ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

A Survey on Wireless Sensor Network Attacks

Manju.V.C.

***Abstract*—Efficient design and implementation of wireless sensor networks have become a hot area of research in recent years due to the vast potential of the sensor networks to enable application that connect the physical world to the virtual world. Wireless platforms are becoming less expensive and more powerful, enabling the promise of widespread use for everything from health monitoring to military sensing. While wireless sensor networks are quite useful in many applications it appears that they are more vulnerable to attacks than wired networks. So there is a need to have better wireless sensor security .This paper studies the security aspects of wireless sensor networks. Here we have done a study on the current security threats, countermeasures, link layer protocols and cryptographic communication schemes.**

***Index Terms*—Wireless Sensor Network, Security, Link Layer Encryption.**

I. INTRODUCTION

A wireless sensor network consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions such as pressure, temperature, sound, vibration motion or pollutants. WSN is used to locate not only the objects whose area of location is known but also the objects whose location is anticipated to be around a certain domain. Each node in a sensor network is typically equipped with a radio receiver, a small micro controller, energy source usually a battery. Sensor networks can be used for target tracking, system control and chemical and biological detection. In military application's sensor, networks can enable soldiers to see around corners and to detect chemical and biological weapons long before they get close enough to cause harm them...Civilian uses include; environmental monitoring, traffic control and providing health care monitoring for the elderly while allowing them more freedom to move around. Sensor networks are typically characterized by restricted power supplies, low bandwidth, small memory size and limited energy. This leads to a very demanding environment to provide security. Radio frequency communication is used in sensor networks for communication between sensor nodes. So security of this broadcast communication is of paramount importance and one of the difficult issues to resolve. In a broadcast medium it is easy to intercept, eavesdrop, inject and change transmitted data .Sensor network installations may be done on an insecure setting; enemies can steal nodes, hack cryptographic material and pose as the authorized nodes. Sensor networks can also be pushed to resource consumption attack. This means enemies would send data to drain a node battery and reduce network bandwidth. Figure 1 below shows a wireless sensor network. Sensor network is typically the cluster based and has irregular topology. Clusters are interconnected to the main base station. Each cluster contains a cluster head responsible for routing data from its corresponding cluster to a base station. Sensor networks often have one or more points of centralized control called base station. The wireless sensor node is equipped with a limited power source such as battery, sensor unit, processing unit, storage unit and wireless radio transceiver; these units communicate each other. A base station is typically a gateway to another network, a powerful data processing or storage center or an access point for human interface; communicating nodes are normally linked by a wireless medium such as radio.

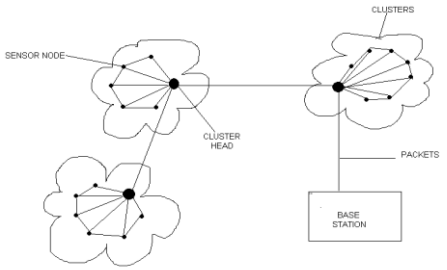

Fig 1 .Wireless sensor network

Most of the research on this topic is revolved around security solutions using the layered approach. The layered approach is shown in the figure 2. In layered approach the protocol stacks consists of the physical layer, data link layer, network layer, transport layer and application layer. These five layers and the three planes, i.e., the power management plane, mobility management plane and task management plane jointly forms the wireless layered architecture. The physical layer forms the hardware layer of the wireless communication path. The transmission and reception of the signal are the responsibility of the physical layer. The next layer the data link layer takes care of the media access control MAC protocol which in turn manages communication over noisy channels. Network layer manages the data routing, and transport layer maintains the data flow. The application layer interacts with the final user.

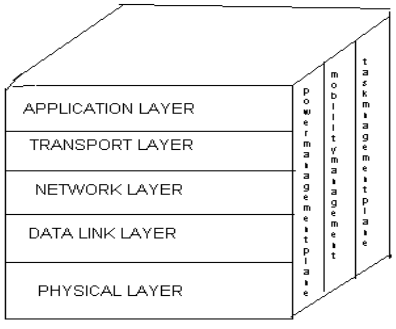

Fig 2. Layered Protocol Architecture

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

II. NECESSARY SECURITY REQUIREMENTS

1. Availability

Ensure that the desired network services are available even in presence of denial of service attacks.

2. Data Confidentiality c

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor reading to neighboring networks. In many applications, nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. Since public key cryptography is too expensive to be used in the resource constrained sensor networks most of the proposed protocols use symmetric key encryption methods.

3. Data Authenticity

In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source Data authentication prevents illegitimate parties from participating in the network, and legitimate nodes should be able to detect messages from illegitimate nodes and reject them. In a two-party communication case, data authentication can be achieved through a purely symmetric mechanism. The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives at the receiver knows that it must have been sent by the sender.

4. Data Integrity

Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Data authentication can provide data integrity also.

5. Data Freshness

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages.

6. Robustness and Survivability

Sensor network should be robust against the various attacks and if an attack succeeds its impact should be minimized.

7. Self-Organization

Nodes should be flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant).

8. Time Synchronization

These protocols should not be manipulated to produce incorrect data.

III. SECURITY THREATS IN WSN

There are many attacks that have been identified in WSN by the researchers. These security attacks can be classified on various criteria, such as the domain of the attackers, or the techniques used in attacks. This security attacks in WSN, and all other networks can be roughly classified as: passive or active, internal or external, attacks on protocol layer, stealthy or non-stealthy.

1. Passive and Active Attack

WSN link layer threats are classified based on damage level or attacker's access level. Passive attack involves data exchange in a network without any interruption in communication. Active attack involves disruption of the normal activity of the network like information interruption, modification or fabrication passive attacks are interception, traffic analysis, and traffic monitoring. Active attacks are jamming, impersonating, and denial of servicing and message replay.

2. Internal Attack and External Attack

The domain attacks can be classified as internal (insider) or external (outsider) attack. External attacks are carried out by nodes that are not part of the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows the valuable and secret information.

3. Stealthy Attacks against Service Integrity

In a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential. DoS attacks against WSNs may permit real-world damage to the health and safety of people.

4. Mote Class versus Laptop Class Attacks

Mote-class versus laptop-class attacks: In mote class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an adversary can use more powerful devices like a laptop, etc. and can do much more harm to a network than a malicious sensor node.

5 Attacks on Network Availability

Attacks on network availability are often referred to as Denial-of-Service (DoS) attacks. DoS target usually targets one of the five OSI layer of a sensor network.

A. Physical Layer Attacks:

Most wireless communications use the RF spectrum and broadcast medium. Signal wireless broadcast over the airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be overheard, and fake messages can be injected into the network. Radio signals can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, the generated signal can even overwhelm the targeted signals and disrupt communication. The most common types of jamming attacks in WSN are constant, deceptive, random, or reactive. A constant jamming attack corrupts packets attacks are the typical examples. Sinkhole attack is an attack in which the attacking node is inserted into the traffic of the network by giving greed to the other nodes that it contains some useful information and allowing its entry. Wormhole Attack: In wormhole attack, the attacker takes the message from one area and

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

displays in the other area. However, this attack requires a significant amount of energy. This attack might not be feasible if the attacker is under similar power constraints as the target network. Instead of transmitting a random signal, a deceptive jammer sends a constant stream of bytes into the network.

B. Link Layer Attacks

MAC protocols to operate at the link layer, and most require coordination between nodes to arbitrate channel use, making them, particularly vulnerable to DoS attacks. Link-layer threats include collisions, interrogation, and packet replay. You can reduce some collisions by using error-correcting codes. Even though, ECCs adds transmission overhead, consuming additional energy. An interrogation attack exploits the two-way Request-To-Send/Clear To- Send (RTS/CTS) handshake that many MAC protocol used to reduce the hidden-node problem. An attacker can exhaust the node's resources by repeatedly sending RTS messages to allow CTS responses from a targeted neighbor node. Anti-replay protection and strong link-layer authentication can also reduce these attacks. However, a targeted node receiving the bogus RTS messages still consumes energy and network bandwidth. Another link-layer threat to WSNs is the denial-of-sleep attack, which prevents the radio from going into sleep mode, which is called the denial of sleep attack. MAC protocols are a natural focus for denial-of-sleep attacks. WSN is susceptible to denial-of-sleep attacks, which reduce the network life span from years to days. The attack imposes large amount of energy consumption on the sensor nodes that the entire charge is consumed by the load levied upon the network, and the nodes stop working.

C. Network Layer Attacks

By attacking the routing protocols, attackers can absorb network traffic, inject into the path between the source and destination, and control the network traffic flow. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Routing message flooding attacks such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are targeting the route discovery phase. A malicious node advertises routes that change non-existent nodes to the authorized nodes present in the network. This happens in proactive routing algorithms, where routing information is updated periodically. The attacker tries to create enough routes to prevent new routes from being created. The proactive routing algorithms are more vulnerable to table overflow attacks as they attempt to discover routing information before its actual need. An attacker can simply send excessive route advertisements to overflow the receivers routing table. There are attacks that target the route maintenance phase by broadcasting false control messages. More sophisticated and subtle routing attacks have been identified in recent research papers. The black hole (or sinkhole), Byzantine, and the wormhole makes the adversary eavesdrop upon useful information and display it in another area, thus redirecting the message traffic. The packets of information are tunneled and then displayed. Sybil attack: The Sybil attack is a case where each node presents more than one identity to the network protocols and affected algorithms include fault-tolerant schemes, distributed storage, and network-topology maintenance. For example, a distributed storage scheme may rely being there with three replicas of the same data to achieve a given level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved not, in reality.

D. Transport Layer

The objectives of Transport layer protocol in WSN include setting up of end-to-end connection, end to- end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection .SYN flooding attack: The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a receiver or victim node, but never completes the handshake to fully open up the connection. For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. The three messages exchanged during the handshake allow both nodes to learn that the other node is ready to communicate and also agree on initial sequence numbers for the conversation. During the attack, a malicious node sends a large amount of SYN packets to a victim/receiver node, spoofing the return addresses of the SYN packets. The victim after receiving the SYN packets from the attacker sends them and awaits the ACK packet response. Without receiving the ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed size table while it awaits the acknowledgement of the three-way handshake, all the pending connections would result in an overflow of buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection.

E. Application Layer

The application layer communication is also vulnerable in terms of security when compared with other layers. The application layer contains user data, and supports many protocols such as HTTP, SMTP, TELNET, and FTP, which provide many vulnerabilities and access points for attackers. The application layers attacks are more attractive as they have direct access to the application data malicious node attacks: Malicious node, such as viruses, worms, spy wares, and Trojan Horses, can attack both operating systems and the user applications. These malicious programs spread themselves across the network and resulting in computer or

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

network slow down or even damaged. Repudiation attacks: Repudiation refers to a denial of participation in all part of the communication.

IV. LINK LAYER ENCRYPTION TECHNIQUES

As we described before the four major parts of security requirements are data confidentiality, data authentication, and data integrity and data freshness. In a cryptographic communication scheme encrypted data (cipher text) takes the place of plaintext (original payload) to achieve the data confidentiality. Security's installations use encryptions to transmit digital data over sensor networks. For the authentication of an encrypted communication between two sensor devices a digital key is needed. This authentication and encryption process should work on low power mode and should have low complexity requirements. The two basic encryption techniques used for WSN are symmetric and asymmetric. In a symmetric-key algorithm, both parties use the same key for encryption and decryption. Symmetric encryption algorithm uses multiple rounds of substitution and transposition to convert plaintext to cipher text. Substitution involves mapping one element with another element of the same size, and transposition simply rearranges elements. One drawback of this symmetrical encryption is the potential difficulty of securely distributing the encryption key throughout the network. Some well known symmetrical ciphers are data encryption standard (DES) and the advanced encryption standard (AES). Asymmetric cryptography uses different keys for encryption and decryption. Each node in the network has a pair of keys, the private key and the public key (RSA, Diellman, and ECC). Asymmetric or public key cryptography eases the problem of key distribution by removing the requirement for security in the key distribution mechanism. In public, key each node has a private key which it alone maintains and a public key which is distributed in plaintext to all potential communication partners. Text encrypted with the pubic key can only be decrypted using private key. If a node wants to send a secure data to another node it simply encrypts the data using receiver's public key, and the only receiver is able to decrypt it. Public key provides for message integrity asymmetric uses longer key sizes up to 1024 bits, which consume more RAM on sensor devices. Since public key cryptography are too expensive to be used in the resource constrained sensor network most of the proposed protocols use symmetric key encryption methods. Symmetric encryption is preferred in WSN due to significantly lower computational and key storage overheads. A Message Authentication Code functions as the cryptographic check sum providing data integrity and data authentication. We take a packet as correctly transmitted MAC value equals the transmitted MAC value and assumes the difference is caused by a malicious attacker.

V. VARIOUS PROTOCOLS IN SENSOR NETWORKS

The major security needs of wireless sensor network are data integrity and authenticity. Various security mechanisms can be used to provide sensor network security. But most security schemes are a resource intensive. Cryptographic and protocol based solutions are the most important schemes for sensor network security. This is some of the protocol based schemes.

A) *SPINS*

Adrian Perig et al developed a suite of security block, which consist of: SNEP and µTesla. The functionality of the Sensor Network Encryption Protocol (SNEP) block includes data confidentiality and authentication. SNEP has minimal data over the head of only 8 bytes. As stated earlier data transmission over wireless is energy intensive. Like other protocols SNEP also uses a counter, but the counter is shared between sender and receiver to keep a low communication overhead. As a shared counter mechanism is used, and this counter is incremented after each block, the counter is not transmitted with the message. SNEP uses message authentication (MAC) to achieve data authentication during communication between two parties. The value of the counter in MAC prevents re transmission of old messages again. The counter also helps verifying the message order ie, previous message counter value should be lower than the current one. µTesla is used to achieve asymmetric cryptography and is a micro version of timed efficient streaming loss tolerant authentication protocol. by delaying the disclosure of the symmetric keys. Message generated with a secret key is broadcasted, and the secret key is disclosed by the sender after some time. The message packet is buffered by the receiver until the secret key is disclosed.

B)TINYSEC

Karlof. Designed the replacement for the unfinished SNEP known as Tiny Sec. Tiny sec architecture is based on link layer security and is light weight package integrated into sensor networks. It supports both message authentication and encryption or authentication only. Non encrypted packet is used to compute the authentication code. A major difference between Tiny Sec and SNEP is that there are no counters used in Tiny Sec. In Tiny sec; encryption is done using CBC mode with cipher text stealing, and authentication is done using CBC-MAC. . There are two packet formats defined by Tiny Sec. this is Tiny Sec-Auth, for authenticated messages, and Tiny Sec-AE, for authenticated and encrypted messages. In Tiny Sec-AE packet, a payload of up to 29 bytes is specified, with a packet header of 8 bytes length. Encryption of the payload is necessary, but the MAC is computed over the payload and the header. Tiny Sec- Auth's packet can carry up to 29Bytes of payload. The MAC is computed over the payload, and the packet header is 4 bytes long. Generally, the security of CBC-MAC is directly related to the length of the MAC. Tiny Sec specifies a MAC of 4 Bytes, much less

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

than the conventional 8 or 16 bytes of previous security protocols in the context of sensor networks, Tiny sec uses an 8 byte Initial Vector and cipher block chaining. The structure of IV is dst//AM//l//src//ctr where dst is the destination address of the receiver. AM is the active message handler type, l is the length of the data payload, src is the source address of the sender and ctr is a 16bit counter. The counter starts at 0, and the sender increases it by 1 after each message sent.

C) MINISEC

Mini sec consumes lower energy than tiny sec but the level of security achieved is equivalent or more than Zigbee. Mini sec uses offset codebook (OCB) mode as its cipher mode. Usually an authenticated encryption is done by two passes over the message packet but achieved with only one pass in OCB. In OCB, the cipher text is of the same length as the plain text; so padding or cipher text stealing is not used. Minisec offers higher replay protection over another security protocols without transmission over heads or problems related to countering synchronization. Mini sec operates in different modes for unicast packets (Mini Sec-U) and one for broadcast packets.

D) LEAP (Localized Encryption and Authentication Protocol)

Sencun Zhu et. al. proposed LEAP Protocol, which is a key management protocol for sensor network. It supports access control, data encryption and frame integrity to provide the basic security services such as confidentiality and authentication. LEAP supports four types of keys for each sensor node those are individual key, group key, cluster key and pair wise shared key. LEAP includes an efficient protocol for inter node traffic authentication based on the use of key chains. And also it supports source authentication without precluding in network processing and passive participation.

E) ZIGBEE

IEEE 802.15.4 is also known as Zigbee. It gives the details of the architectural requirement for a particular class of wireless radios and protocols for personal area network devices in wireless sensor nodes. The specification provides hardware support for data confidentiality and integrity in compliant devices mandating the use of Advanced Encryption Standard (AES) encryption and message integrity code (MIC) to provide support.

V. CRYPTOGRAPHIC MODES

A mode of operation is a scheme to provide flexible implementation of a symmetric key block cipher when operating on a large amount of data. In symmetric encryption, messages are broken down into blocks of data, and transformations are executed over these blocks. A given plain text block is encrypted using a specific encryption key will always result in the same cipher text. This makes it easier for adversaries to break an encryption mechanism or to remove or substitute message blocks to prevent different types of attack. Mode determines how to use the block cipher to derive the cipher text and has an impact on the communication energy cost in WSN. Tiny Sec and SPINS are examples of proposals, which do explicitly recommend a mode of operation for block ciphers applied to WSN .Block cipher modes of operation are used to ensure that repeated plaintext blocks result in different cipher text by using a portion of the previous encrypted block. Block cipher modes are Electronic Codebook (ECB), Cipher Block Chaining CBC, Cipher feedback (CFB), Counter (CTR) and Output feedback (OFB) Selection of an appropriate mode of operation for the block cipher is vital otherwise possible troubles might occur when applying the scheme in a realistic WSN, such as an operation mode related security weaknesses, error propagation, and loss of data synchronization. IV plays an important role in cryptography. . When encrypting a block of data unique initialization vector is used in the initial stages of this process to ensure that cipher text will be different even for the same plaintext. Generally, the IV is XOR ed with the first data block before encryption, so that the plaintext data can be randomized thereby effectively eliminating the repetition of data input to the cipher - an important security consideration in counter mode, the IV is used to initialize the counter value In CFB mode. The IV can be used to reset the feedback at the block cipherinput.

VI. CIPHER BLOCK CHAINING

Cipher block chaining mode is a usual selection for encrypting large amount of data and is proposed to be used in tiny sec. Cipher text size cannot be decreased below the block size when the amount of plaintext is less than the block size of the cipher. In CBC mode of encryption, IV is included in each packet transmitted so that the receiver can retrieve the IV straight from the received packet while decryption. The negative side of this system is that IV needs extra bits to be transmitted which enhance the energy cost of each packet.

VII. COUNTER MODE

Counter mode is proposed to be used in the SPINS scheme taking advantage of the efficiency and security of a stream cipher approach. Counter mode of encryption demand a periodic transfer of IV to assure the encryption decryption process remain synchronized. For this function IV can be communicated periodically within a particular IV packet which is different from IV packet. A newly received IV initializes the counter and later on the count increases by one after each block encryption

VIII. CIPHER FEEDBACK MODE

In CFB mode. Block cipher can be assembled in a packet encrypted by XORing the plaintext block with the output of the block cipher which has used the previous cipher text

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

block as input. We shall consider an approach that resets the feedback at the start of each packet by using the preceding cipher text from the payloads of previous packets as an IV block to be fed to the block cipher input. CFB scheme does not consume extra energy for either including IV bits in each packet or transmitting separate packets of IV frequently.

IX. CONCLUSION

In this paper, we give the brief description of the Wireless sensor network requirements and security problems. We also discuss about the various security challenges, and an analysis is done on various link layers protocols and cryptographic mode.

ACKNOWLEDGMENT

The authors would like to thank all reviewers; whose comments helped to improve this paper.

REFERENCES

[1] "Authentication and Anti-replay Security Protocol for Wireless Sensor Networks" Laura Gheorghe, Răzvan Rughiniş, Răzvan Deaconescu, Nicolae Ţăpuş. 2010 Fifth International Conference on Systems and Networks Communications.

[2] "Security and Performance Aspects of an Agent-Based Link-Layer Vulnerability Discovery Mechanism" Ziyad S. Al-Salloum.Information Security Group Royal Holloway, 2010 International Conference on Availability, Reliability and Security.

[3] Shivangi Raman et al. "Wireless sensor networks: A Survey of Intrusions and their Explored Remedies" International Journal of Engineering Science and Technology Vol.2 (5), 2010.

[4] "An Analysis of Link Layer Encryption Schemes in Wireless Sensor Networks." Xue ying Zhang, Howard M. Heys, and Cheng Li IEEE communications. 2010 proceeding.

[5] An isolation Intrusion Detection system for hierarchical wireless sensor networks.Rung-ching chen,Chia Fen Hsiegh and Yung Fa Huang .ung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang Chaoyang University of Technology, Taichung, Taiwan, R.O.C.

[6] David R. Raymond et al "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols "IEEE Transactions on Vehicular Technology, Vol 58, No.1 January 2009.

[7] Replay Protection at the Link layer Security in Wireless Sensor Networks. Devesh Jinwala S. V. National Institute of Tech., Surat, India, Dhiren Patel.

[8] http://en.wikipedia.org/wiki/Wireless_sensor_network.

[9] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.

AUTHOR'S PROFILE

Manju.V.C received BE Degree from M.S university, India and M.E Degree from M.K University .Currently she is doing PhD under University of Kerala, India. Her research interest includes wireless networks .wireless sensor networks and link layer protocols