Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 2, February -2016

Future Technology and Trends in wireless Sensors: A Survey

Impana Appaji [1]

[1]*Assistant Professor, Computer Science & Engineering, Academy for Technical and Management Excellence college of Engineering, Mysore, Karnataka, India,*

Abstract- *Sensor networks consist of a large number of very small nodes that are deployed in some geographical area. The purpose of the network is to sense the environment and report what happens in the area it is deployed in. Sensor networks are used in many applications. In military applications they are used for surveillance and target tracking. In industrial applications, sensor networks are used in monitoring hazardous chemicals. They are also used in monitoring the environment and in early fire warning in forests as well as seismic data collections. Sensor networks face new challenges not known in cellular and ad-hoc wireless networks. In this paper, we report on currents and new trends in sensor networks. We also present some of the challenges and future work in sensor Networks.*

Keywords- *wireless sensor networks; multipath routing; reliability; security; energy conservation.*

I INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Wireless Sensor Networks (WSNs) that consist of a large number of small low cost, battery operated sensor node capable of wireless communication has wide range of application in many areas like environmental monitoring, field survey, disaster relief and so on. The efficiency of the sensor network is directly related with the length of the reliable monitoring duration of the field which must be achieved with better energy control of sensor nodes and the network management. Therefore, the limited battery resource of the sensors should be handled efficiently.

Wireless sensor networks enable people to observe details of real-world phenomena in both temporal and spatial dimensions. Data collection and sending data to sink are the fundamental function of WSNs, but also a challenging tasks due to limited resources of those tiny sensor nodes. Therefore, data collection scheme, which avoids abundant communication overhead yet keeps the data quality sand Multiple sink schema which reducing the distance from source to sink becomes the effective method to achieve a longer network lifetime of WSNs for data-driven applications, which require sensor nodes to perform data sampling and transmit data to Sink periodically, such as environmental monitoring .

Recent advances in VLSI technology, and MEMS (Micro-Electro-Mechanical Systems), as well as in wireless communication technology made it possible to manufacture sensor networks where very large numbers of very small nodes are scattered across some environment in order to sense and report to a central node (user). Sensor networks have many applications. In military, they are used for battlefield surveillance, and object tracking. They are used for seismic data collection and reporting, in addition to factories and warehouses for tracking and monitoring. It is also used in monitoring weakness in building structure or vehicles and airplanes. Before reviewing sensor networks, we will briefly describe the different types of wireless networks in order to show why sensor networks are different.

Wireless networks could be in one of three types, cellular, ad-hoc, or sensor networks. Cellular networks, best exemplified by the cellular phones consist of mobile devices roaming an area that is divided into cells, with a base station located in every cell in order to serve the devices in that cell. The cell radius ranges from few kilometres (in old networks) to few tens of meters for modern networks. The mobile devices communicate by establishing a connection to the base station; all the base stations are connected to the phone network. The base station acts as a gateway to make and receive phone calls. Traditionally, the cellular networks use circuit-switching mode of operation. However, recently a movement towards packet switching is gaining acceptance. Ad-hoc networks are networks that are deployed without an existing infrastructure. Mobile devices communicate among themselves by relaying the message over many devices. In this case, each mobile device works as a user and a routing switch at the same time. Usually, ad-hoc networks are networks that are established on a small geographical area in emergency situation. However, there are some proposals for wide area ad-hoc networks. Since both cellular and ad-hoc networks use mobile devices, low power circuits are very important.

However, the mobile devices are rechargeable. As we will see shortly, sensor nodes may not be rechargeable, the network works as long as the power supply is working, and then it ceases to work when the power supply is drained off. Sensor networks consist of very small devices that could be deployed in some areas. Each node is equipped with a sensor in order to perform monitoring, tracking, or surveillance and reports its finding to some central node. Most of the time the batteries in the nodes are not rechargeable, the networks operates as long as the power supply is O.K. when the power is off, the network ceases to operate. Thus low power is of utmost important in sensor networks.

II SENSOR NETWORKS

Sensor networks consist of very small nodes (sensors) that are deployed in some geographical area. Sensor networks are used to measure temperature or pressure, or it could be used for target tracking or border surveillance. It could be also deployed in factories in order to monitor toxic or hazardous materials. It is also used to measure the weakness in building structures, or in vehicles and airplanes.

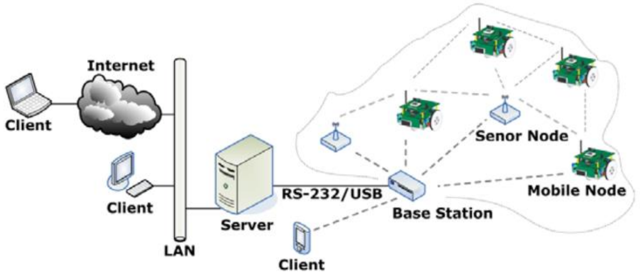

Fig.1.1: Typical Wireless sensor Network Topology.

A typical sensor node consists of 4 main parts. Power supply, sensor and analog to digital converter (ADC), processor and storage memory, finally, transceiver to send and receive data .

Two configurations for sensor networks The power supply is to power the node. The sensor circuitry can transform physical quantities into an electric signal. The ADC changes the analog signal generated by the sensor into a digital signal and sends it to the processor. The processor can perform simple operations on the received digital signal, and can store it into memory. Finally, the transceiver sends and receives data.

In both configurations the nodes are scattered in a geographical are, the area is divided into clusters with a gateway in each cluster. Nodes in each cluster communicate with the gateway. The gateway collects the data and forwards it to the user. In (a) nodes directly communicate with the gateway in its cluster, while in (b) nodes use chaining in order to communicate with the gateway. Using chaining reduces the energy used in transmission, but increases the energy used in processing since each node should receive and forward the message to and from other nodes. Some sensor networks may have more than one level of aggregation. Typically, sensor networks works in one of two modes. Continuous operation, or query mode. In continuous operation mode, the node is continuously sensing the environment and sending the data (or the processed data) to neighbouring or a central node. In query mode, the node is usually powered down waiting for a command from a central node, or neighbouring node. When the node receives the commands (usually on the form of report on so and so). It collects data from the sensor, processes it and sends it to the requesting node.

Wireless Sensor Networks (WSNs) consist of small nodes with sensing, computation, and wireless Communications capabilities. Many routing, power management, and data dissemination protocols have been specially designed for WSNs where energy awareness is an essential design issue. The focus, however, has been given to the routing protocols which might differ depending on the application and network architecture.

Overall, the routing techniques are classified into three categories based on the underlying network structure:

- Flat
- Hierarchical and
- Location-based routing.

Furthermore, the protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, and coherent-based depending on the protocol operation. Due to recent technological advances, the manufacturing of small and low cost sensors became technically and economically feasible. The sensing electronics measure ambient condition related to the environment surrounding the sensor and transforms them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. A large number of these disposable sensors can be networked in many applications that require unattended operations.

2.1 Multipath routing for Intrusion Tolerance

Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery.

While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the trade-off between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

Here we use multipath routing to tolerate intrusion. However, we specifically consider energy being consumed for intrusion detection, and both CHs and SNs can be compromised for lifetime maximization. In a randomized dispersive multipath routing protocol is proposed to avoid black holes. The randomized multipath routes are dispersive to avoid the black hole and to enhance the probability of at least *k* out of *n* shares based on coding theory can reach the receiver. The approach, however, does not consider intrusion detection to detect compromised nodes. Relative to our work also uses multipath routing to circumvent black hole attacks for intrusion tolerance. Moreover, we consider intrusion detection to detect and evict compromised nodes as well as the best rate to invoke intrusion detection to best trade-off energy consumption vs. security and reliability gain to maximize the system lifetime.

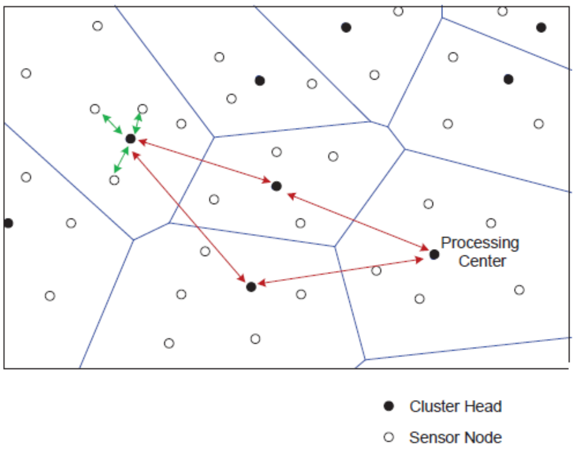

Fig.1.2: Source and path redundancy for WSNs

In general there are two approaches by which energy efficient IDS can be implemented in WSNs.

1. Flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbour nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status.
2. Another approach is local host-based IDS for energy conservation (with SNs monitoring neighbour SNs and CHs monitoring neighbour CHs only), coupled with voting to cope with node collusion for implementing IDS functions. Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions.

The solution considers the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime.

2.2 Removal of Malicious Nodes using IDS

To remove malicious nodes from the system, a voting based distributed IDS is applied periodically in every interval. A CH is being assessed by its neighbour CHs and a SN is being assessed by its neighbour SNs. In each interval, m neighbour nodes (at the CH or SN level) around a target node will be chosen randomly as voters and each cast their votes based on their host IDS results to collectively decide if the target node is still a good node. The m voters share their votes through secure transmission. When the majority of voters come to the conclusion that a target node is bad, then the target node is evicted. Here we note that increasing source or path redundancy enhances reliability and security. However, it also increases the energy consumption, thus contributing to the decrease of the system lifetime. Thus, there is a trade-off between reliability/security gain v/s. energy consumption. The distributed IDS design attempts to detect and evict compromised nodes from the network without unnecessarily wasting energy so as to maximize the query success probability and the system lifetime.

2.3 Design Factors

Because of the way sensor networks are envisioned, it is different than regular wireless networks. The design of sensor networks must concentrate on the challenges that are inherent to sensor networks. Most sensor networks are application specific and have different application requirements. Thus, all or part of the following main design objectives is considered in the design of sensor networks:

Fault tolerance: In sensors networks, hundreds, and in the extreme, hundreds of thousands of sensors are deployed in a large geographical area. In some cases dropped from airplanes, or deployed using artillery shells. Requiring that every node must work in order for the network to operate is impossible to achieve. The network must have a high level of fault tolerance in order to be of any practical value. Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of selftesting, self-calibrating, self-repairing, and self-recovering.

Scalability: As we mentioned above, sensor networks may include from tens to hundreds of thousands of sensors. Sometimes new nodes are added to the network after some nodes power supplies are completely exhausted. That results in a variable number of nodes. The protocols used in the networks must be scalable in order to survive under these circumstances.Since the number sensor nodes in sensor networks are in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.

Cost: because of the large number of nodes required, as well as the fact that in most networks the nodes are disposable (work until they drain off their power supply, then, then they are disposed of. The cost is a very important design factor for sensor networks. Having a low cost for sensor nodes is a must.

Power consumption: Power consumption is the most important design factor for sensor networks. Saving power during the operation of the electronic device could be achieved on more than one level. First, on the circuit or VLSI level, power could be saved by using less power for state transition (capacitor charging and discharging) and state maintenance. On the architecture level, power could be saved by the proper implementation of the processor, the cache, and the instruction set. A study on the StrongARM110 processor revels that the power dissipation in the instruction cache, data cache, and TLB accounts for almost 60% of the power consumption of the processor that means there is a room for power saving by the proper implementation of the memory system. Also power could be saved at the medium access control, and network level protocol. Minimizing the number of collisions or the path length results also in energy saving. Transmission and reception of radio signal is another candidate for power minimization. Short distance transmission and simple circuitry for modulation/demodulation results in power saving.

Small node size: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers, reducing node size can facilitate node deployment. It will also reduce the power consumption and cost of sensor nodes.

Low node cost: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, reducing cost of sensor nodes is important and will result into the cost reduction of whole network.

Low power consumption: Since sensor nodes are powered by battery and it is often very difficult or even impossible to charge or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

Reliability: Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.

Self-configurability: In sensor networks, once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

Adaptability: In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

Channel utilization: Since sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

Security: A sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

QoS support: In sensor networks, different applications may have different quality-of-service (QoS) requirements in terms of delivery latency and packet loss. Thus, network protocol design should consider the QoS requirements of specific applications.

2.4 Batteries

Power supply has always been a problem for mobile devices. The gap between the battery power and processor power requirements is widening every year. Recent research studies show that low power design is not the only solution for this problem. The total energy that could be delivered by the battery depends on how the energy is drawn from the battery. In [the authors argue that battery driven design is an important concept for electronic devices that depends on batteries. There are many types of batteries for use in mobile devices. Nickel Cadmium batteries are one of the oldest battery technology. The new Lithium Polymer batteries with their very thin form factor are a promising technology for tomorrow's mobile devices. Also, some batteries may be rechargeable. Rechargeable batteries could substantially increase the lifetime of a network. However it might not be always easy to recharge batteries in sensor networks. Another important step in the design of low power devices is how to model the battery energy supply? Batteries could be modelled using analytical model in which the battery is modelled as a reservoir of energy that is drained by a rate depends on the load.

Batteries also could be modelled as an electric circuit using standard circuit elements. A spice model to represent a battery is presented in Batteries also modelled using stochastic models, and using electrochemical models .

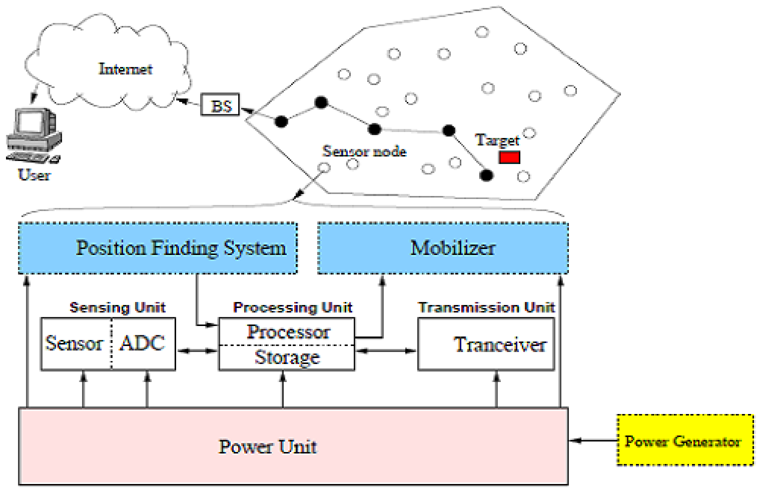

Fig.1.3: The Components of Sensor Node

III ROUTING AND MAC PROTOCOLS

Routing in sensor networks has some challenges that are not present in general wireless networks. The two main challenges are the varying topology nature of sensor networks, and the low power requirement on sensor networks, the authors proposed a medium access protocol for ad-hoc wireless sensor networks. They emphasized in their design that the main objective in wireless sensor networks in the power consumption rather than fairness, throughput, or delay, which are the main concern in useroriented networks. And they proposed a protocol called SMAC.

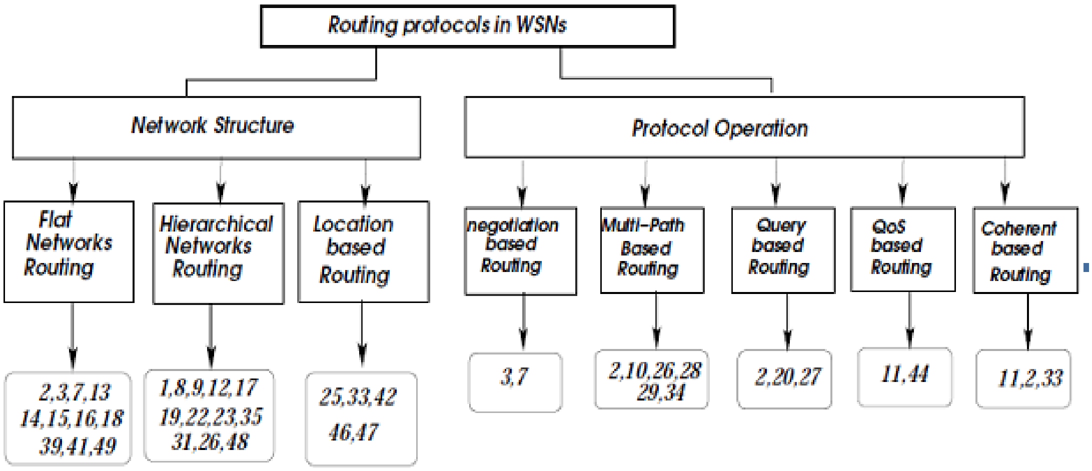

Fig.1.4: Routing Protocols in WSNs - A Taxonomy

In their design, they assumed that the network consists of many small nodes scattered in an ad-hoc fashion in order to collect some information about the environment. The nodes usually are in the idle mode until some event occurs; in this case, they record the event and send messages to other nodes. Other nodes may process the messages before forwarding it to a monitoring station. Their protocol depends on the RTS/CTS mechanism of the IEEE802.11 to avoid collisions. However in their protocol nodes alternate between listening and sleeping according to a specific schedule. Each node either determines its own schedule and broadcasts it, or follows the broadcast schedule of a neighbouring node. They implemented their protocol on the UCB Motes, using the Atmel AT90LS8535 microcontroller with 8K bytes of programmable flash and 512 bytes of data memory and they showed that their protocol consumes 2-6 times less power than IEEE802.11. In the authors proposed a power control extension to the IEEE802.11 MAC protocol. They used a concept similar to the power control in CDMA networks. Their simulation shows an improvement in both energy consumption and network throughput. In the authors investigated the effect of low energy routing on delay-constrained data, they also proposed a new energy-aware constrained routing for sensor networks. In addition, they used multihop routing to minimize transmission energy. The authors also used a weighted fair queuing packet scheduling methodology in order to achieve a soft real time guarantees. The problem of repositioning the base stations for enhancing the network performance is addressed ,Although many research projects in both industry and universities are being pursued. There is a lot of work to be done in the area of wireless networks protocols. Most of the work in sensor networks assumed the 5 layer TCP model which is very popular for wireline and wireless networks. However, there is no indication that this is the best model for sensor networks. This is almost unexplored area and a lot of work needs to be done especially at the application layer level.

Location-based Protocols : MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF

Data-centric Protocols : SPIN, Directed Diffusion, Rumor Routing, COUGAR, ACQUIRE, EAD, Information-Directed Routing, GradientBased Routing, Energy-aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination

Hierarchical Protocols : LEACH, PEGASIS, HEED, TEEN, APTEEN

Mobility-based Protocols: SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Base Data Dissemination

Multipath-based Protocols : Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery

Heterogeneity-based Protocols: IDSQ, CADR, CHR

QoS-based protocols : SAR, SPEED, Energy-aware routing

IV COMMUNICATIONS

Communication between nodes is done using either light, infrared, or radio transmission. Radio transmission is the most widely used communication medium between nodes, with the ISM (Industrial, Scientific, and Medical) band used in most networks. For wireless communication, the energy required to for the signal to travel a distance of d in free space is dn , where $2 \leq n \leq 4$ and n depends on the environment and is closer to 4 for short (near earth) antennas which is the case for wireless sensor networks. That shows how important it is for sensor nodes to communicate over short distance. Multihop communication is widely used in sensor networks. Not only it reduces power consumption, but is more immune to shadowing which makes it an attractive solution in sensor networks. Another factor to consider is the modulation scheme. M-ary scheme uses less bandwidth and higher data rate than binary scheme. However it uses more complex circuitry for the sender and receiver, which result in more power consumption at the transceiver. That requires a very detailed trade-off between the different modulation schemes in order to increase the network lifetime. Ultra Wide Band (UWB), or Impulse radio (IR), is another promising technology for wireless sensor networks. Its resistance to multipath makes it a very good candidate especially for indoor wireless networks. The best physical layer implementation for wireless sensor networks is mainly still an open problem. We expect that it will attract a lot of attention in the near future.

V CONCLUSION

In this paper, there are some of the challenges in designing wireless sensor networks, as well as the state-of the-art and future direction in wireless sensor networks. The field of sensor networks is very recent, and a lot of work needs to be done in it in order to mature and become an acceptable technology. To improve the fairness, analysis of the impact of other parameters on the proposed scheme's performance and implementing this scheme on a real sensor test-bed and compare the results with those obtained in the simulations.

REFERENCES

[1]. M. Ding, X. Cheng, and G. Xue, “Aggregation Tree Construction in Sensor Networks,” in Proc. of the IEEE 58th Vehicular Technology Conference (VTC), Vol. 4, pp. 2168-2172, October 2003.

[2]. M. Ettus, “System Capacity, Latency, and Power Consumption in Multihop-Routed SS-CDMA Wireless Networks,” in Proc. Of the IEEE Radio and Wireless Conference (RAWCON), pp. 55-58, Colorado Springs, August 1998.

[3] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing forIntrusion Tolerance in Heterogeneous Wireless Sensor Networks" IEEE Trans. networking, vol. VOL: 10 NO: 2 YEAR 2013.

[4] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," J. Netw. Comput. Appl., vol. 33, no. 4, pp. 422-432, 2010.

[5] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications, vol. 29, no. 2, pp. 216-230, 2006.

[6] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing Geographic Routing in Wireless Sensor Networks," 9th Annu. Cyber Security Conf. on Information Assurance, Albany, NY, USA, 2006.