Wireless Sensor Network and its Security – A Survey

M. Ravi[1], P. Subramaniam[2]

[1, 2]Assistant Professor, Department of Computer Science, Muthayammal College of Arts and Science, Rasipuram, Tamilnadu, India

Abstract: ***A wireless sensor network (WSN) has vital applications such as remote environmental monitoring and target tracking. This has been assisted by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are furnished with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, cost, hardware, and system constraints. The goal of our survey is to present a comprehensive review of the Wireless Sensor Network and its various types. A survey mainly focusing the security methods helps to protecting the data from the unauthorised users, Following the WSN security methods, we give an overview of several new WSN applications.***

Keywords: Wireless Sensor Network, Sensor network types, network security, WSN application.

1. Introduction

A. Wireless Sensor Network

Wireless sensor network is a collection of sensor nodes interconnected by wireless Communication channels. Each Sensor node is a small device that can collect data from its surrounding area, carry out simple computations, and communicate with other Sensors or with the base station (BS).Recent years have witnessed an increasing interest in using wireless sensor networks (WSNs) in many applications, including environmental monitoring and military field surveillance. In these applications, tiny sensors are deployed and left unattended to continuously report parameters such as temperature, pressure, humidity, light, and chemical activity. Reports transmitted by these sensors are collected by observers (e.g., Base Stations).The dense deployment and unattended nature of WSNs makes it quite difficult to recharge node batteries. Therefore, energy efficiency [20] is a major design goal in these networks. Several WSN applications require only an aggregate value to be reported to the observer. In this case, sensors in different regions of the field can collaborate to aggregate their data and provide more accurate reports about their local regions. For example, in a habitat monitoring application, the average reported humidity values may be sufficient for the observer.

In military fields where chemical activity or radiation is measured, the maximum value may be required to alert the troops. In addition to improving the fidelity of the reported measurements, data aggregation reduces the communication overhead in the network, leading to significant energy savings [7], [15]. The concept of wireless sensor networks is based on a simple equation:

Sensing + CPU + Radio = Thousands of potential applications

As soon as people understand the capabilities of a wireless sensor network, hundreds of applications spring to mind. It seems like a straightforward combination of modern technology. However, actually combining sensors, radios, and CPU's into an effective wireless sensor network requires a detailed understanding of the both capabilities and limitations of each of the underlying hardware components, as well as a detailed understanding of modern networking technologies and distributed systems theory. Each individual node must be designed to provide the set of primitives necessary to synthesize the interconnected web that will emerge as they are deployed, while meeting strict requirements of size, cost and power consumption.

A core challenge is to map the overall system requirements down to individual device capabilities, requirements and actions. To make the wireless sensor network vision a reality, architecture must be developed that synthesizes the envisioned applications out of the underlying hardware capabilities. To develop this system architecture we work from the high level application requirements down through the low-level hardware requirements. In this process we first attempt to understand the set of target applications. To limit the number of applications that we must consider, we focus on a set of application classes that we believe are representative of a large fraction of the potential usage scenarios. We use this set of 11 application classes to explore the system-level requirements that are placed on the overall architecture.

From these system-level requirements we can then drill down into the individual node-level requirements. Additionally, we must provide a detailed background into the capabilities of modern hardware. After we present the raw hardware capabilities, we present a basic wireless sensor node. The Rene node represents a first cut at a system architecture, and is used for comparison against the system architectures.

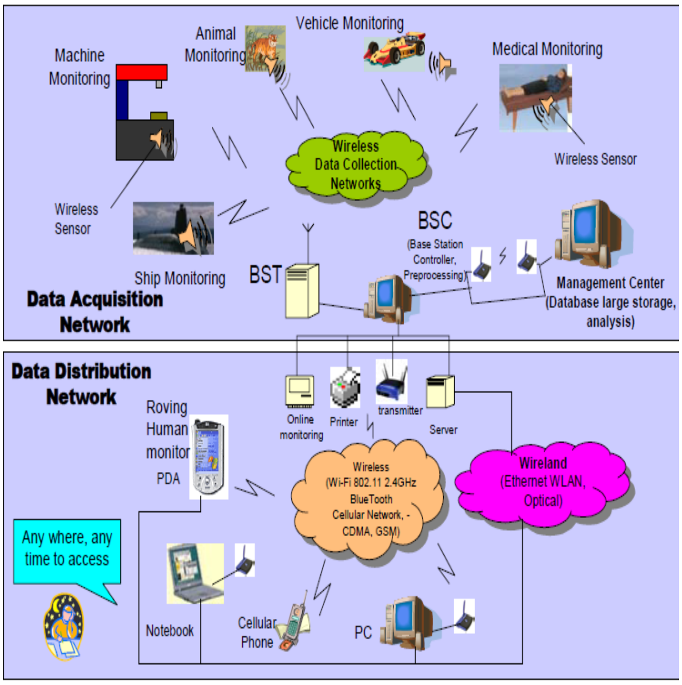

Figure 1: Wireless Sensor network architecture

2. Sensor Networks

Current WSNs are deployed on land, underground, and underwater. Depending on the environment, a sensor network faces different challenges and constraints. There are five types of WSNs:

- Terrestrial WSN
- Underground WSN
- Underwater WSN
- Multi-media WSN
- Mobile WSN

A. Terrestrial WSNs[11]

It is typically consist of hundreds to thousands of inexpensive wireless sensor nodes deployed in a given area, either in an ad hoc or in a pre-planned manner. In ad hoc deployment, sensor nodes can be dropped from a plane and randomly placed into the target area. In pre-planned deployment, there is grid placement, optimal placement [18], 2-d and 3-d placement [14, 5] models.

In a terrestrial WSN, reliable communication in a dense environment is very important. Terrestrial sensor nodes must be able to effectively communicate data back to the base station. While battery power is limited and may not be rechargeable, terrestrial sensor nodes however can be equipped with a secondary power source such as solar cells. In any case, it is important for sensor nodes to conserve energy. For a terrestrial WSN, energy can be conserved with multi-hop optimal routing, short transmission range, in-network data aggregation, eliminating data redundancy, minimizing delays, and using low duty-cycle operations.

B. Underground WSNs [9, 16]

It consists of a number of sensor nodes buried underground or in a cave or mine used to monitor underground conditions. Additional sink nodes are located above ground to relay information from the sensor nodes to the base station. An underground WSN is more expensive than a terrestrial WSN in terms of equipment, deployment, and maintenance. Underground sensor nodes are expensive because appropriate equipment parts must be selected to ensure reliable communication through soil, rocks, water, and other mineral contents. The underground environment makes wireless communication a challenge due to signal losses and high levels of attenuation. Unlike terrestrial WSNs, the deployment of an underground WSN requires careful planning and energy and cost considerations. Energy is an important concern in underground WSNs. Like terrestrial WSN, underground sensor nodes are equipped with a limited battery power and once deployed into the ground, it is difficult to recharge or replace a sensor node's battery. As before, a key objective is to conserve energy in order to increase the lifetime of network which can be achieved by implementing efficient communication protocol.

C. Underwater WSNs [8, 13]

It consists of a number of sensor nodes and vehicles deployed underwater. As opposite to terrestrial WSNs, underwater sensor nodes are more expensive and fewer sensor nodes are deployed. Autonomous underwater vehicles are used for exploration or gathering data from sensor nodes. Compared to a dense deployment of sensor nodes in a terrestrial WSN, a sparse deployment of sensor nodes is placed underwater. Typical underwater wireless communications are established through transmission of acoustic waves. A challenge in underwater acoustic communication is the limited bandwidth, long propagation delay, and signal fading issue. Another challenge is sensor node failure due to environmental conditions. Underwater sensor nodes must be able to self-configure and adapt to harsh ocean environment. Underwater sensor nodes are equipped with a limited battery which cannot be replaced or recharged. The issue of energy conservation for underwater WSNs involves developing efficient underwater communication [9] and networking techniques.

D. Multi-media WSNs[10]

It has been proposed to enable monitoring and tracking of events in the form of multimedia such as video, audio, and imaging. Multi-media WSNs consist of a number of low cost sensor nodes equipped with cameras and microphones. These sensor nodes interconnect with each other over a wireless connection for data retrieval, process, correlation, and compression. Multi-media sensor nodes are deployed in a pre-planned manner into the environment to guarantee coverage. Challenges in multi-media WSN include high bandwidth demand, high energy consumption, quality of service (QoS) provisioning, data processing and compressing techniques, and cross-layer design. Multi-media content such as a video stream requires high bandwidth in order for the content to be delivered. As a result, high data rate leads to high energy consumption. Transmission techniques that support high bandwidth and low energy consumption have to be developed. QoS provisioning is a challenging task in a multi-media WSN due to the variable delay and variable channel capacity. It is important that a certain level of QoS must be achieved for reliable content delivery. In-network processing, filtering, and compression can significantly improve network performance in terms of filtering and extracting redundant information and merging contents. Similarly, cross-layer interaction among the layers can improve the processing and the delivery process.

E. Mobile WSNs

It consists of a collection of sensor nodes that can move on their own and interact with the physical environment. Mobile nodes have the ability sense, compute, and communicate like static nodes. A key difference is mobile nodes have the ability to reposition and organize itself in the network. A mobile WSN can start off with some initial deployment and nodes can then spread out to gather information. Information gathered by a mobile node can be communicated to another mobile node when they are within range of each other. Another key difference is data distribution. In a static WSN, data can be distributed using fixed routing or flooding while dynamic routing is used in a mobile WSN. Challenges in mobile WSN include deployment, localization, self-organization, navigation and control, coverage, energy, maintenance, and data process.

Mobile WSN applications include but are not limited to environment monitoring, target tracking, search and rescue, and real-time monitoring of hazardous material. For environmental monitoring in disaster areas, manual deployment might not be possible. With mobile sensor nodes, they can move to areas of events after deployment to provide the required coverage. In military surveillance and tracking, mobile sensor nodes can collaborate and make decisions based on the target. Mobile sensor nodes can achieve a higher degree of coverage and connectivity compared to static sensor nodes. In the presence of obstacles in the field, mobile sensor nodes can plan ahead and move appropriately to obstructed regions to increase target exposure.

3. Security on Wireless Sensor Network

A WSN is vulnerable to threats and risks. An adversary can compromise a sensor node, alter the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resource. Unlike wired networks, wireless nodes broadcast their messages to the medium. Hence, the issue of security must be addressed in WSNs. There are constraints in incorporating security into a WSN such as limitations in storage, communication, computation, and processing capabilities. Designing security protocols requires understanding of these limitations and achieving acceptable performance with security measures to meet the needs of an application. Below we review several security proposals at different layers of the protocol stack.

Decentralized key-exchange protocol: This protocol guarantees the confidentiality of a key exchange even if an attacker has compromised some nodes in the network. The objective of the protocol is to minimize resource consumption on the individual devices in terms of memory requirements, CPU usage, and network traffic. The protocol guarantees the secrecy of a key exchange as long as there is less than s subverted nodes. The protocol uses s node-disjoint paths in an s-connected graph to distribute key shares. The nodes will use these key shares to generate a session key. If a key graph contains s node-disjoint paths between the source and destination, the source will randomly generates s key shares $k_1 \ldots k_s$ of identical length and sends them over the s node-disjoint paths to the destination. On each link of the path, the key share is encrypted and integrity protected with the existing share key for this link. Once key share is established, the attacker cannot recover data without access to all the key shares. Simulation results show that the network traffic grows linearly during key establishment.

LKE: Location-aware key establishment (LKE) is resilient against node capture attacks in large-scale sensor networks. LKE requires only a small amount of space to store keying information. LKE consist of four phases: pre-distribution phase, node self-configuration phase, polynomial share-distribution phase, and pairwise key establishment phase. In the pre-distribution phase, all sensors are programmed and configured the same before deployment [5]. A sensor's role and position is configured after deployment in the node self-configuration phase. Sensors determine their position based on a localization technique. Using the location information, each sensor differentiates itself as either a worker or a service node. Service nodes are self-elected. They are in charge of key space generation and key information distribution. If a sensor is not a service node, it is a worker node. Worker nodes get their key information from the service nodes in order to communicate with other nodes in the network. The polynomial share-distribution phase securely disseminates the polynomial share information to the worker nodes in three steps. The first step is the key space advertisement where the service node broadcasts its location, and public key information to the worker nodes. The second step is secure channel establishment. A worker node, which receives the server message, checks its validity to prevent false information. For each valid announcement that the server node receives, a computationally-asymmetric channel based on Rabin's cryptosystem is established. Both the service node and the worker node agree on a shared key. With the shared key, the service node encrypts the computed location-aware polynomial share and transmits it to the worker node in the last step. LKE employs an efficient pairwise key-establishment scheme for node communication. Two sensors sharing a common key space based on their location information can communicate with a common key. If two sensors do not share any key space, intermediate nodes are exploited for path key establishment. LKE is resilient against node capture attacks as long as no more than t sensor nodes are captured with the same key space. When more than t sensor nodes are compromised, all secure links within the key space are compromised. Results show that LKE requires low storage overhead in worker nodes and provides resilience against attacks.

TinySec: TinySec uses link-layer security architecture to guarantee message authenticity, integrity, and confidentiality. Message authenticity is the ability to detect false messages and reject them. Similar to message authenticity is message integrity, the detection of a tampered message. TinySec provides message authenticity and integrity by including a message authentication code (MAC) with each packet. The MAC is a cryptographically secure checksum of a message. The MAC is computed using a share secret key between the sender and the receiver. The sender computes the MAC of a packet using its secret key. The packet and the MAC are sent to the receiver. The receiver sharing the same secret key re-computes the MAC value of the message and compares it against the MAC received. If they are the same, the packet is accepted, else it is dropped. If an adversary alters the message during transit, he/she would not be able to re-compute the MAC value. Hence, the receiver will reject the message. Message confidentiality keeps information safe from unauthorized members. In this case, the encryption mechanism should achieve semantic security. Semantic security implies that adversaries cannot learn any property of the message even if they have obtained the message. TinySec achieves semantic security by using a unique initialization vector (IV) as a side input to the encryption algorithm. The purpose of IV is to add variation to the encryption process when there is little variation in the message set. The receiver must use IV to decrypt messages. Using IV, adversaries will not be able to determine the contents of messages simply by looking at its encryption.

TinySec supports authentication encryption (TinySecAE) and authentication only (TinySec-Auth) modes of operation. With TinySec-AE, the data payload is encrypted and the packet is authenticated using the MAC. With TinySecAuth, only authentication is performed on the packet with a MAC. TinySec utilizes cipher block chaining (CBC) for data encryption. CBC is used together with non-repeating IV to provide strong confidentiality guarantees.

4. Open Research Issues

Provisioning, management, and control services are needed to sustain network connectivity and maintain operations. Provisioning services such as localization and coverage can improve network performance. Efficient algorithms can reduce the cost of localization while sensor nodes are able to self-organize and identify themselves in some spatially coordinated system. Localization has been studied extensively to minimize energy, cost, and localization errors. The problem of energy conservation while maintaining a desired coverage has also been studied. Coverage efficiency depends on the number of active nodes. The more active nodes there are in the network, the higher is the degree of coverage. Coverage protocols should meet different levels of coverage requirements and be energy efficient. Existing solutions have investigated different degrees of coverage along with network connectivity. Future research and development should continue to focus on optimizing coverage for better energy conservation.

Management and control services include synchronization, data aggregation and compression, security, and cross-layer optimization. In a dense WSN, there is a need for network-wide time synchronization. Time synchronization eliminates event collision, energy wastage, and non-uniform updates. Proposed time synchronization protocols aim to synchronize local node clocks in the network and reduce energy overhead. Continuing research should focus on minimizing uncertainty errors over long periods of time and dealing with precision.

With large amounts of data generated over time, the cost of transferring all of the sensed data to the base station is expensive. Data compression and aggregation techniques aid in reducing the amount of data to be transferred. The development of various compression and aggregation scheme for event-based or continuous data collection network is a challenging research topic. For security monitoring in a WSN, secure protocols have to monitor, detect, and respond to attacks with uninterrupted service. Many proposed secure protocols are for the network layer and data-link layer. Malicious attacks can occur at any layer in the protocol stack. Secure monitoring for different layers of the protocol stack need to be explored. Cross-layer secure monitoring is another challenging area for research.

5. Sensor Networks Applications

Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions that include the following [3]:

- Temperature,
- Humidity,
- Vehicular movement,
- Lightning condition,
- Pressure,
- Soil makeup,
- Noise levels,
- The presence or absence of certain kinds of objects,
- Mechanical stress levels on attached objects, and
- The current characteristics such as speed, direction, and size of an object.

Sensor nodes can be used for continuous sensing, event detection, event ID, location sensing, and local control of actuators. The concepts of micro-sensing and wireless connection of these nodes promise many new application areas. We categorize the applications into military, environment, health, home and other commercial areas. It is possible to expand this classification with more categories such as space exploration, chemical processing and disaster relief.

A. Military Applications

Wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) systems. The rapid deployment, self-organization and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military C4ISRT. Since sensor networks are based on the dense deployment of disposable and low-cost sensor nodes, destruction of some nodes by hostile actions does not affect a military operation as much as the destruction of a traditional sensor, which makes sensor networks concept a better approach for battlefields. Some of the military applications of sensor networks are monitoring friendly forces, equipment and ammunition; battlefield surveillance; reconnaissance of opposing forces and terrain; targeting; battle damage assessment; and nuclear, biological and chemical (NBC) attack detection and reconnaissance.

Monitoring friendly forces, equipment and ammunition: Leaders and commanders can constantly monitor the status of friendly troops, the condition and the availability of the equipment and the ammunition in a battlefield by the use of sensor networks. Every troop, vehicle, equipment and critical ammunition can be attached with small sensors that report the status. These reports are gathered in sink nodes and sent to the troop leaders. The data can also be forwarded to the upper levels of the command hierarchy while being aggregated with the data from other units at each level.

Battlefield surveillance: Critical terrains, approach routes, paths and straits can be rapidly covered with sensor networks and closely watched for the activities of the opposing forces. As the operations evolve and new operational plans are prepared, new sensor networks can be deployed anytime for battlefield surveillance.

Reconnaissance of opposing forces and terrain: Sensor networks can be deployed in critical terrains, and some valuable, detailed, and timely intelligence about the opposing forces and terrain can be gathered within minutes before the opposing forces can intercept them.

Targeting: Sensor networks can be incorporated into guidance systems of the intelligent ammunition. Battle damage assessment: Just before or after attacks, sensor networks can be deployed in the target area to gather the battle damage assessment data.

Nuclear, biological and chemical attack detection and reconnaissance: In chemical and biological warfare, being close to ground zero is important for timely and accurate detection of the agents. Sensor networks deployed in the friendly region and used as a chemical or biological warning system can provide the friendly forces with critical reaction time, which drops casualties drastically. We can also use sensor networks for detailed reconnaissance after an NBC attack is detected. For instance, we can make a nuclear reconnaissance without exposing a recce team to nuclear radiation.

B. Environmental Applications

Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock; irrigation; macro instruments for large-scale Earth monitoring and planetary exploration; chemical/ biological detection; precision agriculture; biological, Earth, and environmental monitoring in marine, soil, and atmospheric contexts; forest fire detection; meteorological or geophysical research; flood detection; bio-complexity mapping of the environment; and pollution study [1].

Forest fire detection: Since sensor nodes may be strategically, randomly, and densely deployed in a forest, sensor nodes can relay the exact origin of the fire to the end users before the fire is spread uncontrollable. Millions of sensor nodes can be deployed and integrated using radio frequencies/ optical systems. Also, they may be equipped with effective power scavenging methods, such as solar cells, because the sensors may be left unattended for months and even years. The sensor nodes will collaborate with each other to perform distributed sensing and overcome obstacles, such as trees and rocks that block wired sensors' line of sight.

Bio complexity mapping of the environment: A bio complexity mapping of the environment requires sophisticated approaches to integrate information across temporal and spatial scales. The advances of technology in the remote sensing and automated data collection have enabled higher spatial, spectral, and temporal resolution at a geometrically declining cost per unit area. Along with these advances, the sensor nodes also have the ability to connect with the Internet, which allows remote users to control, monitor and observe the bio complexity of the environment.

Although satellite and airborne sensors are useful in observing large biodiversity, e.g., spatial complexity of dominant plant species, they are not fine grain enough to observe small size biodiversity, which makes up most of the biodiversity in an ecosystem. As a result, there is a need for ground level deployment of wireless sensor nodes to observe the bio complexity [17]. One example of bio complexity mapping of the environment is done at the James Reserve in Southern California. Three monitoring grids with each having 25– 100 sensor nodes will be implemented for fixed view multimedia and environmental sensor data loggers.

Flood detection [6]: An example of flood detection is the ALERT system [2] deployed in the US. Several types of sensors deployed in the ALERT system are rainfall, water level and weather sensors. These sensors supply information to the centralized database system in a pre-defined way. Research projects, such as the COUGAR Device Database Project at Cornell University [6] and the Data Space project at Rutgers, are investigating distributed approaches in interacting with sensor nodes in the sensor field to provide snapshot and long-running queries.

Precision Agriculture: Some of the benefits is the ability to monitor the pesticides level in the drinking water, the level of soil erosion, and the level of air pollution in real time.

C. Health Applications

Some of the health applications for sensor networks are providing interfaces for the disabled; integrated patient monitoring; diagnostics; drug administration in hospitals; monitoring the movements and internal processes of insects or other small animals; Telemonitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital [19].

Telemonitoring of human physiological data: The physiological data collected by the sensor networks can be stored for a long period of time, and can be used for medical exploration. The installed sensor networks can also monitor and detect elderly people's behaviour, e.g., a fall. These small sensor nodes allow the subject a greater freedom of movement and allow doctors to identify pre-defined symptoms earlier. Also, they facilitate a higher quality of life for the subjects compared to the treatment centers. A ''Health Smart Home'' is designed in the Faculty of Medicine in Grenoble—France to validate the feasibility of such system.

Tracking and monitoring doctors and patients inside a hospital: Each patient has small and light weight sensor nodes attached to them. Each sensor node has its specific task. For example, one sensor node may be detecting the heart rate while another is detecting the blood pressure. Doctors may also carry a sensor node, which allows other doctors to locate them within the hospital. Drug administration in hospitals: If sensor nodes can be attached to medications, the chance of getting and prescribing the wrong medication to patients can be minimized. Because, patients will have sensor nodes that identify their allergies and required medications.

D. Home Applications

Home automation: As technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs [4]. These sensor nodes inside the domestic devices can interact with each other and with the external network via the Internet or Satellite. They allow end users to manage home devices locally and remotely more easily. Smart environment: The design of smart environment can have two different perspectives, i.e., human-centered and technology-centered. For human-centered, a smart environment has to adapt to the needs of the end users in terms of input/ output capabilities. For technology-centered, new hardware technologies, networking solutions, and middleware services have to be developed. A scenario of how sensor nodes can be used to create a smart environment. The sensor nodes can be embedded into furniture and appliances, and they can communicate with each other and the room server. The room server can also communicate with other room servers to learn about the services they offered, e.g., printing, scanning, and faxing. These room servers and sensor nodes can be integrated with existing embedded devices to become self-organizing, self-regulated, and adaptive systems based on control theory models. Another example of smart environment is the ''Residential Laboratory'' at Georgia Institute of Technology. The computing and sensing in this environment has to be reliable, persistent, and transparent.

E. Other Commercial Applications

Some of the commercial applications are monitoring material fatigue; building virtual keyboards; managing inventory; monitoring product quality; constructing smart office spaces; environmental control in office buildings; robot control and guidance in automatic manufacturing environments; interactive toys; interactive museums; factory process control and automation; monitoring disaster area; smart structures with sensor nodes embedded inside; machine diagnosis; transportation; factory instrumentation; local control of actuators; detecting and monitoring car thefts; vehicle tracking and detection; and instrumentation of semiconductor processing chambers, rotating machinery, wind tunnels, and anechoic chambers.

Environmental control in office buildings: The air conditioning and heat of most buildings are centrally controlled. Therefore, the temperature inside a room can vary by few degrees; one side might be warmer than the other because there is only one control in the room and the air flow from the central system is not evenly distributed. A distributed wireless sensor network system can be installed to control the air flow and temperature in different parts of the room. It is estimated that such distributed technology can reduce energy consumption by two quadrillion British Thermal Units (BTUs) in the US, which amounts to saving of $55 billion per year and reducing 35 million metric tons of carbon emissions [12].

Interactive museums: In the future, children will be able to interact with objects in museums to learn more about them. These objects will be able to respond to their touch and speech. Also, children can participate in real time cause-and-effect experiments, which can teach them about science and environment. In addition, the wireless sensor networks can provide paging and localization inside the museum. An example of such museums is the San Franciso Exploratorium that features a combination of data measurements and cause and-effect experiments.

Detecting and monitoring car thefts: Sensor nodes are being deployed to detect and identify threats within a geographic region and report these threats to remote end users by the Internet for analysis. Managing inventory control: Each item in a warehouse may have a sensor node attached. The end users can find out the exact location of the item and tally the number of items in the same category. If the end users want to insert new inventories, all the users need to do is to attach the appropriate sensor nodes to the inventories. The end users can track and locate where the inventories are at all times.

Vehicle tracking and detection: There are two approaches to track and detect the vehicle: first, the line of bearing of the vehicle is determined locally within the clusters and then it is forwarded to the base station, and second, the raw data collected by the sensor nodes are forwarded to the base station to determine the location of the vehicle.

6. Conclusion

In this paper, we have surveyed issues on Wireless Sensor Network and its five different categories: (1) internal platform and underlying operating system, (2) communication protocol stack, and (3) network security, security issues. We have studied and compared different application on WSN. The security issues are analysed. Moreover, we have highlighted possible improvements and research in each area. There are still many issues to be resolved around WSN applications such as communication architectures, security, and management. By resolving these issues, we can close the gap between technology and application

Reference

[1] B. Halweil, Study finds modern farming is costly, World Watch 14 (1) (2001) 9–10.
[2] C.-Y. Wan, A.T. Campbell, L. Krishnamurthy, PSFQ: a reliable transport protocol for wireless sensor, in: Proceedings of the 1st ACM International workshop on Wireless Sensor Networks and Applications, 2002, pp. 1–11.
[3] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next century challenges: scalable coordination in sensor networks, ACM MobiCom'99, Washington, USA, 1999, pp. 263–270.
[4] D. Lucarelli, I.-J. Wang, Decentralized synchronization protocols with nearest neighbor communication, in: Proceedings of the Sensys'04, Baltimore, MD, 2004.
[5] D. Pompili, T. Melodia, I.F. Akyildiz, Deployment analysis in underwater acoustic wireless sensor networks, in: WUWNet, Los Angeles, CA, 2006.
[6] G. Wener-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, M. Walsh, Deploying a wireless sensor network on an active volcano, Data-Driven Applications in Sensor Networks (Special Issue), IEEE Internet Computing, March/April 2006.
[7] Heinzelman W. R, A. Chandrakasan, and H. Balkrishnan, "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks", in Proceedings of 33rd Hawaii International Conference on System Science, Vol. 2, Jan. 2000, pp.1-10.
[8] I.F. Akyildiz, D. Pompili, T. Melodia, Challenges for efficient communication in underwater acoustic sensor networks, ACM Sigbed Review 1 (2) (2004) 3–8.
[9] I.F. Akyildiz, E.P. Stuntebeck, Wireless underground sensor networks: research challenges, Ad-Hoc Networks 4 (2006) 669–686.
[10] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks Elsevier 51 (2007) 921–960.
[11] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine 40 (8) (2002).
[12] J. Elson, L. Girod, D. Estrin, Fine-grained network time synchronization using reference broadcasts, in: Proceedings of the 5th symposium on Operation System Design and Implementation (OSDI 2002), 2002.
[13] J. Heidemann, Y. Li, A. Syed, J. Wills, W. Ye, Underwater sensor networking: research challenges and potential applications, in: Proceedings of the Technical Report ISI-TR-2005-603, USC/Information Sciences Institute, 2005.
[14] J. Yick, G. Pasternack, B. Mukherjee, D. Ghosal, Placement of network services in sensor networks, Self-Organization Routing and Information, Integration in Wireless Sensor Networks (Special Issue) in International Journal of Wireless and Mobile Computing (IJWMC) 1 (2006) 101–112.
[15] Lindsey S., C.S. Raghavendra, PEGASIS: power efficient gathering in sensor information systems, in: Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.
[16] M. Li, Y. Liu, Underground structure monitoring with wireless sensor networks, in: Proceedings of the IPSN, Cambridge, MA, 2007.
[17] M.P. Hamilton, Hummercams, robots, and the virtual reserve, Directors Notebook, February 6, 2000, available from http://www.jamesreserve.edu/news.html.
[18] S. Toumpis, T. Tassiulas, Optimal deployment of large wireless sensor networks, IEEE Transactions on Information Theory 52 (2006) 2935–2953.
[19] S.-J. Park, R. Vedantham, R. Sivakumar, I.F. Akyildiz, A scalable approach for reliable downstream data delivery in wireless sensor networks, in: Proceedings of the ACM MobiHoc'04, Roppongi, Japan, 2004.
[20] V. Rajendran, K. Obraczka, J.J. Garcia-Luna-Aceves, "Energy efficient, collision-free medium access control for wireless sensor networks", Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.