Appl Geomat (2010) 2:43–48
DOI 10.1007/s12518-010-0022-0

REVIEW

Wireless sensor networks and their applications in geomatics: case study on developments in developing countries

Ravish Khichar · Sai Shivanandan Upadhyay

Received: 1 November 2009 / Accepted: 5 April 2010 / Published online: 4 May 2010

Abstract We are at a time of transition in the fields of planetary geodesy, mapping, and imaging. Planetary exploration has moved from a time of initial reconnaissance of the solar system using mostly planetary flyby missions and images exclusively from framing cameras to much more extensive missions of targeted exploration using orbiting spacecraft, line-scanner cameras, laser altimeters, and other sensors. It is appropriate to review the past history of this effort, recent advances in this area, and the current state of the art in both planetary and terrestrial geodesy, mapping, planetary imaging and surveillance, and reference systems. A wireless sensor network is a network consisting of small sensing devices spatially distributed using sensors to cooperatively monitor various conditions (Römer and Mattern, IEEE Wireless Comm 11(6):54–61, 2004; Thomas Haenselmann, *Sensornetworks*, GFDL Wireless Sensor Network textbook, http://www.informatik.uni-mannheim.de/~haensel/sn_book, 2006). So far, over 100 physical (light, pressure, humidity, etc.), chemical (gas, liquid, solid, etc.), and biological (DNA, protein, acoustics, etc.) properties can be sensed by using in situ sensing technology. With the presence of cheaper, miniature, faster, and smart in situ sensors, the increasing availability of abundant ubiquitous computing devices, wireless and mobile network access, and autonomous and intelligent geospatial software agents, distributed networked in situ sensing becomes clearly a technological trend. Sensor Webs can perform as an extensive monitoring and sensing system that provides timely, comprehensive, continuous, and multi-mode observations on underground mining, wildlife, and various physical infrastructures such as bridges, pipelines, and buildings. These new earth-observation systems open up new avenues to fast assimilation of data from various sensors (both in situ and remote) and to accurate analysis and informed decision-makings. This paper studies the security aspects and present and future applications of these networks. The paper first introduces the revolutionary concept of the Sensor Web and provides a comprehensive study of Sensor Web (both Sensor Web and sensors mean the same), and then presents its related security problems, threats, risks, and characteristics. Additionally, the paper gives a brief introduction to the application and the opportunities available for these networks in rural India and thereby provides an opportunity to improve the quality of life which is integrated with that of domestic animal health, soil and water quality, and plant/crop health. We examine the possibility of setting up of sensor networks to monitor these aspects so as to provide a detailed set of information to the residents as well as planners.

Keywords Wireless sensor network (WSN) · Sensor Web or sensors · Base station controller (BSC) · Base station transmitter (BST) · Web services

R. Khichar (✉)
Information Technology Engineering,
Global Institute of Technology,
Jaipur, Rajasthan, India
e-mail: ravish.khichar@gmail.com

S. Shivanandan Upadhyay
Computer Engineering,
Global Institute of Technology,
Jaipur, Rajasthan, India
e-mail: shiva.upadhyay008@gmail.com

Introduction

Developing countries have a multifaceted challenge in utilizing and maintaining resources most essential to them. Causes of inefficient utilization of resources are complex and their remedies may not be straightforward. To deal with those problems which require reporting of properties of a certain physical phenomena, we can make use of smart micro-

electronic objects called sentinels. The smart sentinels go by the name wireless sensor networks (WSN) and interface the physical world with computers, thereby creating a profound flexibility for awareness and remote controlling. One of the critical components in developing a Sensor Web is to build a geospatial information infrastructure, a backbone that connects the heterogeneous in situ sensors and remote sensors over the wired or wireless networks. They are characterized by their little demand for attention from human operators, their capability of self-management, operation in adverse places and near the occurrence of the actual phenomena, great accommodation of node mobility or failure, and effective node cooperation in order to carry out a distributed sensing task. The relative simplicity, smallness in size and affordable cost of wireless sensor nodes permit heavy deployment in places or objects in which a sensing task is carried out.

Historical developments

Ever since the human has started thinking, he has always tried his level best to compete with the ever-changing human needs. During the past 10–15 years, wireless technology has evolved from an unknown to a very fruitful, helping, and known jargon. Initial development included development of Ethernet in the mid-1970s. After this came Token Ring (1984) and Gigabit Ethernet (1996). All the above developments acted as a firm base for Wireless Fidelity (known as Wi-Fi). Wi-Fi is useful for fast and easy networking of PCs, printers, and other devices in a local environment, e.g., the home. Bluetooth, initiated in 1998, is a short-range RF technology aimed at facilitating communication of electronic devices between each other and with the Internet, allowing for data synchronization that is transparent to the user. Discovery protocols allow new devices to be hooked up easily to the network. Then came WiMAX (Worldwide Interoperability for Microwave Access). It is a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access. Before the onset of wireless sensor networks, Home RF (1988) came into existence. It had similar goals to Bluetooth for WPAN. Its goal is shared data/voice transmission. It interfaces with the Internet as well as the Public Switched Telephone Network. IrDA is a WPAN technology that has a short-range, narrow-transmission-angle beam suitable for aiming and selective reception of signals. But now comes the latest development, i.e. "wireless sensor networks".

Wireless sensor networks

Sensor networks are the key to gathering the information needed by smart environments, whether in buildings, utilities, industrial, home, shipboard, transportation systems automation, or elsewhere. Such characteristics make wireless sensor networks (1) robust to adverse situation and/or node failure, (2) capable of sensing at a considerably higher sensing granularity, (3) capable of functioning without the need for a human agent to manage the network in general or individual nodes in particular, and (4) to communicate a sensing event at long distances in a reliable and energy efficient way. In this paper, we introduce wireless sensor networks, discuss their building blocks, and identify several application domains in the context of developing countries (Dargie and Zimmerling 2007).

Recent terrorist and guerrilla warfare countermeasures require distributed networks of sensors that can be deployed using, e.g., aircraft, and have self-organizing capabilities. In such applications, running wires or cabling is usually impractical. A sensor network is required that is fast and easy to install and maintain (Lewis 2005).

IEEE 1451 and smart sensors Wireless sensor networks satisfy these requirements. Desirable functions for sensor nodes include: ease of installation, self-identification, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces (IEEE 1451 Expo 2001). There are many sensor manufacturers and many networks on the market today. It is too costly for manufacturers to make special transducers for every network on the market. Different components made by different manufacturers should be compatible. Therefore, in 1993, the IEEE and the National Institute of Standards and Technology began work on a standard for Smart Sensor Networks. IEEE 1451, the Standard for Smart Sensor Networks, was the result. The objective of this standard is to make it easier for different manufacturers to develop smart sensors and to interface those devices to networks.

Smart sensor, virtual sensor Figure 1 shows the basic architecture of IEEE 1451. Major components include Smart Transducer Interface Module (STIM), Transducer Electronic Data Sheet (TEDS), Transducer Independent Interface (TIL), Network Capable Application Processor (NCAP) (Lewis 2005). A major outcome of IEEE 1451

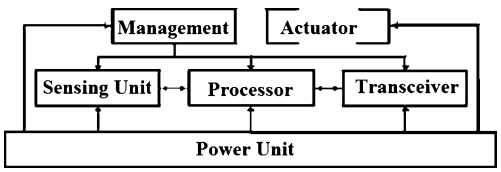

Fig. 1 Detailed basic architecture of a sensor module (Dargie and Zimmerling 2007)

studies is the formalized concept of a Smart Sensor. A smart sensor is a sensor that provides extra functions beyond those necessary for generating a correct representation of the sensed quantity. Included might be signal conditioning, signal processing, and decision-making/alarm functions. A general model of a smart sensor is shown in the figure. Objectives for smart sensors include moving the intelligence closer to the point of measurement; making it cost effective to integrate and maintain distributed sensor systems; creating a confluence of transducers, control, computation, and communications towards a common goal; and seamlessly interfacing numerous sensors of different types. The concept of a Virtual Sensor is also depicted. A virtual sensor is the physical sensor/transducer, plus the associated signal conditioning and digital signal processing required obtaining reliable estimates of the required sensory information. The virtual sensor is a component of the smart sensor.

Limitations in sensor networks

The following section lists the inherent limitations (Zia and Zomaya 2006) in sensor networks which make the design of security procedures more complicated.

Node limitations

A typical sensor node processor is of 4–8 MHz, having 4 kb of RAM, 128 kb flash, and ideally 916 MHz of radio frequency. The heterogeneous nature of sensor nodes is an additional limitation which prevents one security solution. Due to the deployment nature, sensor nodes would be deployed in environments where they would be highly prone to physical vandalism.

Network limitations

Besides node limitations, sensor networks bring all the limitations of a mobile ad hoc network where they lack physical infrastructure, and they rely on insecure wireless media.

Physical limitations

The nature of the deployment of sensor networks in public and hostile environments in many applications makes them highly vulnerable to capture and vandalism. Physical security of sensor nodes with tamper-proof material increases the node cost.

Security issues with wireless sensor networks

Security goals in sensor networks depend on the need to know what we are going to protect. We determine four security goals in sensor networks: Confidentiality, Integrity, Authentication, and Availability. *Confidentiality* is the ability to conceal a message from a passive attacker, where the message communicated on sensor networks remains confidential.

Integrity refers to the ability to confirm if the message has not been tampered, altered, or changed while it was on the network.

Authentication is the need to know if the messages are from the node it claims to be from, determining the reliability of message's origin.

Availability is to determine if a node has the ability to use the resources and the network is available for the messages to move on.

Data Freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. In recent researches, two types of freshness have been identified: weak freshness, which provides partial message ordering but carries no delay information; and strong freshness, which provides a total order on a request–response pair and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.

In *Robustness and Survivability*, the sensor network should be robust against various security attacks; and if an attack succeeds, its impact should be minimized. The compromise of a single node should not break the security of the entire network.

Security threats and types of attacks on sensor networks

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

Having built a foundation of security threats in computing, the next section lists the possible security attacks in sensor networks identified by Zia and Zomaya (2006), Undercoffer et al. (2002), and Karlof and Wagner (2003).

1. Passive information gathering:

An adversary with powerful resources collecting information from sensor networks if information is not encrypted.

2. Node subversion:

Capture of a node may reveal its information including disclosure of cryptographic keys, hence compromising the whole sensor network.

3. False node:

Addition of a malicious node by an adversary to inject the malicious data; false node would be computationally robust to lure other nodes to send data to it.

4. Node malfunction:

A malfunctioning node will generate inaccurate data which would jeopardize the integrity of sensor network especially when that node is a data aggregating node, e.g., a cluster leader.

5. Node outage:

What happens when a cluster leader stop functioning? Sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

6. Message corruption:

When contents of a message are modified by an attacker, it compromises the message integrity.

7. Traffic analysis:

Even if the message transfer is encrypted in sensor networks, it still leaves the high probability of analysis of communication patterns and sensor activities revealing enough information to enable the adversary to cause more malicious harm to sensor networks.

8. Routing loops:

In sensor networks, routing loops attacks target the information exchanged between nodes. False error messages are generated when an attacker alters and replays the routing information. Routing loops attract or repel the network traffic and increases node-to-node latency.

9. Selective forwarding:

Selective forwarding is a way to influence the network traffic by believing that all the participating nodes in the network are reliable to forward the message. In selective forwarding attacks, malicious nodes simply drop certain messages instead of forwarding every message. Once a malicious node cherry picks on the messages, it reduces the latency and deceives the neighboring nodes that they are on a shorter route. Effectiveness of this attack depends on two factors: location of the malicious node and the percentage of messages it drops. When selective forwarder drops more messages and forwards less, it retains its energy level, thus remaining powerful to trick the neighboring nodes.

10. Sinkhole attacks:

In sinkhole attacks, an adversary attracts the traffic to a compromised node. The simplest way of creating a sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or the malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. The nature of sensor networks where all the traffic flows towards one base station makes this type of attacks more susceptible.

11. Sybil attacks:

A type of attack where a node creates multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can be used against routing algorithms and topology maintenance; they reduce the effectiveness of fault tolerant schemes such as distributed storage and dispersity. Another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously.

12. Wormholes:

In wormhole attacks, an adversary positioned closer to the base station can completely disrupt the traffic by tunneling messages over a low latency link. Here, an adversary convinces the nodes which are a multi-hop away that they are closer to the base station. This creates a sinkhole because the adversary on the other side of the sinkhole provides a better route to the base station.

13. Hello flood attacks:

Broadcasting a message with stronger transmission power and pretending that the HELLO message is coming from the base station. Message receiving nodes assume that the HELLO message sending node is the closest one and they try to send all their messages through this node. In this type of attacks, all nodes will be responding to HELLO floods and wasting the energies. The real base station will also be broadcasting the similar messages but will have only few nodes responding to it.

14. DoS attacks:

Denial of service attacks occur at the physical level causing radio jamming, interfering with the network protocol, battery exhaustion, etc.

Present and possible future applications of WSN

Smart home or smart offices Sensors controlling appliances and electrical devices in the house such as Better lighting and heating in office buildings. For example, the Pentagon building has used sensors extensively.

Biomedical Can be used for health monitoring of patients (such as monitoring of glucose level, heart rate or cancer detection, etc.) and in hospitals to monitor vital signs and to record anomalies.

Military Remote deployment of sensors for tactical monitoring of enemy troop movements.

Industrial and commercial Numerous industrial and commercial applications such as Agricultural Crop Condition Monitoring, Inventory Tracking, In-Process Parts Tracking, Automated Problem Reporting, RFID—Theft Deterrent and Customer Tracing, and Plant Equipment Maintenance Monitoring.

Traffic management and monitoring Can be used in future vehicles (to handle accidents and thefts) and roads (to monitor traffic flows and to provide real-time route updates).

Present and possible future applications of WSN in India

With all the above applications included, we could add more applications of WSN related specifically for India. India is a country which is totally dependent on its rural counterpart; so if we want a developed India, we need to think first about the problems faced by village people. To overcome the basic routine problems faced by them, many wireless sensor networking projects are in pipeline and few have been implemented successfully. Given below are the solutions to some of those basic day-to-day problems.

(a) Panchard J, Hubaux J-P, Pigneur Y COMMONSense Net: sensor networks for water management in rural India. First outdoor testing started in January 2005 and system field testing in End 2005, Project ends by End 2007

COMMONSense Net, a wireless sensor network for resource-poor agriculture in the semi-arid areas of developing countries, is an ongoing research project that focuses on the design and implementation of a sensor network for agricultural management in developing countries, with a special emphasis on the resource-poor farmers of semi-arid regions (see Fig. 2). The results highlighted the potential the environment-related information has for the improvement of farming strategies in the face of highly variable conditions, in particular for risk management strategies (choice of crop varieties, sowing and harvest periods, prevention of pests and diseases, efficient use of irrigation water, etc.).

Panchard J, Rao S, Prabhakar TV, Hubaux J-P, Jamadagni HS (2007) COMMONSense Net: a wireless sensor network for resource- poor agriculture in the semiarid areas of developing countries

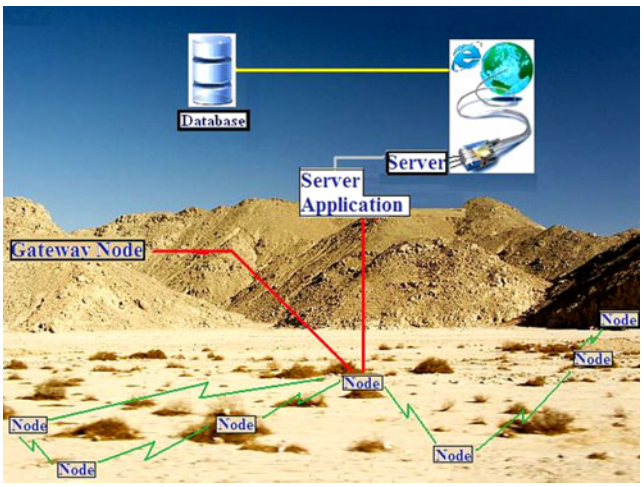

Fig. 2 Overview of wireless sensor nodes in a farmland

I. Technical challenges:

- Energy consumption and power management
- Localization of sensors
- Communication range
- Highly connected or sparse network?
- Application of decision models to the data
- Tampering with the hardware
- From sensing to actuation

II. Technical requirements:

- Communication range: up to 500 m
- Power-saving mechanisms: lifetime of every node over 1 year (the longer the better)
- Possibility to connect heterogeneous sensors to a single communication node
- Cost constraints

(b) Precision farming:

Precision farming is a term applied to utilizing new information and communication technology techniques to get localized environmental conditions of farm through the use of satellite imagery, Global Positioning System, and other means. The information gained is utilized to make decisions regarding appropriate use of water, nutrients, pest control, etc. to make optimal use of resources and improve productivity and quality. Wireless sensor networks promise to provide very detailed, spatially resolved crop and soil data from the ground rather than macro-level information available through remote imagery. The two complement each other (Ranjan 2008).

(c) Groundwater monitoring:

Water consumption has grown in many folds in the last century to the extent that extensive use of groundwater has been made. This has resulted in a drastic reduction in groundwater table level, and drying up of wells has become very common. It is estimated that nearly 15% of the earth's population has no access to clean water. According to some estimates, nearly 70% of the freshwater use is in agriculture, and out of this nearly 40% water is lost without being utilized due to evaporation, etc. In rural India (and most of the developing countries), water resources are shared by human beings, animals, and plants. Thus, these also interlink many of the health-related issues, and a detailed monitoring of water resources along with soil conditions is important to understand the quality of life in rural India. Some field trials are already going on in India under the aegis of COMMONSense Net System, aimed at designing and developing an integrated network of sensors for agricultural management in the rural semi-arid areas of developing countries. On top of having an impact on yield and efficiency at the local level, the system will allow the collection of extensive data that can be reused to better understand the effects of water and other environmental parameters on agriculture, and thus permit one to develop

replicable strategies. Here, a network of ground sensors periodically monitors salinity, humidity, etc. of the soil (Ranjan 2008).

(d) Animal health:

A large population in rural India depends highly on domesticated animals, and this dependence is integrated in the lifestyle of rural communities. Monitoring of animal health, location, and movement will allow forecasting of likely events, which can influence human health. It would also permit prevention of diseases which may affect animal health. In certain cases, some micro-climatic conditions have higher chances of infecting animals with some specific disease. Use of sensor networks to monitor local micro-climate allows us to take preventive action at the right time. These would not only permit us to save the animal but also prevent the spread of epidemics (Ranjan 2008).

(e) Monitoring lakes and ponds:

Rural India is basically dependent on rainwater; this rainwater gets collected in ponds and rivers. Placing wireless sensors in the lakes, ponds, and in rivers could continuously monitor their state and how they are being utilized. Also, by monitoring their pollution level, we could stop many epidemics from happening, thus improving the life of people.

(f) Disaster prevention etc.:

Sensor networks can be used at hazardous workspaces like underground mining, steelworks, and refineries. All these are situated in remote areas where it is very costly to set up an advanced monitoring system, so wireless sensors can be very fruitful at that instance. Most of these places entail a high risk by nature which is amplified by poorly engineered constructions in developing countries. Wireless sensor networks can be deployed in underground mining for surveillance of deteriorating grounds, toxic gases, and unstable grounds. In refineries, sensors can be used to track workers which can facilitate in alerting an operator if someone accidentally enters a temporary hazard zone or to guide firefighters to the people in danger. These applications can help to increase workplace safety and thus save many people's lives.

Conclusion

Wireless sensor networks have a promising future in many applications. In the absence of adequate security, deployment of sensor networks is vulnerable to a variety of attacks. Sensor node's limitations and the nature of wireless communication pose unique security challenges. Current research in sensor network security is mostly built on a trusted environment; however, several research challenges remain unanswered before we can trust on sensor networks. In this paper, we have discussed the limitations, threat models, and unique security issues faced by wireless sensor networks. On the basis of our observation, we motivate the need of a security framework to provide countermeasures against attacks in wireless sensor networks, and when these security issues are counter measured, we could really have a promising future in wireless security networks. The first step after developing countermeasures is to make wireless technology fruitful to humans and hence their lives because all the technologies are developed for the human welfare only. A large number of people die in road accidents, so we decided to develop an efficient, reliable system to overcome the wastage of time spent by the medical staff to reach the victim. This is the first step from our side to overcome the unnecessary deaths caused due to delay in providing the help and medical aid to the victims.

References

Dargie W, Zimmerling M (2007) Wireless sensor networks in the context of developing countries. 3rd IFIP World Information Technology Forum (WITFOR), Addis Ababa, Ethiopia

Haenselmann T (2006) Sensornetworks. GFDL Wireless Sensor Network textbook. Available at: http://www.informatik.uni-mannheim.de/~haensel/sn_book. Retrieved on 2006-08-29

Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks 1(2–3):293–315

Lewis FL (2005) Wireless sensor networks. In: Smart Environments: Technologies, Protocols, Applications, Cook DJ, Das SK (Eds), Chapter 2. Wiley, New York. Research supported by ARO Research Grant DAAD 19-02-1-0366

Ranjan P (2008) Sensor networks to monitor quality of life in rural area

Römer K, Mattern F, (2004). The design space of wireless sensor networks. IEEE Wireless Comm 11(6):54–61. doi:10.1109/MWC.2004.1368897.http://www.vs.inf.ethz.ch/publ/papers/wsn-esignspace.pdf

Undercoffer J, Avancha S, Joshi A, Pinkston J (2002) Security for sensor networks. CADIP Research Symposium

Zia T, Zomaya A (2006) Security issues in wireless sensor networks. In Proceedings of the International Conference on Systems and Networks, Nov 2–4, pp. 40, Tahiti, French Polynesia