begin{cases} \dfrac{p}{1 - p * (r \bmod \dfrac{1}{p})} & \text{if } n \in G \\ 0 & \text{if } n \notin G \end{cases}$$

Where n refers the node identification in the current sensor network; p is the percentage of cluster-heads; r is the current round number; G is the set of nodes that have not been elected as cluster-head in the last 1/p rounds.

Steady-state phase is the stable data transfer phase, members of the cluster send data to the cluster-head in the way of single-hop during the allocated slot according to the TDMA table, the cluster-head receives all the data from each node in the cluster, fuses all the data into a single signal, then the fusion signal is transmitted to the base station by cluster-head. Data transmission lasts a certain time, and then the entire network comes into the next round.

For Security of data in WSN:-We are using a symmetric key algorithm ie. RC6 (Rivest Cipher 6)[15] for security of data. RC6 is a symmetric key block cipher derived from RC5.RC6 has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits.

Encryption and Decryption Operation.:- RC6 works with four w-bit registers A,B,C,D which contain the initial input plaintext as well as the output cipher text at the end of encryption. The first byte of plaintext or cipher text is placed in the least-significant byte of A; the last byte of plaintext or cipher text is placed into the most-significant byte of D.

We use (A;B;C;D) = (B;C;D;A) to mean the parallel assignment of values on the right to registers on the left.

4. CONCLUSION

Hence we have studied various energy efficiency techniques and have also proposed the protocol which is used to improve efficiency of node. We have proposed an algorithm ie. RC6 (Rivest Cipher 6) to transmit the data securely over WSN, which has a key size of 128 bits. Thus the proposed technique is an effective and secure approach to improve efficiency of node.