www.ijsrnsc.org
Available online at www.ijsrnsc.org
IJSRNSC
Volume-6, Issue-1, Jan 2018
Review Paper
Int. J. Sc. Res. in Network Security and Communication
ISSN: 2321-3256

WSN: Infrastructure and Applications

Poonam M. Mahajan

Dept. of Computer Sci. and IT,Bhusawal Arts, Science and P. O. Nahata Commerce College, India

Abstract - With the popularity of laptops, cell phones, PDAs, GPS devices, RFID, andintelligent electronics in the post-PC era, computing devices have becomecheaper, more mobile, more distributed, and morepervasive in daily life. In recent years an efficient design of a Wireless Sensor Network has become a leading area of research. A Sensor is a device that responds and detects some type of inputfrom both the physical or environmental conditions, such as pressure, heat, light, etc. The output of the sensor is generally an electrical signal that is transmitted to a controller for furtherprocessing.Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components. Thesecomponents are integrated on a single or multiple boards, and packaged ina few cubic inches. The era of WSNs is highly anticipated in the near future. This paper depicts WSN architecture and its applications. The scope of WSN is highlightedthrough the applications of WSN.

Keywords - Ad Hoc Network, Cluster head, Surveillance, WSAN, WSN etc.

I. Introduction

Ad Hoc Networks consists of large number of self-organizing static or mobile nodes that are possibly randomly deployed. It is helpful nearest-neighbour communication. Ad hoc network deploys wireless connections. Links are fragile, possibly asymmetric and connectivity depends on power levels and fading. Interference is high for omnidirectional antennas. Sensor Networks (WSNs) and Sensor-Actuator Networks (WSANs) are thebest examples.

A Wireless Sensor Network (WSN) is a distributed network and it is composed of a largenumber of distributed, self-directed, and tiny, low powered devices called sensor nodes. WSN naturally encompasses a large number of spatially dispersed, diminutive,battery-operated, embedded devices that are networked to supportively collect, process,and put forward data to the users, and it has limited computing and processing capabilities.Nodes are the small computers, which work collectively to form the networks. Nodes areenergy efficient, multi-functional wireless device. The necessities for nodes inindustrial applications are widespread. A group of nodes collects the information from theenvironment to accomplish particular application objectives. They make links with eachother in different configurations to get the maximum performance. Motes communicatewith each other using transceivers. In WSN there may be hundreds or thousands sensor nodes. In comparison with sensor networks, Ad Hocnetworks will have less number of nodes without any infrastructure [4].

Presently wireless network is the most popular services utilized in industrial andcommercial applications, because of its technical advancement in processor,communication, and usage of low power embedded computing devices. Sensor nodes areused to supervise environmental conditions like temperature, pressure, humidity, sound,vibration, position etc. WSN can be used for real time applications, in which sensor nodes are performingdifferent tasks like neighbour node discovery, smart sensing, data storage and processing,data aggregation, target tracking, control and monitoring, node localization, synchronization and efficient routing between nodes and base station.

II. Components of WSN

WSN system composed of sensor node, rely node, actor node, cluster head,gateway and base station.

Sensor Node: This node executes data processing, gathers data and communicates with additional associated nodes in the network. A distinctive sensor node capability is about 4-8 MHz, having 4 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency.

Relay node: It is a middle node used to communicate with the adjacent node. It is usedto improve the network reliability. A rely node is a special type of field device that doesnot have process sensor or control equipment and as such does not interface with theprocess itself. A distinctive rely node processor speed is about 8 MHz, having 8 KB ofRAM, 128 KB flash and preferably 916 MHz of radio frequency.

Actor node: It is a high end node used to perform and construct a decision dependingupon the application requirements. Typically these nodes are resource rich devices whichare outfitted with high quality processing capabilities, greater transmission powers andgreater battery life. A distinctive actor node processor capability is about 8 MHz, having16 KB of RAM, 128 KB flash and preferably 916 MHz of radio frequency.

Cluster head: It is a high bandwidth sensing node used to perform data fusion and dataaggregation functions in WSN. Based on the system requirements and applications, therewill be more than one cluster head inside the cluster. A distinctive cluster head processoris about 4-8 MHz, having 512 KB of RAM, 4 MB flash and preferably 2.4 GHz of radio frequency. This node assumed to be highly reliable, secure and is trusted by all thenodes in the sensor network.

Gateway: Gateway is a periphery between sensor networks and outside networks. Gateway node is most powerful interms of program and data memory, the processor used, transceiver range and thepossibility of expansion through external memory as compared with the sensor node and cluster head. Anindividual gateway processor speedis about 16 MHz, having 512 KB of RAM, 32 MB flash and preferably 2.4 GHz of radiofrequency[1].

Base station: It is an peculiar type of nodes having high computational energy and processing capability. Smart functionality of sensor nodes in a WSN includes effortlessness installation,fault indication, energy level diagnosis, highly reliability, easy coordination with othernodes in the network, control protocols and simple network interfaces with other smartdevices.

The following figure shows the components of sensor nodes.

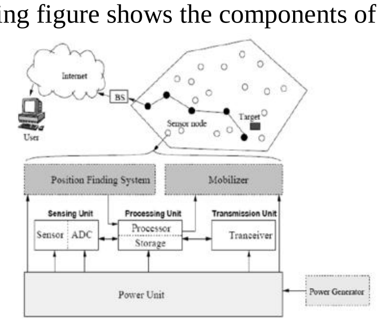

Figure1. Components of sensor node

III. WORKING MECHANISM

The sensor nodes are usually distributed in a sensor field as shown in Fig. 1. Each of these distributed sensor nodes has the capabilities to gather data and transmit data back to the sink and the end users. Data are transmitted back to the end user by a multi-hop infrastructure-lessarchitecture through the sink as shown in Fig. 1. The sink may communicate with the taskmanager node through Internet or Satellite.

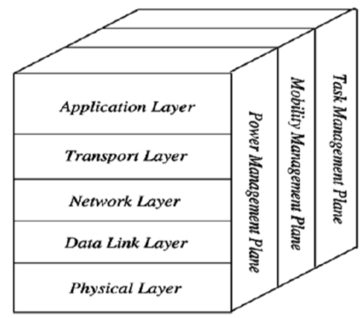

Figure 2. Wireless Sensor Network protocol stack

The sink and the sensor nodes use the protocol stack, given in Fig. 2. This protocol stack integrates power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium and promotes cooperative efforts of sensor nodes. The protocol stack comprises the application layer, transport layer, network layer, data link layer, physical layer, power management plane, mobility management plane, and task management plane. Different types of application software can be built and used on the application layer depending on the sensing tasks. This layer makes hardware and software of the lowest layer translucent to the end-user [2]. The transport layer helps to maintain the flow of data if the sensor networks application requires it. The network layer looks after routing the data supplied by the transport layer, specific multi-hop wireless routing protocols between sensor nodes and sink. The data link layer is responsible for multiplexing of data streams, frame detection, Media Access Control (MAC) and error control. The physical layer is responsible for the needs of a simple but vigorous modulation, frequency selection, data encryption, transmission and receiving techniques.

In addition, the power, mobility, and task management planes supervise the power,movement, and task distribution among the sensor nodes. These planes assist the sensor nodes coordinate the sensing task and lower the overall energy consumption.

IV. SECURITY ISSUES

Sensor networks pretense exclusive challenges, so conventional security techniques usedin traditional networks cannot be applied directly for WSN. The sensor devices areinadequate in their energy, computation, and communication capabilities. When sensornetworks are deployed in a hostile environment, security becomes extremely important,as they are prone to different types of malicious attacks. For example, an opponent caneasily listen to the traffic, impersonate one of the network nodes, or deliberately providedeceptive information to other nodes. WSN works together closely with their corporalenvironments, posing new security troubles. As a result, existing securitymechanisms are insufficient, and novel ideas are needed.

- Sensor nodes are randomly organized in an open and unattended environment, sosecurity is vital for such networks
- WSN uses wireless communication, which is mostly easy to eavesdrop on.
- An attacker can easily inject malevolent node in the network.
- WSN covers a large number of nodes in the network. Implementing security in allthe levels is important and also too complex.
- Sensor nodes are resource constraints in terms of memory, energy, transmissionrange, processing power. Hence asymmetric cryptography is too expensive andsymmetric cryptography is used as alternatives.
- Cost of implementing damage resistant software is very high.

WSN's general security objectivesare confidentiality, integrity, authentication,availability, survivability, efficiency, freshness and scalability [8]. WSN is vulnerable to many attacks because of its transmission nature, resourcerestriction on sensor nodes and deployment in uncontrolled environments. To ensure thesecurity services in WSN many crypto mechanisms like symmetric and asymmetricmethods are proposed. To achieve security in wireless sensor networks, it is important tobe able to encrypt and authenticate messages sent between sensor nodes.

V. APPLICATIONS

The use of WSN paradigm has elicited extensive researchon many aspects of it. The applicability of sensor networks has long beendiscussed with prominence on potential applications that can be realized usingWSNs. Following are some of the applications of WSN.

Military or Border Surveillance Applications

WSNs are becoming an essential part of military command, control, communicationand intelligence systems. The need of rapid use and self-organizationcharacteristics of sensor networks make them a very promisingsensing technique for military applications. Since sensor networks are basedon the dense utilization of disposable and low-cost sensor nodes, whichmakes the sensor network concept a better approach for battlefields. Sensorscan be deployed in a battle field to monitor the presence of forces andvehicles, and track their movements, enabling close inspection of opposingforces.

Environmental Applications

The self-sufficientsynchronization capabilities of WSNs are utilized in therealization of a wide variety of environmental applications. Some environmentalapplications of WSNs comprise tracking the movements of birds, smallanimals, and insects; monitoring environmental conditions that affect cropsand livestock; temperature, humidity and lighting in office buildings; irrigation;large-scale earth monitoring and planetary exploration. These supervisingmodules could even be combined with actuator modules which cancontrol, for example, the amount of fertilizer in the soil, or the amount ofcooling or heating in a building, based on distributed sensor measurements.

Health Care Applications

Wireless sensor networks can be used to observe and follow elders andpatients for health care purposes, which can notably relieve the rigorousshortage of health care human resourcesand reduce the health care overheads in the current health care systems. For example sensors can be installed ina patient's home to keep an eye on the behaviors of the patient. It can alertdoctors when the patient falls and requires instant medical attention. Inaddition, the developments in fixed biomedical devices and smart incorporatedsensors make the usage of sensor networks for biomedical applicationspossible.

Home Intelligence

Wireless sensor networks can be used to provide more suitable andintellectual living environments for human beings. For example, wireless sensorscan be used to distantly read utility meters in a home like water, gas,electricity and then send the readings to a remote Centre through wirelesscommunication. Moreover, smart sensor nodes and actuators can be hidden in appliances such as vacuum cleaners, microwave ovens, refrigerators, andDVD players. These sensor nodes inside domestic devices can cooperate witheach other and with the external network via the Internet or satellite. Theypermit end-users to more easily manage home devicesbothlocally and remotely.Accordingly, WSNs enable the interconnection of various devices atresidential places with well-located control of various applications at home.

Industrial Process Control

In industrial fields such asindustrial sensing and control applications, building automation, and accesscontrol, networks of wired sensors have been used for long ages.

However, the cost associated with the deployment and the maintenanceof wired sensors restricts the applicability of these systems. Whilesensor-based systems acquire high deployment costs, manual systems havelimited accuracy and require human resource. Instead, WSNs are a hopefulalternative solution for these systems due to their ease of deployment, highgranularity, and high accuracy provided through battery-powered wirelesscommunication units. Some of the commercial applications are examiningmaterial fatigue; monitoring product quality; building smart officespaces; environmental control of office buildings; robot control and guidancein automatic manufacturing environments; monitoring disaster areas; smartstructures with embedded sensor nodes.

Agriculture

Using wireless sensor networks within the agricultural industry is gradually morecommon; using awireless network frees the farmer from the preservationof wiring in a difficult environment.Gravity feed water systems can beobserved using pressure transmitters to monitor water tank levels, pumpscan be controlled using wireless I/O devices and water use can be measuredand wirelessly transmitted back to a central control center for billing. Irrigationmechanization enables more efficient water use and reduces waste.

VI. FUTURE AND CHALLENGES

To design a WSN, we require considering different factors such as the flexibility, energy efficiency, fault tolerance, high sensing fidelity, low-cost and rapid deployment, above all the application requirements. We look forward to the wide range of application areas will make sensor networks an integral part of our lives in the future. However, realization of sensor networks need to satisfy several constraints such as scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly tight and specific for sensor networks, new wireless ad hoc networking protocols are required. To meet the requirements, many researchers are engaged in developing the technologies needed for different layers of the sensor networks protocol stack.

Future research on WSN will be directed towards maximizing area throughput in clustered Wireless Sensor Networks designed for temporal or spatial random process estimation, accounting for radio channel, PHY, MAC and NET protocol layers and data aggregation techniques, simulation and experimental verification of lifetime-aware routing, sensing spatial coverage and the enhancement of the desired sensing spatial coverage evaluation methods with practical sensor model. The advances of wireless networking and sensor technology open up an interesting opportunity to manage human activities in a smart home environment. Real-life activities are often more complex than the case studies for both single and multi-user. Investigating such complex cases can be very challenging while we consider both single- and multi-user activities at the same time. Future work will focus on the fundamental problem of recognizing activities of multiple users using a wireless body sensor network. Wireless Sensor Networks hold the promise of delivering a smart communication paradigm which enables setting up an intelligent network capable of handling applications that evolve from user requirements. We believe that in near future, WSN research will put a great impact on our daily life. For example, it will create a system for continual observation of physiological signals while the patients are at their homes. It will lower the cost involved with monitoring patients and increase the efficient exploitation of physiological data and the patients will have access to the highest quality medical care in their own homes. Thus, it will avoid the distress and disruption caused by a lengthy inpatient stay.

VII. CONCLUSION

The purpose of this paper is to discuss few important issues of WSNs, from the application, design and technology points of view. To design a WSN, we require considering different factors such as the flexibility, energy efficiency, fault tolerance, high sensing fidelity, low-cost and rapid deployment, above all the application requirements. We look forward to the wide range of application areas will make sensor networks an integral part of our lives in the future. However, realization of sensor networks need to satisfy several constraints such as scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly tight and specific for sensor networks, new wireless ad hoc networking protocols are required. To meet the requirements, many researchers are engaged in developing the technologies needed for different layers of the sensor networks protocol stack.

REFERNCES

[1] Khichar, R., & Upadhyay, S. S. (2010). Wireless sensor networks and their applications in geomatics: case study on developments in developing countries. *Applied Geomatics*, *2* (2), 43–48.

[2] Manivannan, D., & Neelamegam, P. (2014, Aug 19). Implementation of authenticated key management scheme in wireless sensor networks an embedded approach. India.

[3] Patil, G. M., Kumar, A., & Shaligram, A. D. Performance Comparison of MANET Routing Protocols (OLSR, AODV, DSR, GRP and TORA) Considering Different Network Area Size.

[4] Patil, G. M., Kumar, A. H., & Shaligram, A. D. (2016). T-MANET Method for identification of appropriate parameters for best performance to design MANET in particular scenario. *International Journal of Research in Engineering and Applied Sciences*, *6*(5), 96-107.

[5] Patil, G. M., Kumar, A. H., & Shaligram, A. D. Performance Measurement and Analysis of MANET Routing Protocols on nodes Scalability.

[6] Patil, G. M., Kumar, A. H., & Shaligram, A. D. Performance analysis of MANET routing protocols considering mobility models.

[7] Patil, G. M., Kumar, A., & Shaligram, A. D. Performance Analysis and Comparison of MANET Routing Protocols in Selected Traffic Patterns For Scalable Network.

[8] Zia T, Zomaya A (2006) Security issues in wireless sensor networks. In Proceedings of the International Conference on Systems and Networks, Nov 2–4, pp. 40, Tahiti, French Polynesia

[9] Mahajan, P. M. (2017). Mobile Ad Hoc Networks: An Overview. *International Journal of Computer Trends and Technology , 48* (3), 123-127.

[10] Mahajan, P. M. (2017). Hyper Speed Signalling: The Next Step To Prevent Cyber Attacks. *International Journal of Computer Science and Mobile Computing, 6* (7), 220-226.