IOSR Journal of Electronics and Communication Engineering (IOSRJECE)
ISSN : 2278-2834 Volume 2, Issue 4 (Sep.-Oct. 2012), PP 01-04
www.iosrjournals.org

Wireless Sensor Network: An Emerging Technology

Monjur Ahmed
Department of Computing and Information Systems
Daffodil Institute of Information Technology, Dhaka Bangladesh.

***Abstract**: Wireless sensor network is a special kind of network that differs from the conventional communication networks in terms of architecture and deployment. Dynamic in nature, the wireless sensor networks have added a new dimension not only to the further exploration in a hard-to-reach environment, but also to the complexity of network management. Wireless sensor networks are emerging very rapidly and have already demanded keen interests from researchers. As a relatively new concept in the world of communication, a number of aspects are being explored by the researchers including routing and security features of the wireless sensor networks. Like any wireless network, power consumption has always been a critical issue for wireless sensor networks. This is also due to the environmental constraint in which the wireless sensor networks are normally deployed. This paper provides an overview of this emerging technology by addressing its architecture, deployment and key issues e. g. energy-efficiency, routing, reliability and security*
***Key words:** wireless sensor network, reliability, routing, security, sensor*

I. Introduction

Wireless sensor networks (WSNs) are special kind of ad-hoc wireless network that has caught attention from the researchers over the last couple of years. WSNs are an emerging technology that is being used to collect information for various environmental phenomena. WSNs are dynamic and ad-hoc in nature, comprising of a number of wireless sensor nodes [1], [2]. WSNs are being used in a variety of fields. It has a number of diversified application domains e. g. home, office, automation and control, transportation, logistics, healthcare, environmental monitoring, security and surveillance, asset tracking and monitoring, process monitoring, vehicle monitoring and detection [3], [10]. Like any other wireless communication technology, WSNs also have concerns about energy-efficiency, security, reliability and scalability [1], [2], [4].

II. Basic Wsn Architecture

A WSN is essentially a networked arrangement of wireless sensor nodes. These nodes can communicate among themselves by means of wireless. The nodes are equipped with different types of sensors depending on the application and hence the name wireless sensor network. The sensor nodes sense data from environment by means of sensors which they process and forward to another sensor node which in turn forwards the information to another node so that it can eventually reach to the gateway node. The gateway node is a wireless sensor node that interfaces all other nodes of a WSN to a server computer [4], [5], [10]. The server stores the sent information for further processing. As all the nodes in a WSN acts as routers apart from their respective sensing, processing and transmission tasks; it is very crucial for the sensor nodes of a WSN to work in a co-operative and collaborative manner [5]. The server can have the capability to access or control any specific sensor nodes for network management or any other purpose.

A typical architecture of any wireless sensor network looks like the following:

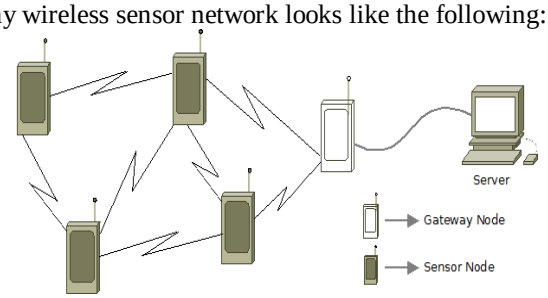

Figure 1: Wireless Sensor Network architecture

The gateway node can have wired or wireless connectivity to the server which is determined by the environment where the network is deployed. A WSN may consists of as low as few sensor nodes to as large as several thousand sensor nodes.

The wireless sensor nodes of a WSN have three major parts – radio, microcontroller and sensor. The radio is for wireless transmission, microcontroller is the processing unit for the node and sensor is the device to

acquire information from the environment. The nodes need to be tiny and cheap to ensure deployment and financial feasibility of the WSNs. A sensor node can be as tiny as a coin. A tiny WSN node combines the power of sensing, processing, routing and transmitting of information [6], [10].

III. Wsn Deployment

The beauty of WSNs lies in their capability of being deployed in remote environment where human-being cannot reach or at least cannot establish long term presence for monitoring or research purpose [7]. A WSN can be deployed in desert, underwater, in a battle field or in any other hard-to-reach environment. WSNs can be used for agricultural purpose, where automatic monitoring can be embedded for precision agriculture. Sensors can detect soil moisture, light level and temperature from different points of an agricultural field [8], [9]. These data can be acquired and analyzed for precision agriculture. The chemical plants or other industrial plants can be automatically monitored for incidents to raise the alarm automatically [10], [11], [15]. Underwater deployment of WSNs can help monitoring various phenomena related to underwater life, detecting unwanted event e.g. rise of a certain element in water that is harmful, underwater surveillance and so on [12], [13]. WSNs have already proven their applicability in healthcare where seamless monitoring of the patients has become possible [3], [10], [14], [15]. For smart home and office, WSNs have their own appeal [15]. One of the supreme applications of WSNs is in security and surveillance where monitoring and collecting information about any violation of rules can be predicted, monitored and captured which subsequently promise a safer community [15]. In near future, WSNs will contribute in almost every aspect of human life.

The deployment of WSNs is more cost-effective compared to their wired counterpart networks where a substantial investment needs to be in place for planning and developing a wired infrastructure and for laying the wires. Drastically reduced installation cost is one of the driving factors for WSNs to become popular over the years [4], [9]. An ideal WSN is the one which is smart, software programmable, reliable over long term, cheap, easy to install, fast in data acquisition and demands almost no real maintenance.

IV. Key Issues in Wsn

A. Energy-efficiency

As WSN nodes may be deployed in remote or hard-to-reach and hazardous environment, they can be left alone for long period with the expectation that they will keep functioning without interruption caused by power failure. Thus energy efficiency has always been a critical factor for WSNs [1], [16], [17]. The sensor nodes of a WSN tend to be tiny for practical reason, thus the capability of containing power is subsequently smaller. Though the sensor nodes can be operated by means of solar power, the provision to use this kind of power source is very limited due to the various environments where the WSNs are deployed. For this reason the sensor nodes are mainly battery powered. The energy from the battery is used for three main purposes. Firstly, the energy is needed for the sensor node to keep itself alive. Secondly, battery power is utilized for the processing of data received or to be sent. The third main functionality that consumes energy is the transmission. Batteries are always limited in power. The power constraint has always been a challenge for WSNs. Maximizing the battery lifetime is an approach to make the sensor networks more energy-efficient. As this is not always achievable to the desired level, some alternative approach has also been adopted. One approach is to minimizing the processing and transmission overheads to a minimum to save battery power [16] – [19]. It has a significant impact towards the energy-efficiency of WSNs as power consumption is directly proportional to the amount of processing or transmission. Another approach is known as 'wake-up-on-demand' where the nodes sleep all the time using minimum power except when they are needed to perform any transmission or processing task [20], [21]. Upon demand, the sleeping nodes wake up and perform their task and then go to standby mode again, saving power to make the WSNs energy-efficient. Towards the accomplishment of the above stated approaches, a number of different algorithms have been proposed [22] – [24].

B. Routing

The meaning of routing has achieved a supreme level of dynamism in the case of WSN where routing means a lot more along with its conventional meaning of justifying and determining the path through which data should travel from source to destination. Routing decision is taken by the routers of any given network for which, they need to work in a collaborative and co-operative manner so that data can reach the destination while ensuring optimum and efficient use of network resources [5], [21]. In the case of WSNs, the concept of routing is somewhat different than any conventional network [1]. Interestingly, all the sensor nodes in a WSN need to perform routing tasks as part of their total functionality. This makes the scenario of a WSN very complex from routing point-of-view. The dynamic nature of WSNs where any sensor node can 'die' at any time or any sensor node can 'wake up' upon demand, or the sensor nodes can be moving all the time – the total network scenario remains constantly changing [20], [21]. The changing scenario needs to be learned by all the routing elements of a network to keep the robustness of routing, WSNs are no exception from this point-of-view. This dynamism contributes to added complexity in WSN routing algorithms [2], [21]. As routing is associated with huge

information processing which in turn has a direct impact on power consumption, an energy-efficient routing algorithm is of supreme interest since the of birth of WSN concept [5]. There are a number of proposals on energy aware MAC protocol and energy efficient routing. Examples of some approaches are physical level design decisions including voltage and modulation scaling [25].

C. Reliability

One of the major considerations for any communication network is the reliability of data transmission. Achieving reliable data transmission in a WSN is difficult due to a number of reasons. The first reason is the limited processing capability of the sensor nodes. Transmission range of the sensor nodes is limited which is another barrier in reliable data transmission. Besides, the sensor nodes are deployed in the close proximity of the ground level. This leads to signal attenuation. Whereas energy-efficiency is one of the goals for WSNs to be achieved, it is a problem for reliable data transmission when 'wake-up-on-demand' approach is adopted [5], [20]. All these characteristics may cause data loss within the context of a WSN.

At the same time, WSNs provide some unique features to combat with reliability issue. Data aggregation is one of the unique features by which reliability can be improved. Data aggregation makes the loss of data acceptable up to a certain level. As the sensor nodes are normally deployed in a dense fashion, a number of possible routing path also improve the reliability. A consequence of data aggregation is smaller data packets which minimizes data loss. Though reliability is an issue for WSNs, dense deployment and data aggregation properties make them loss tolerance [5], [15], [20]. Future research in WSN will essentially involve in developing new algorithms to address reliability problem of the sensor nodes [26]. Addressing reliability is very important for WSNs as it has a direct correlation to scalability, power efficiency, mobility and responsiveness [27].

D. Security

Security is a general concept within the context of communication networks which addresses authentication, integrity and privacy. Security is a logical concern in the case of WSNs too. WSNs are vulnerable to security threats like any other wireless networks [6]. With the characteristics of unguided transmission and broadcast by nature, WSNs are prone to eavesdropping where sniffing to the transmitted data is possible. Various security issues and threats of wireless networks equally apply to WSNs.

One of the common types of security threat for WSNs is the DoS (Denial of Service) attack which arises from malicious acts. The transmitted information in WSNs can be attacked while they are in transit. As WSNs are vulnerable to eavesdropping, the transmitted information can be monitored, interrupted, intercepted or modified [28], [29]. In Sybil attack, a sensor node forges identities from one or more sensor nodes [29], [30]. Another type of attack is known as blackhole attack. This type of attack is associated with a malicious node which acts as the balckhole to attract all the traffic from other sensor nodes [31]. A critical type of attack for WSNs is known as wormhole attack. In wormhole attack, the attacker intercepts and records transmitted information from one place of the network. The intercepted information is then forwarded into another part of the network. This critical attack is distinguished from other types of attacks in the way that no compromising of sensor nodes is required for carrying out a wormhole attack [32].

Security models for WSNs have been proposed for different types of threats. Some proposed models show that the weakness of the WSNs can be tuned in such a way that they will act as the strength against security threats. A holistic approach has been proposed towards the achievement of a more secured WSN. The holistic approach addresses the improvement of WSN performance in a dynamic environment in terms of security, connectivity and longevity [33].

V. Conclusion

WSNs are emerging very rapidly due to their diversified applications. In last few years, notable improvement and successful application of WSNs have been observed. Despite of having issues related to energy-efficiency, security, reliability and scalability, the ongoing research and development has already made the WSN a promising and evolving technology.

References

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal: "Wireless Sensor Network Survey", Computer Networks, 52, pp. 2292-2330. (2008)

[2] Deepak Ganesan, Alberto Cerpa, Wei Ye, YanYu, Jerry Zhao, and Deborah Estrin: "Networking Issues in Wireless Sensor Networks", Journal of parallel and distributed computing, 64, pp. 799-814. (2004)

[3] Moshaddique Al Ameen, Kyung-sup Kwak: "Social Issues in Wireless Sensor Network with Health Perspective", The International Arab Journal of Information Technology, 8, pp. 52-58. (2011)

[4] Tarique Haider, Mariam Yusuf: "A Fuzzy Approach to Energy Optimized Routing for Wireless Sensor Networks", The International Arab Journal of Information Technology, 6, pp. 179-185. (2009)

[5] Shio Kumar Singh, M P Singh, D K Singh: "Routing Protocols in Wireless Sensor Networks – A Survey", International Journal of Computer Science & Engineering Survey (IJCSES), 1, pp. 63-83. (2010)

[6] Hemanta Kumar Kalita, Avijit Kar: "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), 1, pp. 1-10. (2009)

[7] Kavi K. Khedo, Rajiv Perseedoss, Avinash Mungur: "A Wireless Sensor Network Air Pollution Monitoring System", International Journal of Wireless & Mobile Networks (IJWMN), 2, pp. 31-45. (2010)

[8] Kshitij Shinghal, Dr. Arti Noor, Dr. Neelam Srivastava, Dr. Raghuvir Singh: "Intelligent Humidity Sensor for Wireless Sensor Network Agricultural Application", International Journal of Wireless & Mobile Networks (IJWMN), 3, pp. 118-128. (2011)

[9] Ning Wang, Naiqian Zhang, Maohua Wang: "Wireless Sensors in Agriculture and Food Industry – Recent Development and Future Perspective", Computers and Electronics in Agriculture, 50, pp. 1-14. (2006)

[10] Mr. Puneet Garg, Mr. Kuntal Saroha, Mrs. Ruchika Lochab: "Review of Wireless Sensor Networks – Architecture and Applications", International Journal of Computer Science & Management Studies, 11, pp. 34-38. (2011)

[11] K. Nirmal Kumar, V.R. Sarma Dhulipala, R. Prabakaran, P. Ranjith: Future sensors and utilization of sensors in chemical industries with control of environmental hazards, 2nd International Conference on Environmental Science and Development IPCBEE, IACSIT Press, Singapore, 4, pp. 224-228. (2011)

[12] Dario Pompili, Tommaso Melodia, Ian F. Akyildiz: "Deployment Analysis in Underwater Acoustic Wireless Sensor Networks", WUWNet, pp. 48-55. (2006)

[13] K. Ovaliadis, N. Savage, V. Kanakaris: "Energy Efficiency in Underwater Sensor Networks: a Research Review", Journal of Engineering Science and Technology Review, 3, pp. 151-156. (2010)

[14] Pervez Khan, Md. Asdaque Hussain, Kyung Sup Kwak: "Medical Applications of Wireless Body Area Networks", International Journal of Digital Content Technology and its Applications, 3, pp. 185-193. (2009)

[15] Syed Muhammad Khaliq-ur-Rahman Raazi, Sungyoung Lee: "A Survey on Key Management Strategies for Different Applications of Wireless Sensor Networks", Journal of Computing Sciences and Engineering, 4, pp. 23-51. (2010)

[16] Patrick Vincent, Murali Tummala, John McEachen: "A New Method for Distributing Power Usage Across a Sensor Network", Ad Hoc Networks, 6, pp. 1258–1280. (2008)

[17] Kan Baoqiang, Cai Li, Zhu Hongsong & Xu Yongjun: "Accurate Energy Model for WSN Node and its Optimal Design", Journal of Systems Engineering and Electronics, 19, pp. 427–433. (2008)

[18] Luiz H.A. Correia, Daniel F. Macedo, Aldri L. dos Santos, Antonio A.F. Loureiro, Jose´ Marcos S. Nogueira: "Transmission Power Control Techniques for Wireless Sensor Networks", Computer Networks; 51, pp. 4765–4779. (2007)

[19] KAN Baoqiang, CAI Li , XU Yongjun: "Reliable and Energy Efficient Protocol for Wireless Sensor Network", Tsinghua Science and Technology, 12, pp. 95-100. (2007)

[20] Justin Jones, Mohammad Atiquzzaman: "Transport Protocols for Wireless Sensor Networks: State-of-the-Art and Future Directions", International Journal of Distributed Sensor Networks, 3, pp. 119-133. (2007)

[21] Kemal Akkaya, Mohamed Younis: "A Survey on Routing Protocols for Wireless Sensor Networks", Ad Hoc Networks, 3, pp. 325-349. (2005)

[22] F. Akyildiz: "A Survey on Sensor Networks", Computer Journal of IEEE Communications Magazine, 40, pp. 102-114. (2002)

[23] R. Heinzelman: Energy scalable algorithms and protocols for wireless sensor networks, Proceeding of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP'00), Turkey, pp. 773-776. (2000)

[24] A Wang: Energy-scalable protocols for battery operated micro sensor networks, Proceedings of 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, USA, pp. 398-415. (2006)

[25] W. Ye, J. Heidemann, D. Estrin: An energy efficient MAC protocol for wireless sensor networks, Proceedings of IEEE Infocom, USA, pp. 1567-1576. (2002)

[26] Louis A. Petingi: "Introduction of a New Network Reliability Model to Evaluate the Performance of Sensor Networks", International Journal of Mathematical Models and Methods in Applied Sciences, 5, pp. 577-585. (2011)

[27] Vijay Kumar, R. B. Petal, Manpreet Singh, Rohit Vaid: "A Neural Approach for Reliable and Fault Tolerant Wireless Sensor Networks", International Journal of Advanced Computer Science and Applications (IJACSA), 2, pp. 113-118. (2011)

[28] W. J. Blacket, D. M. Gregg, A. K. Castner, E. M. Kyle, R. L. Hom, R. M. Jokerst: Analyzing interaction between distributed denial of service attacks and mitigation technologies, Proceedings in DARPA Information Survivability Conference and Exposition, 1, 22-24 April, 2003, pp. 26-36. (2003)

[29] B. T. Wang, H. Schulzrinne: An IP traceback mechanism for reflective DoS attacks, Canadian Conference on Electrical and Computer Engineering, 2, 2-5 May 2004, pp. 901-904. (2004)

[30] J Douceur: The Sybill attack, 1st International Workshop on Peer-to-Peer Systems. (2002)

[31] B. J. Culpepper, H. C. Tseng: Sinkhole intrusion indicators in DSR MANETs, Proceeding in First International Conference on Broadband Networks, pp. 681-688. (2004)

[32] Y. C. Hu, A. Perrig, D. B. Johnson: Packet leashes: a defense against wormhole attacks in wireless networks, 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE INFOCOM 2003, 3, 30 March – 2 April 2003, pp. 1976-1986. (2003)

[33] S. Avancha: A holistic approach to secure sensor networks, PhD Dissertation, University of Maryland. (2005)