ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

An Appraisal on Secured Wireless Sensor Networks

Rasmiprava Singh, Sujata Khobragade, Snehlata Barde

Abstract - A wireless sensor network is a collection of nodes organized into a cooperative network. All of this sensor network research is producing a new technology which is already appearing in many practical applications. The future should see an accelerated pace of adoption of this technology. Recent advances in wireless sensor networks have led to many new protocols specifically designed for sensor networks where energy awareness is an essential consideration. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture. This paper will provide a brief overview for sensor networks and the routing protocol used for wireless sensor networks. Programming abstractions and languages for WSN are very active areas of research. Significant and important studies have been collecting empirical data on the performance of WSN. Such data is critical to developing improved models and solutions. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace.

Keywords— **WSN (Wireless Sensor Networks), ALOHA, MAC.**

I. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network [10]. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way we live and work. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces. Since a wireless sensor network is a distributed real-time system a natural question is how many solutions from distributed and real-time systems can be used in these new systems? Unfortunately, very little prior work can be applied and new solutions are necessary in all areas of the system. Smart environments represent the next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world. Sensory data comes from multiple sensors of different modalities in distributed locations. The smart environment needs information about its surroundings as well as about its internal workings.

The challenges in the hierarchy of: detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous. The information needed by smart environments is provided by Distributed Wireless Sensor Networks, which are responsible for sensing as well as for the first stages of the processing hierarchy.

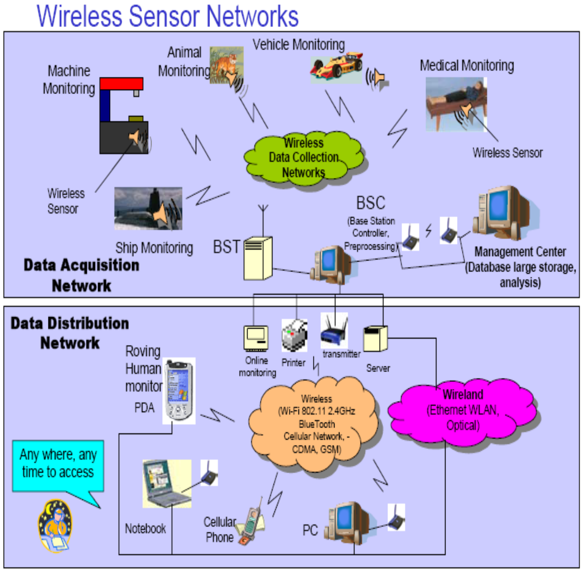

Wireless Sensor Networks
Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC
(Base Station Controller, Preprocessing)
Management Center (Database large storage, analysis)
Data Acquisition Network
Data Distribution Network
Online monitoring
Printer
transmitter
Server
Roving Human monitor
PDA
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN, Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

Fig 1. Wireless Sensor Network

The importance of sensor networks is highlighted by the number of recent funding initiatives, including the DARPA SENSIT program, military programs, and NSF Program Announcements. The figure shows the complexity of wireless sensor networks, which generally consist of a data acquisition network and a data distribution network, monitored and controlled by a management center. The plethora of available technologies makes even the selection of components difficult, let alone the design of a consistent, reliable, robust overall system.

A. Communication Networks

The study of communication networks can encompass several years at the college or university level. To understand and be able to implement sensor networks.

B. Network Topology

A communication network is composed of nodes, each of which has computing power and can transmit and receive messages over communication links, wireless or cabled. The basic network topologies are shown in the figure and include fully connected, mesh, star, ring, tree, bus. A single network may consist of several interconnected subnets of different topologies. Networks are further classified as Local Area Networks (LAN), e.g. inside one building, or Wide Area Networks (WAN), e.g. between buildings.

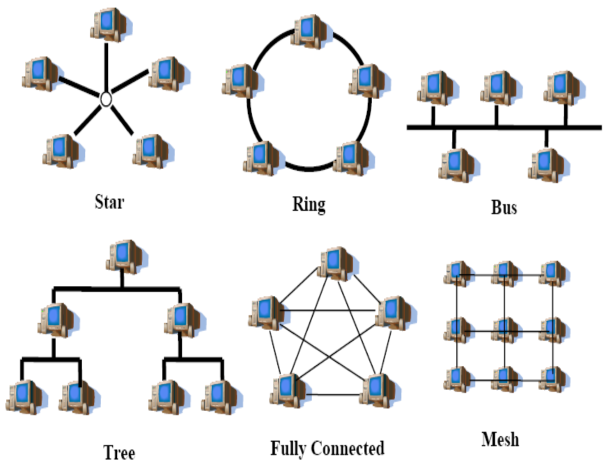


Fig 2. Network Topologies

Fully connected networks suffer from problems of NP-complexity [Garey 1979]; as additional nodes are added, the number of links increases exponentially. Therefore, for large networks, the routing problem is computationally intractable even with the availability of large amounts of computing power.

Mesh networks are regularly distributed networks that generally allow transmission only to a node's nearest neighbors. The nodes in these networks are generally identical, so that mesh nets are also referred to as peer-to-peer (see below) nets. Mesh nets can be good models for large-scale networks of wireless sensors that are distributed over a geographic region, e.g. personnel or vehicle security surveillance systems. All nodes of the star topology are connected to a single hub node. The hub requires greater message handling, routing, and decision-making capabilities than the other nodes. If a communication link is cut, it only affects one node. However, if the hub is incapacitated the network is destroyed.

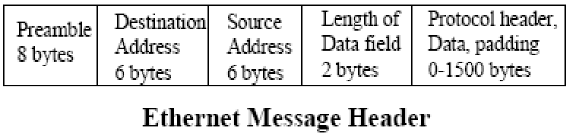
In the ring topology all nodes perform the same function and there is no leader node. Messages generally travel around the ring in a single direction.

In the bus topology, messages are broadcast on the bus to all nodes. Each node checks the destination address in the message header, and processes the messages addressed to it. The bus topology is passive in that each node simply listens for messages and is not responsible for retransmitting any messages.

1) Communication Protocols and Routing

The topics of communication protocols and routing are complex and require much study. Some basics useful for understanding sensor nets are presented here.

Headers. Each message generally has a header identifying its source node, destination node, length of the data field, and other information. This is used by the nodes in proper routing of the message. In encoded messages, parity bits may be included. In packet routing networks, each message is broken into packets of fixed length. The packets are transmitted separately through the network and then reassembled at the destination. The fixed packet length makes for easier routing and satisfaction of QoS. Generally, voice communications use circuit switching, while data transmissions use packet routing.



Preamble 8 bytes	Destination Address 6 bytes	Source Address 6 bytes	Length of Data field 2 bytes	Protocol header, Data, padding 0-1500 bytes

Ethernet Message Header

Fig 3. Ethernet Message Header [3].

In addition to the information content messages, in some protocols (e.g. FDDI- see below) the nodes transmit special frames to report and identify fault conditions. This can allow network reconfiguration for fault recovery. Other special frames might include route discovery packets or ferrets that flow through the network, e.g. to identify shortest paths, failed links, or transmission cost information. In some schemes, the ferret returns to the source and reports the best path for message transmission.

Switching. Most computer networks use a store-and-forward switching technique to control the flow of information [Duato 1996]. Then, each time a packet reaches a node; it is completely buffered in local memory, and transmitted as a whole. More sophisticated switching techniques include wormhole, which splits the message into smaller units known as flow control units or flits. The header flit determines the route. As the header is routed, the remaining flits follow it in pipeline fashion. This technique currently achieves the lowest message latency. Another popular switching scheme is virtual-cut-through. Here, when the header arrives at a node, it is routed without waiting for the rest of the packet. Packets are buffered either in software buffers in memory or in hardware buffers, and various sorts of buffers are used including edge buffers, central buffers, etc.

Multiple Access Protocols. When multiple nodes desire to transmit, protocols are needed to avoid collisions and lost data. In the ALOHA scheme, first used in the 1970's at the University of Hawaii, a node simply transmits a message when it desires. If it receives an acknowledgement, all is well. If not, the node waits a random time and re-transmits the message. A medium access control (MAC) protocol coordinates actions over a shared channel. The most commonly used solutions are contention-based. One general contention-based strategy is for a node which has a message to transmit to test the channel to see if it is busy, if not busy then it transmits, else if busy it waits and tries again later. After colliding, nodes wait random amounts of time trying to avoid re-colliding. If two or more nodes transmit at the same time there is a collision and all the nodes colliding try again later. Many wireless MAC protocols also have a doze mode where nodes not involved with sending or receiving a packet in a given timeframe go into sleep mode to save energy. Many variations exist on this basic scheme. In general, most MAC protocols optimize for the general case and for arbitrary communication patterns and workloads. However, a wireless sensor network has more focused requirements that include a local uni-or broad-cast, traffic is generally from nodes to one or a few sinks (most traffic is then in one direction),have periodic or rare communication and must consider energy consumption as a major factor. An effective MAC protocol for wireless sensor networks must consume little power, avoid collisions, be implemented with a small code size and memory requirements, be efficient for a single application, and be tolerant to changing radio frequency and networking conditions.

Since a distributed network has multiple nodes and services many messages, and each node is a shared resource, many decisions must be made. There may be multiple paths from the source to the destination. Therefore, message routing is an important topic. The main performance measures affected by the routing scheme are throughput (quantity of service) and average packet delay (quality of service). Routing schemes should also avoid both deadlock and live lock Routing methods can be fixed (i.e. pre-planned), adaptive, centralized, distributed, broadcast, etc. Perhaps the simplest routing scheme is the token ring [Smythe 1999]. Here, a simple topology and a straightforward fixed protocol result in very good reliability and precomputable QoS. A token passes continuously around a ring topology.

Multihop routing is a critical service required for WSN. Because of this, there has been a large amount of work on this topic. Internet and MANET routing techniques do not perform well in WSN. Internet routing assumes highly reliable wired connections so packet errors are rare; this is not true in WSN. Many MANET routing solutions depend on symmetric links (i.e., if node A can reliably reach node B, then B can reach A) between neighbors; this is too often not true for WSN. These differences have necessitated the invention and deployment of new solutions. For WSN, which are often deployed in an ad hoc fashion, routing typically begins with neighbor discovery. Nodes send rounds of messages (packets) and build local neighbor tables. These tables include the minimum information of each neighbor's ID and location. This means that nodes must know their geographic location prior to neighbor discovery. Other typical information in these tables include nodes' remaining energy, delay via that node, and an estimate of link quality..

Beyond the basics of WSN routing just presented, there are many additional key issues including:

- Reliability,
- Integrating with wake/sleep schedules,
- Unicast, multicast and any cast semantics,
- Real-time,
- Mobility,
- Voids,
- Security, and
- Congestion.

II. SYSTEM ARCHITECTURE AND DESIGN ISSUES

Depending on the application, different architectures and design goals/constraints have been considered for sensor networks. Since the performance of a routing protocol is closely related to the architectural model, in this section we strive to capture architectural issues and highlight their implications.

A. Network Dynamics

There are three main components in a sensor network. These are the sensor nodes, sink and monitored events. Aside from the very few setups that utilize mobile sensors most of the network architectures assume that sensor nodes are stationary. On the other hand, supporting the mobility of sinks or cluster-heads (gateways) is sometimes deemed necessary. Routing messages from or to moving nodes is more challenging since route stability becomes an important optimization factor, in addition to energy, bandwidth etc. The sensed event can be either dynamic or static depending on the application.

B. Node Deployment

Another consideration is the topological deployment of nodes. This is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data is routed through pre-determined paths. However in self organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

III. CONCLUSION

Routing in sensor networks has attracted a lot of attention in the recent years and introduced unique challenges compared to traditional data routing in wired networks. The goal of is to make a comprehensive survey of design issues and techniques for sensor networks describing the physical constraints on sensor nodes and the protocols proposed in all layers of network stack. Our survey is more focused and can serve those who like deeper insight for routing issues and techniques in wireless sensor networks. Other possible future research for routing protocols includes the integration of sensor networks with wired networks (i.e. Internet). Most of the applications in security and environmental monitoring require the data collected from the sensor nodes to be transmitted to a server so that further analysis can be done.

REFERENCES

[1] I.F. Akyildiz et al., Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393–422.

[2] K. Sohrabi et al., Protocols for self-organization of a wireless sensor network, IEEE Personal Communications 7 (5) (2000) 16–27.

[3] R. Min et al., Low power wireless sensor networks, in: Proceedings of International Conference on VLSI Design, Bangalore, India, and January 2001.

[4] J.M. Rabaey et al., Pico Radio supports ad hoc ultra low power wireless networking, IEEE Computer 33 (7) (2000) 42–48.

[5] R.H. Katz, J.M. Kahn, K.S.J. Pister, Mobile networking for smart dust, in: Proceedings of the 5th Annual ACM/ IEEE International Conference on Mobile Computing and Networking (MobiCom_99), Seattle, WA, August 1999.

[6] W.R. Heinzelman et al., Energy-scalable algorithms and protocols for wireless sensor networks, in: Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP _00), Istanbul, Turkey, and June 2000.

[7] T. He, S. Krishnamurthy, J. Stankovic, T. Abdelzaher, L. Luo, T. Yan, R. Stoleru, L. Gu, G. Zhou, J. Hui and B. Krogh, VigilNet: An Integrated Sensor Network System for Energy Efficient Surveillance, ACM Transactions on Sensor Networks, to appear.

[8] T. He, P. Vicaire, T. Yan, L. Luo, L. Gu, G. Zhou, R. Stoleru, Q. Cao, J. Stankovic, and T. Abdelzaher, Real-Time Analysis of Tracking Performance in Wireless Sensor Networks, IEEE Real-Time Applications Symposium, May 2006.

[9] T. He, P. Vicaire, T. Yan, Q. Cao, L. Luo, L. Gu, G. Zhou, J. Stankovic, and T. Abdelzaher, Achieving Long Term Surveillance in VigilNet, Infocom, April 2006.

[10] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, System Architecture Directions for Networked Sensors, ASPLOS, November 2000.

[11] C. Intanagonwiwat, R. Govindan, and D. Estrin, Directed Diffusion: A Scalable Routing and Robust Communication Paradigm for Sensor Networks, Mobicom, August 2000.

[12] B. Karp, Geographic Routing for Wireless Networks, PhD Dissertation, Harvard University, October 2000.

[13] S. Tilak et al., A taxonomy of wireless micro sensor network models, Mobile Computing and Communications Review 6 (2) (2002) 28–36.

[14] W. Heinzelman, A. Chandrakasan, H. Bal Krishnan, Energy-efficient communication protocol for wireless sensor networks, in: Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[15] M. Younis, M. Youssef, K. Arisha, Energy-aware routing in cluster-based sensor networks, in: Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS2002), Fort Worth, TX, October 2002.

[16] A. Manjeshwar, D.P. Agrawal, TEEN: a protocol for enhanced efficiency in wireless sensor networks, in: Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[17] W. Heinzelman, Application specific protocol architectures for wireless networks, PhD Thesis, MIT, 2000.

[18] C. Intanagonwiwat, R. Govindan, and D. Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks, in: Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_00), Boston, MA, and August 2000.

[19] M. Maroti, B. Kusy, G. Simon, and A. Ledeczi, The Flooding Time Synchronization Protocol, ACM SenSys, November 2004.

[20] M. Maroti, et. al., Radio Interferometer Geolocation, ACM SenSys, November 2005.

[21] D. Mills, Internet Time Synchronization: The Network Time Protocol, In Z. Yang and T. Marsland, editors, Global States and Time in Distributed Systems, IEEE Computer Society Press, 1994.

[22] A. Perrig, J. Stankovic, and D. Wagner, Security in Wireless Sensor Networks, invited paper, CACM, Vol. 47, No.6, June 2004, pp. 53-57, rated Top 5 Most Popular Magazine and Computing Surveys Articles Downloaded in August 2004, translated into Japanese.

Author Biography

Rasmiprava Singh, MTECH, NIT Raipur, international journal and national journal in manet, wireless communication, image processing..

Sujata Khobragade.MCA, NIT Raipur, International and national journal in network, mobile computing, image processing.

Snehlata Barde, MCA, National and international journals in Image processing, Network.