A Review : Wireless Sensor Networks (WSN) and Security Aspects

Ashok Kishtwal
M.tech (CSE) 3rd SEM.
Baddi University of emerging science and technology

Jasvinder Singh
Assistant Prof., CSE
Baddi University of emerging science and technology

Rohika Bhatt
M.tech (CSE) 3rd SEM.
Baddi University of emerging science and technology

Abstract

Wireless sensor network has become one of the dominating technologies which are affecting our daily life. In wireless sensor networks small sensors are spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data, which continuously collects the data from the surroundings and after some processing, sends them to the base station. The computers in the base station, then interprets the data and suggests the desired action. Sensor nodes in WSN have its own operating system that is Tiny-OS. Wireless sensor networks used in different applications in different fields. This review paper works on general description about the sensor nodes and networks with its routing and security issues.

Keywords: *WSN, Sensor Node, Base Station, Tiny-OS.*

1. Introduction

Wireless sensor networks have recently come into prominence because they hold the potential to revolutionize many segments of our economy and life, from environmental monitoring and conservation, to manufacturing and business asset management, to automation in the transportation and health care industries. The design, implementation, and operation of a sensor network requires the confluence of many disciplines, including signal processing, networking and protocols, embedded systems, information management and distributed algorithms. Such networks are often deployed in resource-constrained environments, for instance with battery operated nodes running untethered. These constraints dictate that sensor network problems are best approached in a hostile manner, by jointly considering the physical, networking, and application layers and making major design tradeoffs across the layers.

Wireless sensor networks are typically used in highly dynamic, and hostile environments with no human existence (unlike conventional data networks), and therefore, they must be tolerant to the failure and loss of connectivity of individual nodes. The sensor nodes should be intelligent to recover from failures with minimum human involvement. Networks should support process of autonomous formation of connectivity, addressing, and routing structures. Recent researches on Autonomic Networking can serve as basis for design of Autonomic Wireless Sensor Networks [1].

Wireless sensor networks are composed of hundreds or thousands of small sized sensor nodes that are able to cooperate in detecting physical environments. One of the advantage of wireless sensor network is the ability to operate unattended in harsh environment in which contemporary human-in-the-loop monitoring schemes are risky, inefficient and sometimes infeasible [2], [3].

Sensor networks have emerged as a promising tool for monitoring the physical worlds, utilizing self-organizing networks of battery-powered wireless sensors that can sense, process and communicate [4]. Wireless sensor networks consist of small low power nodes with sensing, Computational and wireless communications capabilities that can be deployed randomly or deterministically in an area from which the users wish to collect data. Typically, wireless sensor networks contain hundreds or thousands of sensor nodes that are generally identical. These sensor nodes have the ability to communicate either among

each other or directly to a base station (BS). The sensor network is highly distributed and the nodes are lightweight. Intuitively, a greater number of sensors will enable sensing over a larger area. As the manufacturing of small, low-cost sensors become increasingly technically and economically feasible, a large number of these sensors can be networked to operate cooperatively unattended for a variety of applications like military applications, disaster management, habitat monitoring, health applications, home applications etc [5].

At present, research on wireless sensor networks has generally assumed that nodes are homogeneous. In reality, homogeneous sensor networks hardly exist, even homogeneous sensors also have different capabilities like different levels of initial energy, depletion rate, etc. This leads to the research on heterogeneous networks where at two or more types of nodes are considered. However, most researchers prevalently assume that nodes are divided into two types with different functionalities, advanced nodes and normal nodes. The powerful nodes have more initial energy and fewer amounts than the normal nodes, and they act as clustering heads as well as relay nodes in heterogeneous networks. Moreover, they all assume the normal nodes have identical length data to transmit to the base station [6].

1.1. Application of WSNs

- Disaster relief operations
- Biodiversity Mapping
- Intelligent Buildings/Bridges
- Precision Agriculture
- Medicine and health care
- Logistics
- Air pollution Monitoring System
- Habitat Monitoring
- Fire and Flood Detection
- Seismic Monitoring
- Civil Structural Health Monitoring
- Monitoring Groundwater Contamination
- Rapid Emergency Response
- Industrial Process Monitoring
- Perimeter Security and Surveillance
- Automated Building Climate Control
- Secure Area Monitoring

2. Wireless Sensor Networks

2.1. Architecture of Wireless Sensor Node

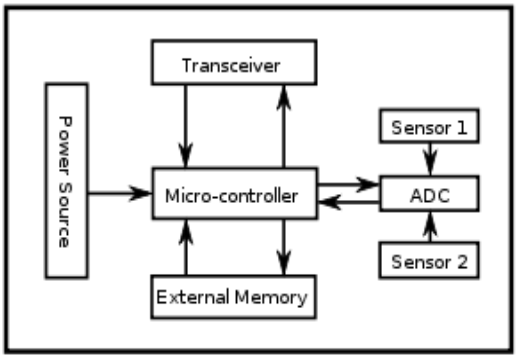

Figure 1. Basic Architecture of Wireless Sensor Node.

A sensor node is made up of four basic components as shown in figure 1:

- A sensing unit
- A processing unit
- A transceiver unit
- A power unit

They may also have application dependant additional components such as location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs).The analog signals produces by the sensors based on the observed phenomenon are converted to digital signals by the ADC, then fed into the processing unit .The processing unit, which is generally associated with a small storage unit manage the procedures that make the sensor node collaborative with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One the most important components of a sensor node are the power unit.

The power supply is the critical constituent of the wireless sensor network because this controls the life and long-term capabilities of the nodes. The most general and practical power source is through the use of small, long-lived batteries.

2.2. Wireless Sensor Network

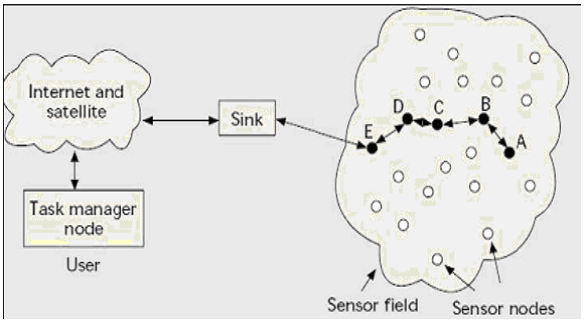

Figure 2. Basic Architecture of Wireless Sensor Network. (Ref [07])

A wireless sensor network (WSN) is a network that is made of hundreds or thousands of sensor nodes which are densely deployed in an unattended environment with the capabilities of sensing, wireless communications and computations (i.e. collecting and disseminating environmental data). These spatially distributed autonomous devices cooperatively monitor physical and environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The basic architecture of Wireless sensor Network is shown in Figure2 [1].

3. Related Work

3.1. Routing Protocols

Low Energy Adaptive Clustering Hierarchy LEACH [8] is the most popular energy efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption. In LEACH, the clustering task is rotated among the nodes, based on duration. Direct communication is used by each CH to forward the data to the Base Station (BS). It is an application specific data dissemination protocol that uses clusters to prolong the life of the WSN. LEACH is based on an aggregation (or fusion) technique that combines or aggregates the original data into a smaller size of data that carry only meaningful information to all individual sensors. LEACH divides the network into several clusters of sensors, which are constructed by using localized coordination and control not only to reduce the amount of data that are transmitted to the sink, but also to make routing and data dissemination more scalable and robust [6]. More clustered protocols have been proposed that are based on LEACH protocol, like PEGASIS [9], TEEN [10], HEED [11] and BCDCP [12] etc, but they all comes under the homogenous condition.

In [2], authors proposed a distributed passive cluster-based multipath routing protocol for wireless sensor networks. The proposed protocol logically divides nodes into clusters and uses hierarchical management strategies to achieve high energy efficiency, low end-to-end delay and high delivery reliability. Passive clustering is used in first round while active clustering is adopted in the other rounds. The new proposed protocol achieves the better performance in energy efficiency and QoS, and it is also suitable for event driven large-scale sensor networks.

Multihop-LEACH is the one of the cluster based routing algorithm. Basic operation of Multihop-LEACH is similar to LEACH protocol. There are two major modifications in Multihop-LEACH protocol with respect to LEACH protocol. Multihoping is applied to both inter cluster and intra cluster communication.

In [4], authors proposed improved Multihop-LEACH routing protocol. The overall conclusion is that improved Multihop-LEACH routing protocol is best choice to move towards a network with less energy consumption as it involve energy minimizing techniques like multihop, clustering and data aggregation.

In [6], authors proposed a cluster based routing protocol based upon the LEACH algorithm, which considers residual energy of sensor nodes to avoid unbalanced energy consumption of the sensor node and to extend the overall network lifetime without performance degradation. To increase the lifetime of network, the proposed algorithm uses a probability function. the proposed algorithm is able to prolong the network lifetime as compared to LEACH.

Cluster-based multipath delivery scheme (CMDS) [13] use an improved ID- based algorithm to organize the network into clusters, which reduces the number of messages that have to be delivered in the network. Cluster based protocol to support reliable and energy efficient data delivery that is completely distributed (CREED) [14] partitions the network into several grids based on the optimum direct transmission range to control the cluster head distribution. Zigbee multipath hierarchical tree routing (Z-MHTR) [15] is a multipath routing protocol. It relies on cluster-tree structure. Z-MHTR enhances the reliability and robustness. Energy-efficient hybrid clustering routing protocol (EEHCRP)[16] integrates the advantages of concentrated clustering and distributed clustering. Multipath routing protocol (MRP) [17] is a multipath routing protocol based on dynamic clustering and ant colony optimization (ACO).

3.2. SECURITY ISSUES IN SENSOR NETWORKS

Sensor nodes have several constraints, involving battery power, recharge ability, sleep patterns, working memory, transmission range, tamper protection, time synchronization and unattended operation. There are several other constraints related to the network as well, such as adhoc networking, limited reconfigurations, data rate and packet size, channel error rate, intermittent connectivity, latency and isolated subgroups. These constraints make it especially challenging to design security protocols for such networks.

In addition to those traditional security issues, we observe that many general-purpose sensor network techniques (particularly the early research) assumed that all nodes are cooperative and trustworthy. This is not the case for most, or much of, real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality [18].

3.2.1. Attack and Attacker

An attack can be an effort to get illegal access to a service, information, or the assay to conciliation integrity, confidentiality, or availability of a system. Attacks are originated by attackers or intruders. WSN Adversary can be:

- Passive: A person or another entity that only monitors the communication channel which threatens the confidentiality of data.
- Active: Effort to add, delete or alter the transmission on the cannel which threatens to confidentiality, authentication and data integrity.
- Insider: Steal key material and run malicious code by compromise some authorized nodes of the network. Outsider: attacker has no particular access to the network.
- Mote-Class Attacker: Has access to the minority nodes with similar capabilities.
- Laptop-Class Attackers: they have access to powerful devices such as laptop which has advantages greater than legal nodes, for instance more capable processor, greater battery power and high power antenna [19].

Here we point out the major attacks in wireless sensor networks.

3.2.2. Denial of Service

Denial of Service (DoS) [20] is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources avail able to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service.

3.2.3. Attacks on Information in transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate [21] packets thus, provide wrong information to the base stations or sinks.

3.2.4. Sybil Attack

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack [22], [23]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [23]. Basically, any peer-to-peer network (especially wireless adhoc networks) is vulnerable to Sybil attack.

3.2.5. Black hole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker

listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations [24],[25].

In [18] the author had described the four main aspects of wireless sensor network security: obstacles, requirements, attacks and defenses.

In[26] authors havee presented a computationally lightweight wireless sensor network security framework which is composed of four components: (1) secure triple-key management scheme, (2) secure routing mechanism, (3) secure localization technique, and (4) malicious node detection mechanism. The secure routing mechanism presented ensures a secure node to base station and vice versa communication. They have presented a triple-key management scheme based on two network pre-deployed keys and one cluster deployed key. Triple keys mitigate the confidentiality and authentication related attacks. Localization mechanism presented addresses location determination issues from security perspectives. Lastly the malicious node detection mechanism protects the network from insiders and outsider adversaries. The presented analysis shows that the proposed framework as a whole addresses the security issues competently without increasing the overheads. In contrast to the computationally extensive security solutions, the framework has great potential for emerging applications. Results presented show the effectiveness of the framework to ensure the total security for wireless sensor networks by reducing the packet transmission time, low latency and less packet overheads.

4. Conclusion

In this paper, we have described the main features of wireless sensor network, network protocols and security aspects of WSN. The main challenges in wireless sensor networks are to develop efficient and energy saving routing algorithm and security protocols. Development of Cost-effective as well as energy efficient mechanism for wireless sensor networks is challenging job for the researcher.

References

[1] Shah Sheetal. Automatic Wireless Sensor Networks. Available from the World Wide Web (WWW): www-scf.usc.edu/~sheetals/publications/AutonomicWSN.doc

[2] Ren-Cheng Jin,Teng Gao, Jin-Yan-Song, Ji-Yan Zou, Li-Ding Wang(2013). Passive cluster-based multipath routing protocols for wireless sensor networks.Springer Science+Business Media. Doi: 10.1007/s11276-013-0648-z.

[3] Abbasi, A.A., & Younis, M.(2007). A survey on clustering algorithms for wireless sensor networks. Computer communications, 30(14-15), 2826-2841.

[4] J S Rauthan, S Mishra. An improved cluster based multi-hop routing in self organizing wireless sensor networks. International Journal of Engineering Research & Technology (IJERT) ISSN, 2278-081, Vol. 1 Issue 4, June-2012

[5] C.Shen, C. Srisathapronphat, C. Jaikaeo. Sensor Information Networking Architecture and Applications. Proceedings of IEEE Personal Communications, Vol.8, No. 4,pp.52-59, August 2001.

[6] S Taruna, Sakshi Shringi. A Cluster Based Routing Protocol for Prolonging Network Lifetime in Heterogeneous Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering. Vol.3, Issue 4, April 2013.

[7] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on Sensor Networks. IEEE Communications Magazine, vol. 40, Issue: 8, pp. 102-114, August 2002. Available from WWW: http://citeseer.ist.psu.edu/akyildiz02survey.html

[8] W.R. Heinzelman, Anantha Chandrakasan, and H. Balakrishnan, An Application-Specific Protocol Architecture for Wireless Microsensor Networks. In IEEE Transcations on Wireless Communications (October 2012), Vol.1 (4), pp.660-670.

[9] Lindsey, S., Raghavendra, C.S.: PEGASIS: Power-efficient gathering in sensor information systems. In: Proc. of the IEEE Aerospace Conf. Montana: IEEE Aerospace and Electronic Systems Society, pp. 1125–1130 (2002)

[10] Manjeshwar, A., Agrawal, D.P.: TEEN: A protocol for enhanced efficiency in wireless sensor networks. In: Int'l Proc. of the 15th Parallel and Distributed Processing Symp., pp. 2009–2015. IEEE Computer Society, San Francisco (2001)

[11] Ossama Younis and Sonia Fahmy, .Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach., September 2002.

[12] Qiu, M., Xue, C., Shao, Z., Zhuge, Q., Liu, M., Sha Edwin, H.M.: Efficent Algorithm of Energy Minimization for Heterogeneous Wireless Sensor Network. In: Sha, E., Han, S.- K., Xu, C.-Z., Kim, M.H., Yang, L.T., Xiao, B (eds.) EUC 2006. LNCS, vol. 4096, pp. 25–34. Springer, Heidelberg (2006)

[13] Yang, J.,M.,Xu, J.F., Xu, B.G., & Hong, L.(2009). A cluster based multipath delivery scheme for wireless sensor networks. In Proceedings of 2nd IEEE International conference on broadband network and multimedia technology, IEEE IC-BNMT2009(pp.286-291). doi:10.1109/ICBNMT.2009.5348484.

[14] Li, S. S., Zhu, P. D., Liao, X. K., & Fu, Q.(2006). Reliable data delivery in wireless sensor networks: An energy-efficient, cluster based approach. Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), LNCS, 4003, 384–395.
[15] Zahia, B., Hafid, H., & Moufida, M. (2011). Node disjoint multipath routing for ZigBee cluster-tree wireless sensor networks. International conference on multimedia computing and systems, ICMCS'11. doi:10.1109/ICMCS.2011.5945672.
[16] Li, J., Chen, Z. G., & Li, Z. Y. (2008). Hybrid cluster-based routing protocol in wireless sensor networks. Computer Science, 35(8), 32–34.
[17] Yang, J., Xu, M., Zhao, W., & Xu, B. G. (2010). A multipath routing protocol based on clustering and ant colony optimization for wireless sensor networks. Sensors, 10, 4521–4540.
[18] Dr. Manoj Kumar Jain. Wireless Sensor Networks: Security Issues and Challenges. IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 02, ISSUE 01, MANUSCRIPT CODE: 110746
[19] P. Apostolos, "Cryptography and Security in Wireless Sensor Networks," FRONTS 2nd Winterschool Braunschweig, Germany, 2009.
[20] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003,pp. 26 – 36.
[21] Pfleeger, C. P. and Pfleeger, S. L., "Security in Computing", 3rd edition, Prentice Hall 2003
[22] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).
[23] 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.
[24] 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.
[25] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong. Security in Wireless Sensor Networks: Issues and Challenges. Feb. 20-22, 2006 ICACT2006, ISBN 89-5519-129-4
[26] Tanveer A. Zia, Albert Y. Zomaya. A Lightweight Security Framework for Wireless Sensor Networks. Available on WWW: http://isyou.info/jowua/papers/jowua-v2n3-3.pdf