Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.423 – 427

SURVEY ARTICLE

A Survey on Wireless Sensor Network Protocols

T.Mythili[1], R.T.Narmadha[2], R.T.Nivetha[3]

[1]Information Technology & Info Institute of Engineering, India
[2]Information Technology & Info Institute of Engineering, India
[3]Computer Science and Engineering & Sri Eshwar College of Engineering, India
[1] sathyamythili@gmail.com; [2] narmadhahoney@gmail.com; [3] r.t.nivetha@gmail.com

Abstract—***In this research work, a survey on Wireless Sensor Networks (WSN) and their technologies, standards and applications was carried out. Wireless sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities. Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy awareness is an essential design issue. Routing protocols in WSNs might differ depending on the application and network architecture. A multidisciplinary research area such as wireless sensor networks, where close collaboration between users, application domain experts, hardware designers, and software developers is needed to implement efficient systems. The flexibility, fault tolerance, high sensing fidelity, low cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment, power consumption and efficient energy.***

Keywords—WSN; Power Management; Fault Tolerance; Topology; Scalability

I. INTRODUCTION

Wireless ad-hoc sensor networks have recently emerged as a premier research topic. They have great long-term economic potential, ability to transform our lives, and pose many new system-building challenges. Sensor networks also pose a number of new conceptual and optimization problems. Some, such as location, deployment, and tracking, are fundamental issues, in that many applications rely on them for needed information. Coverage in general, answers the questions about quality of service (surveillance) that can be provided by a particular sensor network. The integration of multiple types of sensors such as seismic, acoustic, optical, etc. in one network platform and the study of the overall coverage of the system also presents several interesting challenges. With the refinement of energy harvesting techniques that can gather useful energy from vibrations, blasts of radio energy, and the like, self-powered circuitry is a very real possibility, with networks of millions of nodes, deployed through paintbrushes, injections, and aircraft. Also, the introduction of an additional type of sensor nodes allowing the network to self-organize and "learn", by embedding smart and adaptive algorithms. On the other hand, The use of adaptive power control in IP networks that utilize reactive routing protocols and sleep-mode operation, more powerful mobile agents, QoS (Quality of Service) to guarantee delivery, security mechanisms, robustness and fault-tolerance. Wireless sensors have become an excellent tool for military applications involving intrusion detection, perimeter monitoring, information gathering and smart logistics support in an unknown deployed area. Some other applications: sensor-based personal health monitor, location detection with sensor networks and movement detection.

II. APPLICATIONS OF SENSOR NETWROKS

The development of sensor networks requires technologies from three different research areas: sensing, communication, and computing (including hardware, software, and algorithms). Thus, combined and separate advancements in each of these areas have driven research in sensor networks. Examples of early sensor networks include the radar networks used in air traffic control. The national power grid, with its many sensors, can be viewed as one large sensor network. These systems were developed with specialized computers and communication capabilities, and before the term “sensor networks” came into vogue. Table 1 summarizes the range of possible attributes in general sensor networks. Current and potential applications of sensor networks include: military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, distributed robotics, environment monitoring, and building and structures monitoring. The sensors in these applications may be small or large, and the networks may be wired or wireless.

. TABLE I
ATTRIBUTES OF SENSOR NETWORKS

Attributes	Features
Sensors	Size: Small (e.g., micro-electro mechanical systems (MEMS), large (e.g., radars, satellites) Number: Small, large Type: Passive (e.g., acoustic, seismic, video, IR, magnetic), active (e.g., radar, ladar) Composition or mix: Homogeneous (same types of sensors), heterogeneous (different types of sensors) Spatial Coverage: Fixed and planned (e.g., factory networks), adhoc (e.g., air-dropped) Dynamics: Stationary (e.g., Scismic sensors), mobile (e.g., on robot vehicles)
Sensing Entities of Interest	Extent: Distributed (e.g., environmental monitoring), localized (e.g., target tracking) Mobility: static, dynamic Nature: Cooperative (e.g., air traffic control), non-cooperative (e.g., military targets)
Operating Environment	Benign (factory floor), adverse (battlefield)
Communication	Networking: Wired, wireless Bandwidth: High, low
Processing Architecture	Centralized (All data sent to central site), distributed (located at sensor or other sites), hybrid
Energy Availability	Constrained (e.g., in small sensors), unconstrained (e.g., in large sensors)

A. Infrastructure Security

Sensor networks can be used for infrastructure security and counterterrorism applications. Critical buildings and facilities such as power plants and communication centers have to be protected from potential terrorists. Networks of video, acoustic, and other sensors can be deployed around these facilities. These sensors provide early detection of possible threats. Improved coverage and detection and a reduced false alarm rate can be achieved by fusing the data from multiple sensors. Even though fixed sensors connected by a fixed communication network protect most facilities, wireless ad hoc networks can provide more flexibility and additional coverage when needed. Sensor networks can also be used to detect biological, chemical, and nuclear attacks. Examples of such networks can be found in , which also describes other uses of sensor networks.

B. Environment and Habitat Monitoring

Environment and habitat monitoring is a natural candidate for applying sensor networks, since the variables to be monitored, e.g., temperature, are usually distributed over a large region. The recently started Center for Embedded Network Sensing (CENS), Los Angeles, CA, has a focus on environmental and habitat monitoring. Environmental sensors are used to study vegetation response to climatic trends and diseases, and acoustic and imaging sensors can identify, track, and measure the population of birds and other species. On a very large scale, the System for the Vigilance of the Amazon (SIVAM) provides environmental monitoring, drug trafficking monitoring, and air traffic control for the Amazon Basin. Sponsored by the government of Brazil, this large sensor network consists of different types of interconnected sensors including radar, imagery, and environmental sensors. The imagery sensors are space based, radars are located on aircraft, and environmental sensors are mostly on the ground. The communication network connecting the sensors operates at different speeds. For example, high-speed networks connect sensors on satellites and aircraft, while low-speed networks connect the ground-based sensors.

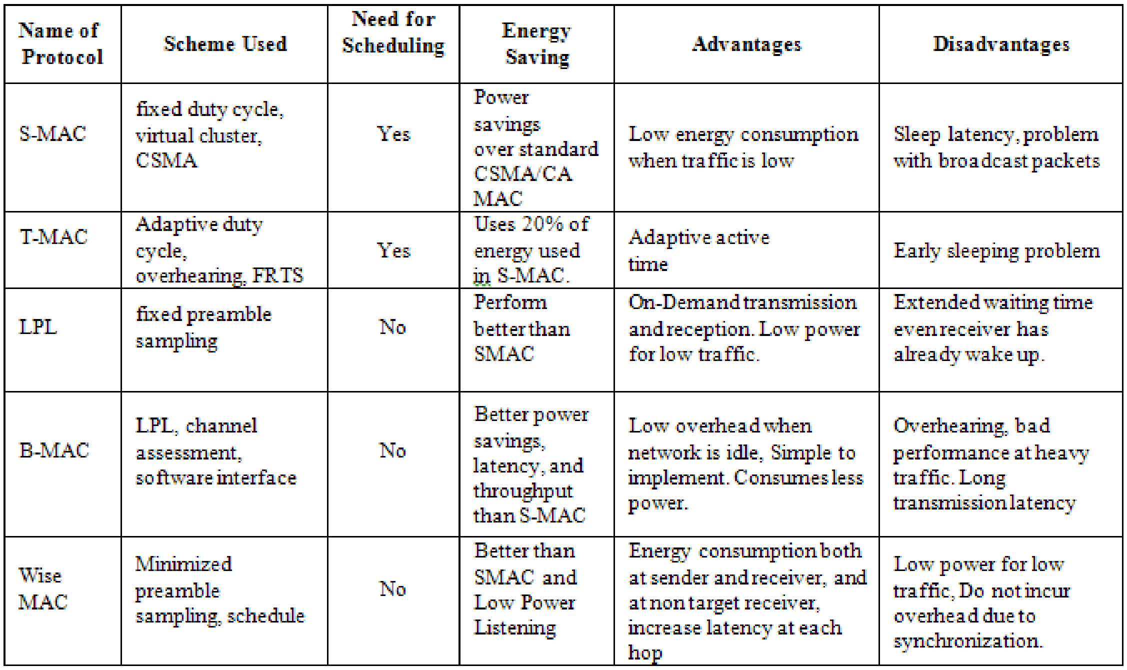
C. *Traffic Control*

Sensor networks have been used for vehicle traffic monitoring and control for quite a while. Most traffic intersections have either overhead or buried sensors to detect vehicles and control traffic lights. Furthermore, video cameras are frequently used to monitor road segments with heavy traffic, with the video sent to human operators at central locations. However, these sensors and the communication network that connect them are costly; thus, traffic monitoring is generally limited to a few critical points. Inexpensive wireless ad hoc networks will completely change the landscape of traffic monitoring and control. Cheap sensors with embedded networking capability can be deployed at every road intersection to detect and count vehicle traffic and estimate its speed.

The sensors will communicate with neighboring nodes to eventually develop a "global traffic picture" which can be queried by human operators or automatic controllers to generate control signals. Another more radical concept has the sensors attached to each vehicle. As the vehicles pass each other, they exchange summary information on the location of traffic jams and the speed and density of traffic, information that may be generated by ground sensors. These summaries propagate from vehicle to vehicle and can be used by drivers to avoid traffic jams and plan alternative routes.

III. **COMPARITIVE STUDY OF EXISTING NERGY-EFFFICIENT MAC PROTOCOLS**

TABLE 2
DIFFERENT MAC PROTOCOLS



Name of Protocol	Scheme Used	Need for Scheduling	Energy Saving	Advantages	Disadvantages
S-MAC	fixed duty cycle, virtual cluster, CSMA	Yes	Power savings over standard CSMA/CA MAC	Low energy consumption when traffic is low	Sleep latency, problem with broadcast packets
T-MAC	Adaptive duty cycle, overhearing, FRTS	Yes	Uses 20% of energy used in S-MAC.	Adaptive active time	Early sleeping problem
LPL	fixed preamble sampling	No	Perform better than SMAC	On-Demand transmission and reception. Low power for low traffic.	Extended waiting time even receiver has already wake up.
B-MAC	LPL, channel assessment, software interface	No	Better power savings, latency, and throughput than S-MAC	Low overhead when network is idle, Simple to implement. Consumes less power.	Overhearing, bad performance at heavy traffic. Long transmission latency
Wise MAC	Minimized preamble sampling, schedule	No	Better than SMAC and Low Power Listening	Energy consumption both at sender and receiver, and at non target receiver, increase latency at each hop	Low power for low traffic, Do not incur overhead due to synchronization.

IV. **FAILURES IN WIRELESS SENSOR NETWORKS**

To comprehend fault tolerance mechanisms, it is important to point out the difference between faults, errors, and failures. Various definitions of these terms have been used. A fault is any kind of defect that leads to an error. An error corresponds to an incorrect (undefined) system state. Such a state may lead to a failure. A failure is the (observable) manifestation of an error, which occurs when the system deviates from its specification and cannot deliver its intended functionality. Fig 1 illustrates the difference between fault, error, and failure. A sensor service running on node A is expected to periodically send the measurements of its sensors to an aggregation service running on node B. However, node A suffers an impact causing a loose connection with one of its sensors. Since the code implementing node A's service is not designed to detect and overcome such situations, an erroneous state is reached when the sensor service tries to acquire data from the sensor. Due to this state, the service does not send sensor data to the aggregation service within the specified time interval. This results in a crash or omission failure of node A observed by node.

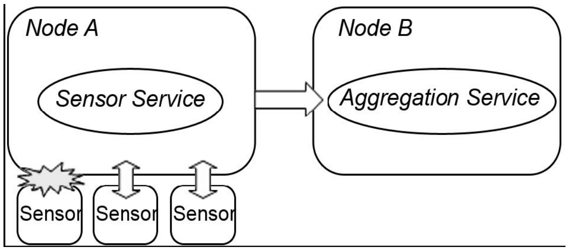


Fig.1 Failure cause by a loosely connected sensor

A. Source of Faults in Real WSN Applications

Wireless sensor networks are commonly deployed in harsh environment and are subject to faults in several layers of the system. To analyze the faults that can occur in real application scenarios we performed a research on several application trial reports. Fig 2 presents a layered classification of components in a WSN that can suffer faults. A fault in each layer of the system has the possibility to propagate to above levels. For example, a power failure of a node will cause the entire node to fail. If this node is on a routing path, the messages of other nodes relying on this routing path will not be delivered making an entire region of the network silent until the routing path is restored. Ultimately, if the application in the back-end which presents the WSN data to the users suffers a fault due to some software bug or hardware failure the entire system is considered faulty.

A small number of nodes are selected to become cluster heads. They are responsible for coordinating the nodes in their clusters, for instance by collecting data from them and forwarding it to the base station. In case that a cluster head fails, no messages of its cluster will be forwarded to the base station any longer. The cluster head can also intentionally or due to software bugs forward incorrect information. While forwarding messages, nodes can aggregate data from multiple other nodes in order to reduce the amount of data sent to the base station. One common simple approach is to calculate the average of correlated measured values such as temperature, humidity and pressure, sending only one message to the back-end. If a node generates incorrect data, the data aggregation results can suffer deviations from the real value. Also, if a node responsible for generating the aggregated data is subject to a value failure, the base station will receive incorrect information of an entire region of the network.

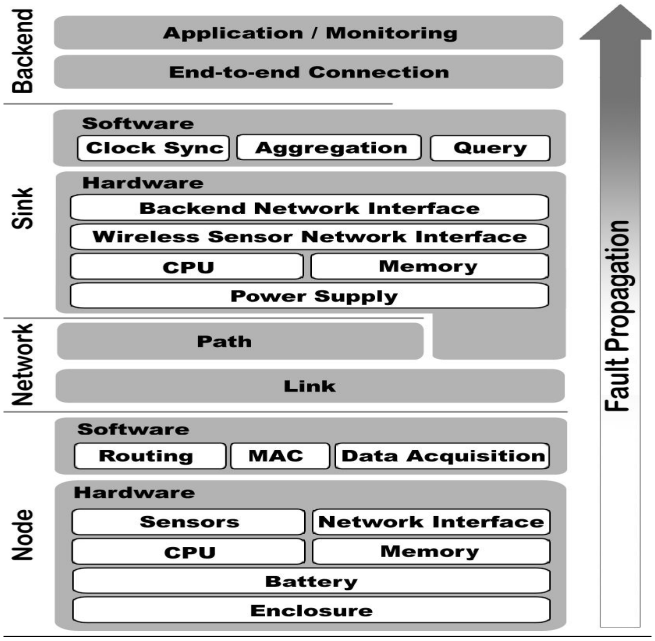


Fig 2: Fault classification and propagation

V. CONCLUSIONS

The flexibility, fault tolerance, high sensing fidelity, low-cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such a fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required. This addresses various factors in the wireless sensor networks.

REFERENCES

[1] Sha Liu, Kai-Wei Fan and Prasun Sinha , "An Energy Efficient MAC Layer Protocol Using Convergent Packet Forwarding for Wireless Sensor Networks", IEEE SECON, 2007

[2] Wei Ye, Fabio Silva, John Heidemann, "Ultra-Low Duty Cycle MAC with schedulled Channel Polling", ACM SenSys 2006, November, 2006.

[3] I. Gupta, D. Riordan, and S. Sampalli. Cluster-Head Election Using Fuzzy Logic for Wireless Sensor Networks. In Proceedings of the 3rd Annual Communication Networks and Services Research Conference, pages 255–260, 2005.

[4] S. Harte and A. Rahman. Fault Tolerance in Sensor Networks Using Self-Diagnosing Sensor Nodes. In The IEEE International Workshop on Intelligent Enviroment, pages 7–12, June 2005.

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In Proceedings of the 33rd Hawaii International Conference on System Sciences, volume 8, page 8020, 2000.

[6] K. Langendoen, A. Baggio, and O. Visser. Murphy loves potatoes: experiences from a pilot sensor network deployment in precision agriculture. In IPDPS 20th International Parallel and Distributed.