International Journal of Mathematical Archive-2(11), 2011, Page: 2201-2204
IJMA Available online through www.ijma.info ISSN 2229 – 5046

WIRELESS SENSOR NETWORK: ISSUES & CHALLENGES

Satvika Khanna[1], Ms. Priyanka Singh[2] and *Akhil Kaushik[3]

Asstt. Prof. IT Department (1), Asstt. Prof. Electronics Department (2), Asstt. Prof. CSE Department (3)
T.I.T&S College, Bhiwani, Haryana, India-127021

E-mail: [1]satvika16@yahoo.com,' [2]singhpriyanka17@gmail.com, [3]akhil.kaushik@yahoo.com

(Received on: 21-10-11; Accepted on: 07-11-11)

ABSTRACT

Wireless sensor networks (WSNs) are a new and emerging type of sensor networks that contain sensor nodes equipped with a radio transceiver, other wireless communications devices like a small microcontroller and an energy source, usually a battery. Wireless sensor network is a wireless ad-hoc network that consists of spatially distributed devices that use sensors to monitor physical or environmental conditions. WSNs merge a wide range of information technology that spans computer hardware, systems software, networking and programming methodologies. WSNs make it possible to perceive what takes place in the physical world in ways not previously possible. In addition to offering the potential to advance many scientific pursuits, they also provide a vehicle for enhancing larger forms of productivity, such as manufacturing, agriculture, construction, and transportation. In this paper, we investigate various issues, applications and challenges in the field of wireless sensor network. We also investigate some of the new technology's potential and describe typical characteristics of wireless multimedia sensor networks (WMSNs). These networks have the potential to enable a large class of applications, ranging from assisting elderly in public spaces to border protection, that benefit from the use of numerous sensor nodes that deliver multimedia content. Then, we introduce the primary challenges in the state-of the-art in wireless sensor networks. Finally, we discuss the existing solutions and possible future research trends.

***Keywords**— Sensor nodes, Wireless Sensor Network (WSN), Wireless Multimedia Sensor Network (WMSN).*

I. INTRODUCTION:

Since the development and advancement of wireless network, it has gained an extra edge over wired networks. The wireless networks are significant because of their abilities to provide services like voice/ video transmission or Internet access at places without cabled networking infrastructure or while being on the move[8]. Wireless technologies have also been identified as a very attractive option for industrial and factory automation, distributed control systems, automotive systems and other kinds of networked embedded systems with mobility, reduced cabling and installation costs, reduced danger of breaking cables, and less hassle with connectors being important benefits[9]. An important characteristic in these application areas is that (wireless) data communications must satisfy tight real-time and reliability requirements *at the same time*, otherwise loss of time and money or even physical damage can result. To achieve this goal, on the one hand certain functionalities that are specific for wireless communications (like mobility management, quick handovers) must be considered, and on the other hand the unfriendly error properties of the wireless channel significantly challenge real-time and reliability. Despite all pros and cons for wireless, it is still predicted as the future of the communication.

Wireless is now widely used in all sort of applications. One area of wireless applications that is currently receiving enormous attention these days due to its unlimited potential is Wireless sensor network (WSN). WSN is purpose-based application-specific wireless network which ensure large scale real time data processing in complex environment. WSN is application specific and are specially designed to serve in emergency environments such as battle field, flood alarming, habitat monitoring, health care etc. Sensor nodes are generally small in size having little memory and computation power, and are densely deployed in the coverage area to achieve accurate results and figures. Wireless sensor network is a wireless ad-hoc network that consists of spatially distributed devices that use networked sensors (nodes) to monitor physical or environmental conditions. A sensor network node's hardware consists of a microprocessor, data storage, sensors, analog-to-digital converters (ADCs), a data transceiver, controllers that tie the pieces together, and an energy source [1].

***Corresponding author:** *Akhil Kaushik[3]*,* ***E-mail:** *akhil.kaushik@yahoo.com*

A wireless sensor network consists of hundreds or thousands of low cost nodes which could either have a fixed location or randomly deployed to monitor the environment. Due to their small size, they have a number of limitations that need to be carefully handled. Sensors usually communicate with each other using a multi hop approach. The flowing of data ends at special nodes called base stations (sometimes they are also referred to as sinks). A base station links the sensor network to another network (like a gateway) to disseminate the data sensed for further processing. Base stations have enhanced capabilities over simple sensor nodes since they must do complex data processing; this justifies the fact that bases stations have workstation/ laptop class processors, and of course enough memory, energy, storage and computational power to perform their tasks well[1][6]. Usually, the communication between base stations is initiated over high bandwidth links. The overall architecture of a sensor node consists of the sensor node processing subsystem, the sensor subsystem and the communication subsystem.

This paper is organized in different sections. Section II describes the connectivity in the WSN. Section III focuses on the security issue. Section IV describes the various applications in the field of WSN. Section V provides conclusion of the paper.

II.CONNECTIVITY:

A major issue in WSNs is the connectivity among the sensor nodes inside WSN. In WSNs, each node has a radio that provides a set of communication links to nearby nodes. By exchanging information, nodes can discover their neighbors and perform a distributed algorithm to determine how to route data according to the application's needs. The networking capability of WSNs is built up in the layers. The lowest layer controls the physical radio device, where radio is a broadcast medium. When one node transmits, a collection of others can receive the signal unless it is garbled by other transmissions at the same time. To avoid congestion for the radio channel, the link layer listens on the channel and transmits only when the channel is clear. It transmits a series of bits that form a packet encoded in the radio signal. When transmission is not taking place, nodes sample the channel and scan for a special symbol at the start of a packet that also lets the receiver align itself with the sender's time. The packet layer manages buffers, schedules packets onto the radio, detects or even corrects errors, handles packet losses, and sends packets to system or application components[4]. WSN emerges as a promising technology for various applications. Networked sensor nodes provide very high redundancy because multiple nodes close to each other increase fault tolerance. Sensor nodes collaborate and combine their data to increase the accuracy of sensed data. Sensor nodes not only perform the sensing functionality, but also provide the forwarding service. Few applications of WSN are traffic controlling, habitat monitoring, flood informing, and health care.

III. SECURITY:

The chief issue to be handled in implementation of any application is security. Security of any application will be responsible for success or failure of any application. With the widespread use of wireless in telecommunication industry, the security attacks have also potentially grown during past few years. Thus security has become an emerging concern in wireless sensor networks. Three common security requirements for any wireless networks are confidentiality, data integrity and service availability[5]. Confidentiality deals with end-users traffic and it ensure that the traffic is not listened or viewed by any entity except the intended recipient. Confidentiality is protected by using strong authentication and encryption mechanisms. Data integrity ensures that the packets are received by the receiver in the same format and sequence as sent by the sender. Here the purpose is to keep the attackers away from packets modifications, alteration, disruption and absorption. Availability is the feature which makes sure that the network and network resources are always available to end-users without any delay or interference.

Three major types of security threats have been observed in wireless networks especially multi-hop wireless networks such as WSN are passive, active and Denial-of-Service (DoS) security threats. Passive attacks compromise the confidentiality by stealing information over the wireless medium using tools like sniffers[2]. Passive attacks are very difficult to detect as they are silent in nature and do not harm the network. Active attacks compromise the data integrity by modifying, tempering and altering the packets. There are no particular routers (gateways) that are involved in such attacks. This kind of attack is actually dynamic in nature. Another daunting threat to WSNs is Denial-of-Service (DoS) attack which basically affects the availability of the network to the users. Here, a hacker or attacker sends huge number of packets to a server, hence slowing down its processing capability and eventually crashing it down[3][7]. This attack can be handled by using "Source-quench" property in IP packet header to slow down such attack in WSNs. Other type of attacks is handled by letting all the nodes communicate with each other having router's capabilities for relaying data for each other. Few of sensor nodes may perform the gateways functionalities and all the nodes send the collected data towards the sink through the gateways. Sink is a repository, which keeps all the collected data and figures to scientifically predict the outcomes. Moreover, most of the security means employed in wired networks are also applicable to the WSNs. For example cryptography (any good encryption algorithm) mechanism is very handy for achieving data integrity while data transfer. Hence, it can be concluded that WSNs are well capable of handling any kind of security problems possible.

IV. APPLICATIONS:

WSN is a new kind of scope that can be applied to a wide range of uses. These can be classified into monitoring space, monitoring things, and monitoring the interactions of things with each other and the encompassing space. The first category includes environmental and habitat monitoring, precision agriculture, indoor climate control, surveillance, treaty verification, and intelligent alarms. The second includes structural monitoring, eco-physiology, condition-based equipment maintenance, medical diagnostics, and urban terrain mapping[6]. The most dramatic applications involve monitoring complex interactions, including wildlife habitats, disaster management, emergency response, ubiquitous computing environments, asset tracking, healthcare, and manufacturing process flow.

Monitoring objects presents different challenges and opportunities. Many applications can be viewed as a form of condition-based maintenance. A physical structure such as a machine, motor, airplane wing, bridge, or building has typical modes of vibration, acoustic emissions, and response to stimuli. Variations in these behaviours indicate wear, fatigue, or other mechanical changes[5]. For example, a bearing often will squeak and shudder before it seizes up. In addition to the sophisticated instrumentation of the actual wafer processing, a modern semiconductor fabrication plant can have several thousand vibration sensors attached to various pieces of routine machinery. A team of electricians tours the plant with a computing device that attaches to a sensor and logs a sample for a short period. The team then carries these logs back to a central computer, which analyzes them for signs of wear and maybe months elapse between visits to a particular machine[1]. This scenario applies to a wide range of manufacturing and power generation plants.

WSN radios consume about 20 milliwatts, and their range typically is measured in tens of meters. For small devices to cover long distances, the network must route the information hop by hop through nodes, much as routers move information across the Internet. Even so, communication remains one of the most energy-consuming operations, with each bit costing as much energy as about 1,000 instructions. Thus WSNs process data within the network wherever possible.

Multimedia surveillance sensor networks are widely used now-a-days. These are the video-based wireless sensor networks are composed of interconnected, battery-powered miniature video cameras, each video and audio sensor camera packaged with a low-power wireless transceiver that is capable of processing and transmitting sensing video signals. This integration of video technology and sensor networks constitutes the fundamental infrastructure for new generations of multimedia surveillance systems

Wireless multimedia sensor networks (WMSNs) are a new and emerging type of sensor networks that contains sensor nodes equipped with cameras, microphones, and other sensors producing multimedia content; hence, quantified multimedia management is required. Multimedia management faces new challenges in WSNs concerned with provision of scalable quality of service (QoS) through the management of metrics, such as coverage, exposure, energy consumption and application specific metrics (e.g., for target detection, possible metrics are miss detection and false detection ratios)[11]. Due to the ad hoc nature of WSNs – which might be deployed in hostile environments with fairly unpredictable conditions — multimedia management must be scalable, self-configurable and adaptive to handle such challenges. A classic approach is the data-centric design of WMSNs, which aims for the integration of application level and network-level operations to provide power-efficient solutions[4][10]. These networks have the potential to enable a large class of applications.

VII. CONCLUSION AND FUTURE WORK:

WSN will likely evolve into a much less distinct and visible form. Instead of being housed in many small devices, these elements will likely become part of the manufacturing process for various materials and objects. These sensors will tend to operate within the ambient energy sources of their intended environment and be placed at key junctures where analysis is most critical. As this vision evolves, so will the need for fundamentally new information technology architectures, from programming languages to signal-processing algorithms. We have presented generalized addresses key issues that arise when dealing with a wireless sensor network device. WSNs appear to represent a new class. They follow the trends of size, number and cost, but have a markedly different function. Rather than being devoted to personal productivity tasks, WSNs make it possible to perceive what takes place in the physical world in ways not previously possible. In addition to offering the potential to advance many scientific pursuits, they also provide a vehicle for enhancing larger forms of productivity, such as manufacturing, agriculture, construction, and transportation.

REFERENCES:

[1] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System Architecture Directions for Networked Sensors," in *ASPLOSIX*, 2000.

[2] Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2-23, 2006.

[3] D.R. Raymond, S.F. Midkiff, "Denial of service in wireless sensor networks: attacks and defenses," IEEE Pervasive Computing, Vol. 7, Issue 1, pp. 74-81, 2008.

[4] R. Venkatesha Prasad, P. Pawtczak, J. A. Hoffmeyer, and H. S. Berger, "Cognitive functionality in next generation wireless networks: Standardization efforts," IEEE Communication Magazine, Vol. 46, Issue 4, pp. 72-78, April 2008.

[5] J. Carle and D. Simplot-Ryl, "Energy-efficient area monitoring for sensor networks," IEEE Computer, Vol. 37, No. 2, pp. 40-46, February 2004.

[6] David Culler, Deborah Estrin,Mani Srivastava' " Overview of sensor networks," IEEE Computer Sopciety, August 2004.

[7] S. Khan, K-k. Loo, T. Naeem, M.A. Khan, "Denial of service attacks and challenges in broadband wireless network," International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6, July 2008.

[8] J. Polastre, R. Szewczyk, and D. Culler, "Telos: Enabling Ultra-Low Power Wireless Research," in *ACM/IEEE IPSN/SPOTS*, 2005.

[9] Zhao, J., Govindan, R., & Estrin, D, Residual energy scans for monitoring wireless sensor networks. In *IEEE Wireless Communications and Networking Conference* (WCNC'02),
Orlando, FL, USA (pp. 356 – 362), 2002.

[10] Gurses, E., & Akan, O.B., Multimedia communication in wireless sensor networks. *Annalsof Telecommunications*, 60(7–8), 799–827, 2005.

[11] Hu, F., & Kumar, S., Multimedia query with QoS considerations for wireless sensor networks in telemedicine. In *Proceedings of the International Conference on Internet Multimedia Management Systems*, Orlando, FL, 2003.

****