Volume 2, No. 5, April 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

REVIEW ARTICLE

Available Online at www.jgrcs.info

SECURITY THREATS IN WIRELESS SENSOR NETWORKS

Sona Malhotra,

Assistant Prof. CSE Dept. UIET (Kurukshetra University, Kurukshetra)
Rahul
Research Scholar, CSE Dept. UIET (Kurukshetra University, Kurukshetra)
kadian.rahul@gmail.com

Abstract: Wireless sensor networks have been emerged as a challenging and unexplored field for researchers worldwide in the past few years. Wireless sensor networks have a vast range of practical applications. Wireless technology can able to reach virtually every location on the surface of the earth. A wireless sensor network is a network of a large number of independently working small sensing units which communicate wirelessly. It may be used for sensing scalar data events like as pressure, acceleration, temperature, proximity, strain etc. It may also be used to sense multimedia data events and transfer of multimedia data like as audio, video, image etc. In this paper, we have discussed the current situation, hardships in implementation & possible solutions.

Keywords: Wireless sensor network, security attacks, system components.

INTRODUCTION

A wireless sensor network is a network of wirelessly interconnected devices that ubiquitously retrieve data from the environment using sensors embedded in them. Such networks can operate on their own without the need of human interaction. The main benefit of these networks is that these networks can be implemented on a vast area with the least or no human interaction at all. These can be implemented with much ease to the region difficult or virtually impossible for us to access. The individual sensing units may be distributed randomly, uniformly or with varying density according to the application. Also the sensing units being used may be of same or different type as long as they follow the same protocols for sending and receiving the data. ***WSN System Components:*** A general wireless sensor network is composed of a number of sensing units or sensor nodes equipped with the appropriate sensors. A sensor field here is referred as the area in which the sensor nodes are placed. A target node is the sensor node which is the source of the information. Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink. A sink is a sensor node which is deployed for fulfilment of the sole purpose of receiving, processing & storing the data from the other sensor nodes and finally transmitting the data to the base station. This reduces the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. Sinks nodes are also known as data aggregation points. User, which also known as the base station and is a centralised point of control within the network, extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and an access point for a human interface. The base station is either a laptop or a workstation. Operation of WSN involves communication between sensor nodes and base station. Each of the sensor node senses environment within its reach, performs some computation (if required) and reports gathered information to the base station through the sink node. Base station can also be connected with some actuator which will then trigger the alarm for human intervention in case of an event of interest.

Main system components of a wireless sensor network are shown in the fig. here. [1, 4, 7, 8]

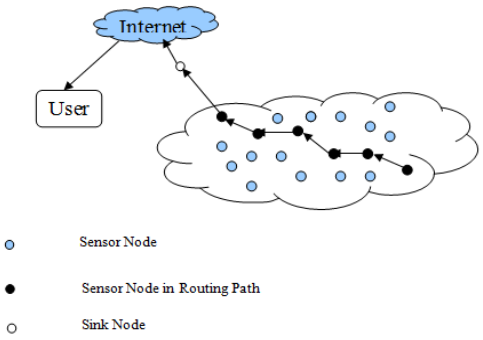
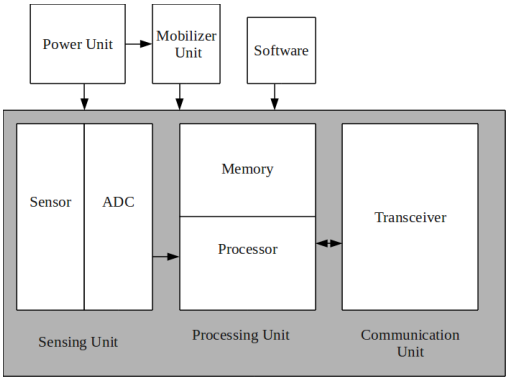


Figure1: General structure of wireless sensor networks

MOTE ARCHITECTURE

A mote is the individual sensor node. Essentially a mote is composed of some basic units, these basic units enables the sensor node to function properly. A sensor node is generally comprised of a Sensing Unit, a Processing Unit, a Communication Unit, a mobilize unit (if required) and a Power Unit along with appropriate software. Here Sensing Unit comprises sensors and ADC (analog to digital converter) while Processing Unit encompasses memory and processor. [5]

Figure 2: Architecture of an individual node



A sensor may be explained as a device that converts one energy-form into another and then results into such a usable energy output that one can easily measure in response to the specific measurable input. This property is referred to as the transduction and such devices are called transducers. A sensor system includes a sensing element and its associated signal processing unit. In this way these are used to measure many physical, chemical or biological quantities, such as temperature, pressure, force, sound light, nuclear radiation, magnetic flux and chemical compositions etc. [6]

Measurements and Measuring Principles for Wireless Sensors

	Measurand	**Transduction Principle**
Physical Properties	Pressure	Piezoresistivity, capacitivity
	Temperature	Thermistor, thermocouple
	Humidity	Resistivity, capacitivity
	Flow	Pressure change, thermistor
	Strain	Piezoresistivity
	Force	Piezoelectricity, piezoresistivity
Kinesis Properties	Position	GPS, contact sensor
	Velocity	Doppler Effect, Hall effect, optoelectronic
	Acceleration	Piezoresistivity, piezoelectricity
	Torque	Piezoresistivity, optoelectronic
Presence	Contact	Contact switch, capacitivity
	Proximity	Seismic Sensing, acoustic, Radio Frequency
	Distance/range	SONAR, RADAR, LIDAR
	Motion	IR, acoustic, seismic (vibration)
Identification	Personal features	Vision
	Personal ID	Fingerprints, retinal scan, voice, heat plume, vision motion analysis

Table1: Measurements and Measuring Principles for Wireless Sensors

PROTOCOL STACK FOR WIRELESS SENSOR NETWORKS

Protocol stack for wireless sensor networks is basically an extension to the Internet protocol stack. For WSN in addition to the layers of the Internet protocol stack three extra layers are also implemented simultaneously. Theses layers are: Task Management, Mobility Management and Power Management. Akyildiz described a Sensor Network Protocol Stack for sensor networks given in the figure. [1]

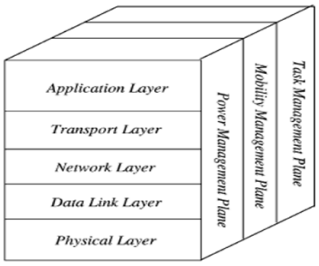


Figure 3: Protocol Stack for WSN

HARDSHIPS IN IMPLEMENTATION OF WIRELESS SENSOR NETWORKS

Coverage Issue: While implementing wireless sensor networks, there may be some regions where coverage of sensor nodes might not be present. We should put efforts in discovering the insufficiently covered regions and once detected we must rearrange sensor nodes in order to eradicate this problem. Power Issue: Another important issue in implementation of wireless sensor networks is power saving. It is well known that the power consumption in wireless communication is quite high and in case of wireless sensor networks it is much more than the power consumed by the sensor node. Therefore the routing protocols for wireless sensor networks should be selected while keeping this in mind. Energy efficient routing protocols should be used always. If there are some nodes which are not being used, then they should be turned off. They can be switched on later in case of wear and tear or any other such condition. Hardware Design Constrains: There is a lot much pressure these days on hardware designers for wireless sensor networks for designing smaller and more efficient components. [3, 5]

SECURITY PROBLEMS

One of many security problems in wireless sensor networks is absence of cryptosystem for wireless sensor networks. The cryptosystems already present are not suitable for application in WSN. Sensor nodes are bound to the constraint on the memory and power consumption. If the encryption- decryption is implemented on the sensor nodes then the power consumption and the memory requirements are highly increased and keeping power & size constraints in mind it is not feasible.

Attacks in Wireless Sensor Networks: [6, 7]

- Denial of Service (DoS): it is resulted by either an unintended failure of a node or by unauthorized access of the sensor node. In this case an intended user is refused of some service.
- Attacks during information flow: these are referred to the attacks which cause the change in the usual information flow.
- Sybil Attack: In this attack a node can pretend to be more than one node using the identities of other legitimate nodes
- Black Hole Attack: In this attack to attract all the traffic in the network some malicious node acts as a black hole / sinkhole node
- Hello Flood: Here to gain access to the wireless sensor network the unauthorized node uses HELLO packet. This step is taken as a measure to get the sensor nodes in confidence.
- Wormhole Attack: In this attack the intruder node keeps record of the packets sent from one node and retransmits them to another node.

.

CONCLUSION

In general, for maximum utility and flexibility across the spectrum of applications, sensor nodes should be as small as possible and must have the capabilities of self-localization and network discovery. In this paper we give the brief description about the Wireless Sensor Network, security problems and power storage capacity of a node. In this paper we also discuss about the various security challenges and their related problems.

REFERENCES

[1] Ian F. Akyiliz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci; A Survey on Sensor Networks in IEEE Communications Magazine, August 2002.

[2] Autonomous sensing and communication in a cubic millimeter http://robotics.eecs.berkeley.edu/~pister/SmartDust/

[3] Yu-Chee Tseng, Chi-Fu Huang "The Coverage Problem in a Wireless Sensor Network" in WSNA' 03, September 19th, 2003

[4] D. Tian and N. D. Georganas "A coverage-preserving node scheduling scheme for large wireless sensor networks. In ACM Int'l Workshop on Wireless Sensor Networks and Applications (WSNA)" 2002.

[5] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon "Hong;Security in Wireless Sensor Networks: Issues and Challenges" in ICACT, 2006.

[6] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses" Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[7] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[8] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defence against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

