International Journal of Computer Engineering Science (IJCES)
Volume 2 Issue 3 (March 2012) ISSN : 2250:3439
https://sites.google.com/site/ijcesjournal http://www.ijces.com/

Wireless Sensor Network

Mr. Madhav Bokare[1] Mrs. Anagha Ralegaonkar[2]
[1] HOD, Dept. of Comp. Sci, ITM, Nanded, Maharashtra, India.
bokaremadhav@yahoo.com
[2] Lecturer, Dept. of Comp. Sci, ITM, Nanded, Maharashtra, India.
anaghakjoshi@yahoo.co.in

Abstract: Sensor networks are expected to play an essential role in the upcoming age of pervasive computing. Due to their constraints in computation, memory, and power resources, their susceptibility to physical capture, and use of wireless communications, security is a challenge in these networks. In this paper we just take a glance at the wireless technology and take a tour of wireless sensor networks. This paper gives brief outline related to wireless sensor network and its applications in various fields. Also we have given the software and hardware platforms for wireless sensor network. Also we mentioned the possible attacks on the WSN and their countermeasures. Finally we have pointed out that for designing a sensor network one must build a mechanism which is secure from external attackers.

1. INTRODUCTION

Sensor networks are a promising approach for a variety of applications, such as monitoring safety and security of buildings and spaces, measuring traffic flows, and tracking environmental pollutants. The continuous miniaturization process of computing devices featuring wireless technologies influences our everyday life. With the popularity of laptops, cell phones, PDAs, GPS devices, RFID, and intelligent electronics in the post-PC era, computing devices have become cheaper, more mobile, more distributed, and more pervasive in daily life. The emergence of wireless sensor networks (WSNs) is essentially the latest trend of Moore's Law toward the miniaturization and ubiquity of computing devices. Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components.

2. WIRELESS NETWORK

Mobile computers, such as notebook computers and personal digital assistants (PDAs), are the fastest-growing segment of the computer industry. Many of the owners of these computers have desktop machines on LANs and WANs back at the office and want to be connected to their home base even when away from home or en route. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless networks.

Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using a transmission system called radio waves. AM radio, FM radio, satellite radio, satellite TV, satellite Internet access and broadcast TV is also, in fact, wireless networks. Wireless technology is very convenient. You do not have to worry about running wires in tight places, or obtaining low-voltage permits. The range of wireless technology can be impressive. While the equipment you use may break (just as wired equipment would) the signals themselves never break. In comparison to wireless eventually getting old or corroded, this is a great advantage. Wireless networks have many uses. A common is the portable office. People on the road want to use their portable electronic equipment to send and receive telephone calls, faxes, and electronic mail, read remote files, login on remote machines, and does this from anywhere on land, sea, or air. Another use is for rescue workers at disaster sites where the telephone system has been destroyed. Computers there can send messages, keep records, and so on.
Wireless Local Area Network (LAN), Wireless Metropolitan Area Networks (MAN), Wireless Wide Area Network (WAN), Wireless Personal Area Network (PAN) is the four main types of wireless networks.

3. WIRELESS SENSOR NETWORK (WSN)

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling

control of sensor activity. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.
Typically, a sensor node is a tiny device that includes three basic components: a sensing subsystem for data acquisition from the physical surrounding environment, a processing subsystem for local data processing and storage, and a wireless communication subsystem for data transmission. In addition, a power source supplies the energy needed by the device to perform the programmed task. This power source often consists of a battery with a limited energy budget. There are different Sensors such as pressure, accelerometer, camera, thermal, microphone, etc. They monitor conditions at different locations, such as temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, the current characteristics such as speed, direction and size of an object. Normally a sensor node combines the abilities to compute, communicate and sense.

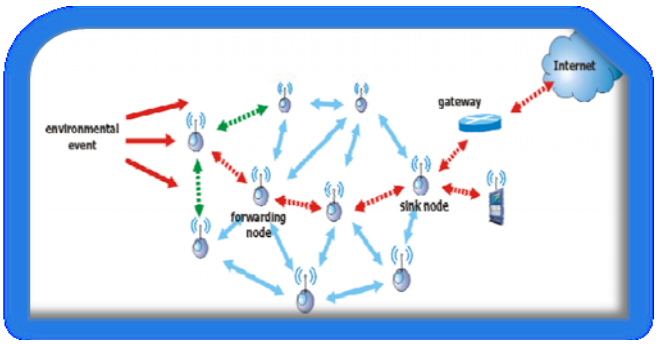

Fig. 1 Wireless Sensor Network

3.1 Sensor node architecture:

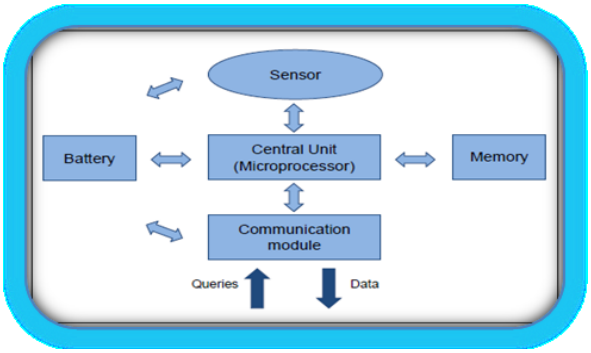

Fig.2 Sensor Node Architecture

A sensor node typically consists of five main parts: one or more sensors gather data from the environment. The central unit in the form of a microprocessor manages the tasks. A transceiver (included in the communication module in Figure 2) communicates with the environment and a memory is used to store temporary data or data generated during processing. The battery supplies all parts with energy (see Figure 2). To assure a sufficiently long network lifetime, energy efficiency in all parts of the network is crucial. Due to this need, data processing tasks are often spread over the network, *i.e.* nodes co-operate in transmitting data to the sinks. Although most sensors have a traditional battery there is some early stage research on the production of sensors without batteries, using similar technologies to passive RFID chips without batteries.

The development of sensor nodes is influenced by

- increasing device complexity on microchips,
- high performance, wireless networking technologies,
- a combination of digital signal processing and sensor data acquisition,
- advances in the development of microelectromechanical systems (MEMS), and
- Availability of high performance development tools.

3.2 Characteristics of WSN:

The main characteristics of a WSN include

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes

- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Unattended operation
- Power consumption

3.3 Fields of applications of wireless sensor network:

1. Security and Surveillance:
Now a day's wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. The sensor devices or nodes should provide services like Battlefield surveillance, Reconnaissance of opposing forces, Targeting, Battle damage assessment, Nuclear, biological and chemical attack detection reconnaissance.
2. Environmental Monitoring:
The term Environmental Sensor Networks has evolved to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests, etc. Some other major areas are listed below.
Air pollution monitoring
Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens.
Forest fires detection
A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fires in the trees or vegetation.; due to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.
Landslide detection
A landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. And through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.
3. Health Applications:
Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital.
Some other similar applications include Glucose level monitors, Organ monitors, Cancer detectors and General health monitors. The idea of embedding wireless biomedical sensors inside human body is promising, although many additional challenges exist: the system must be ultra safe and reliable; require minimal maintenance; energy-harnessing from body heat.
4. Energy Control System:
Societal-scale sensor network can greatly improve the efficiency of energy-provision chain, which consists of 3 components, the energy-generation, distribution, and consumption infrastructure.
5. Area monitoring:
Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A civilian example is the geo-fencing of gas or oil pipelines.
6. Agriculture Applications:
Agriculture
Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing. Irrigation automation enables more efficient water use and reduces waste.
Wireless sensor networks are also used to control the temperature and humidity levels inside commercial greenhouses.
7**.** Industrial applications**:**
Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors. 8. Structural monitoring**:**

Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc. enabling engineering practices to monitor assets remotely without the need for costly site visits.

4. TECHNOLOGIES FOR WSN

4.1 Operating systems

Operating systems such as eCos or uC/OS used for sensor networks. TinyOS is perhaps the first operating system specifically designed for wireless sensor networks. LiteOS and Contiki are the other new operating systems used for sensor networks.

4.2 Hardware standards

A WSN measurement node contains several components including the radio, battery, microcontroller, analog circuit, and sensor interface. In battery-powered systems, one must make important trade-offs because higher data rates and more frequent radio use consume more power. Today, battery and power management technologies are constantly evolving due to extensive research.

Often in WSN applications, three years of battery life is a requirement, so many of the WSN systems today are based on ZigBee or IEEE 802.15.4 protocols due to their low-power consumption. The IEEE 802.15.4 protocol defines the Physical and Medium Access Control layers in the networking model, providing communication in the 868 to 915 MHz and 2.4 GHz ISM bands, and data rates up to 250 kb/s. ZigBee builds on the 802.15.4 layers to provide security, reliability through mesh networking topologies, and interoperability with other devices and standards. ZigBee also allows user-defined application objects, or profiles, which provide customization and flexibility within the protocol.

The base stations are one or more components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, long-range Wi-Fi links etc. Many base stations are ARM-based running a form of Embedded Linux.

4.3 Communication Protocols

Wireless sensor networks use layered architecture like wired network architecture. Characteristics and functions of their each layer are given below.

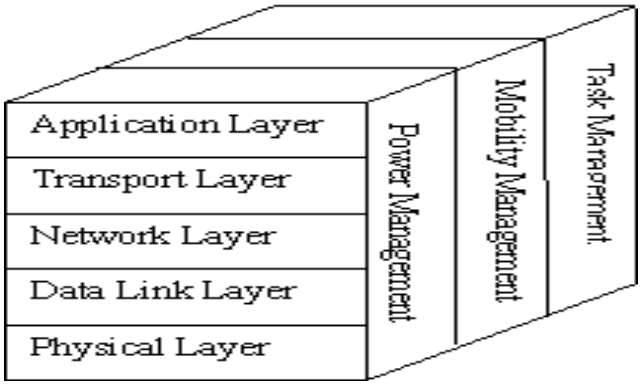

Figure 3. Layered Architecture of WSN

1 Physical Layer

The objective of physical layer is to increase the reliability by reducing path loss effect and shadowing. This layer is responsible for established connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection.

2 Data Link Layer

The objective of Data link layer is to insure interoperability amongst communication between nodes to nodes. This layer is responsible for error detection, multiplexing. Prevention of Collision of packets, repeated transmission etc.

3 Network Layer

The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa. The LEACH and PEGASIS are the protocols which describe the techniques to save the energy consumption (power of sensor) so as to improve the life of sensors. LEACH gives cluster based transmission while PEGASIS is chain protocol. WSN use ID based protocols and data centric protocols for routing mechanism. In WSN, each node in the network acts as a

router (because they use broadcast mechanism), so as to create secure routing protocol. Encryption and decryption techniques are used for secure routing.

4 Transport Layer

The objective of Transport Layer is to establish communication for external networks i.e. sensor network connected to the internet. This is most challenging issue in wireless sensor networks.

5 Application Layer

The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results. SPINS (Security Protocols in sensor Networks) provides data authentication, replay protection, semantic security and low overhead.

5. ATTACKS AND COUNTERMEASURES FOR WSN

Security requirements for WSN mainly include Authentication and Secrecy of the node.

Authentication: Since sensor networks use a shared wireless communication medium, authentication is necessary to enable sensor nodes to detect maliciously injected or spoofed packets. Authentication enables a node to verify the origin of a packet (source authentication) and ensure data integrity, that is, ensure that data is unchanged (data authentication).

Secrecy: Ensuring the secrecy of sensed data is important for protecting data from eavesdroppers. We can use standard encryption functions to achieve secrecy.

The security breaches occur primarily in the form of Interruption (breakdown of communication links), Interception (unauthorized access of WSN), Modification (Change of data by unauthorized access) and fabrication (Addition of false data by unauthorized accesses).

1. Denial of service

This type of attack results into making unavailable the resources to their intended users. As an example node “A” sends request to node “B” for communication and node “B” sends acknowledge to node “A” but “A” keeps on sending request to “B” continuously. As a result “B” is not able to communicate with any other nodes and thus becomes unavailable to all of them. Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization. Most of denial of service attacks may be prevented by powerful authentication and identification mechanisms.

2. Attack of information in transit

In case of wireless sensor networks usually each node reports changes to a cluster head or base station only for data above some threshold. Information in transit may be altered, spoofed, replayed again or vanished. In this type of attack attacker has high processing power and large communication range. This type of attack may be prevented by data aggregation and authentication techniques.

3. Sybil attack

In this attack the attacker gets illegally multiple identities on one node. By this, the attacker mostly affects the routing mechanism. Sybil attacks are generally prevented by validation techniques.

4. Blackhole/ Sinkhole Attack

In this type of attack, attacker places himself in a network with high capability resources (high processing power and high band width) by which it always creates shortest path. As a result, all data passes through attacker’s node.

5. ‘Hello flood’ Attack

This is one of the simplest attacks in wireless sensor networks in which attacker broadcasts HELLO packets with high transmission power to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node. By this attack congestion occurs in the network. This is a specific type of DOS. Blocking techniques are used to prevent Hello Flood attacks.

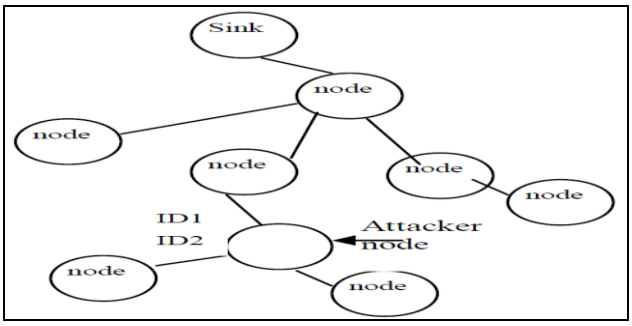

Figure 4: Sybil Attack

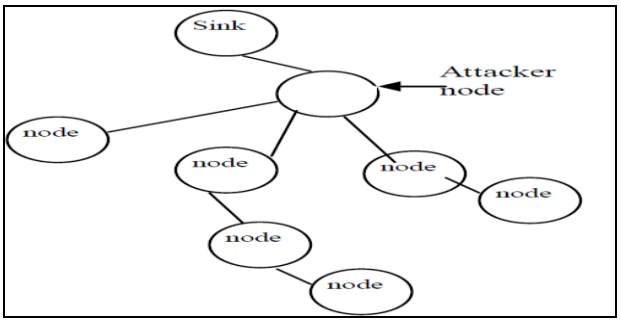

Figure 5: Blackhole/S sinkhole Attack

6. Wormhole Attack

In this type of attack, the attacker uses tunneling mechanism to establish himself between them by confusing the routing protocol. Figure 4 shows mechanism of wormhole attack let "Y" wants to send data by way of broadcasting before sending the data to find path. However the attacker introduces himself as a node "X" and sends acknowledgement to "Y". "Y" sends data to "X" that is received by attacker and attacker sends that data to "X" by tunneling, hiding its own identity. In this case "X" and "Y" are not in a single hop but they think they are in a one hop range. The attacker thus may destroy security by interruption, interception, modification and fabrication.

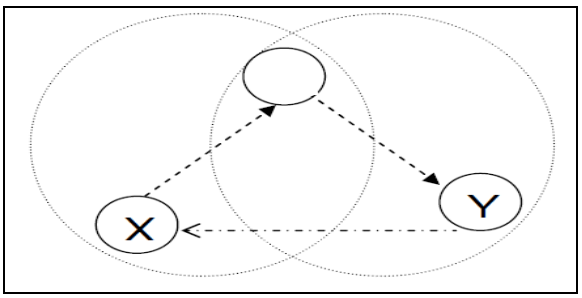

Figure 6: Wormhole Attack

Countermeasures: Standard cryptographic techniques can protect the secrecy and authenticity of communication links from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

Key Establishment — for two sensor nodes to set up a secret and authenticated link, they need to establish a shared secret key.

Broadcast Authentication — in broadcast source authentication possible approach is to use a digital signature, where the source signs each message with a private key and all the receivers verify the message using the public key.

6. CONCLUSION

Sensor nodes are susceptible to physical capture. Similarly, an attacker can easily inject malicious messages into the wireless network. So it is clear that security needs to be taken into account at design time.

Current research on sensor networks is mostly built on a trusted environment. Several exciting research challenges remain before we can trust sensor networks to take over important missions. Security will be important for

most applications for the following reasons. Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored. Such unwanted information leakage often results in privacy breaches of the people in the environment.

7. REFERENCES

1. A. Perrig *et al.*, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks J.*, vol. 8, no. 5, Sept. 2002, pp. 521–34.
2. L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conf. Comp. and Commun. Security*, Nov. 2002, pp. 41–47.
3. E. Amir, S. McCanne, and R. Katz. An active service framework and its application to real-time multimedia transcoding. In *SIGCOMM '98: Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 178–189. ACM Press, 1998.
4. Arch Rock Corporation. Sensor network architecture for the ip enterprise. In Proceedings of the 6th international conference on Information processing in sensor networks, demo session, Cambridge, Massachusetts, USA, 2007.
5. K. K. Chang and D. Gay. Language support for interoperable messaging in sensor networks. In Proceedings of the 2005 workshop on Software and compilers for embedded systems, pages 1–9, Dallas, Texas, 2005. ISBN: 1-59593-207-0
6. J. I. Choi, J. W. Lee, M. Wachs, and P. Levis. Opening the sensornet black box. In Proceedings of the International Workshop on Wireless Sensornet Architecture (WWSNA), Massachusetts, USA, April 2007.
7. "21 ideas for the 21st century," Business Week, pp. 78-167, Aug.39, 1999.
8.http://www.sensornetworks.net.au/applic_health.html 9.http://en.wikipedia.org/wiki/Sensor_Networks
10.Polly Huang, "Sensor Networks Solutions to Real Life Problems" http://cc.ee.ntu.edu.tw/~phuang
11. M. Srivastava, R. Muntz, M. Potkonjak, "Smart kindergarten: sensor-based wireless networks for smart developmental problem-solving environments", Proceedings of the 7th annual international conference on Mobile computing and networking
12. "The Intelligent Home Project", http://dis.cs.umass.edu/research/ihome/