International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 1 Article 12

October 2012

FOR SECURE MEDICAL CARE: USES OF SENSORS & WIRELESS COMMUNICATION

Shankha Mitra Sunani
Department of Electronics & Communication Engineering, Gandhi Institute of Engineering & Technology(GIET), Gunupur-765022, Rayagada, Odisha, India., smsunani@gmail.com

Bandana Malliick
Department of Electronics & Communication Engineering, Gandhi Institute of Engineering & Technology(GIET), Gunupur-765022, Rayagada, Odisha, India., bmalliick@gmail.com

FOR SECURE MEDICAL CARE: USES OF SENSORS & WIRELESS COMMUNICATION

Shankha Mitra Sunani[1], Bandana Malliick [2]

[1] Assistant Professor, Department of Electronics & Communication Engineering, Gandhi Institute of Engineering & Technology(GIET), Gunupur-765022, Rayagada, Odisha, India.
[2] Assistant Professor, Department of Electronics & Communication Engineering, Gandhi Institute of Engineering & Technology(GIET), Gunupur-765022, Rayagada, Odisha, India.

Abstract— Biological, chemical, and radiological agents can tamper with the activities of medical care providers, patient samples, and medicine administration. Which brings patients to a major risk? The challenge is to use the concepts of sensors to detect and monitor any violations in the medical care environment. Wireless devices must communicate multimedia data such as patient information, laboratory results, prescriptions, and X-ray and ECG reports. A discussion of sensors in patient rooms, clinics/wards, hospitals, and measurements of safety and security is presented. The available devices for sensor and wireless communication are also briefly included.

INTRODUCTION

Medical care environments can be vulnerable to malicious behavior and hostile settings. In Ad Hoc hospital setups for military operations, natural disasters, and terrorist attacks; wireless communication is needed in an antagonistic environment that consists of jungles, deserts, mountains, and lack of any fixed infrastructure. Everything is on the move including mobile units, base stations, and users. The nodes in such a distributed control environment may be malicious, selfish, malfunctioning, and compromised. Authentication, key management, integrity of data communication, adaptability to type/timing/duration/extension of failures is major technical challenges. In established hospitals with fixed infrastructures, the prospect of a terrorist attack on the water supply, electric grid, food supply, and the environment can cause havoc.

Biological, chemical, and radiological agents can tamper with the activities of medical care providers, patient samples, and medicine administration can result in a shut down of all medical care leaving patients at major risk. The technical challenge is to develop sensors to detect and monitor any violations in the medical care environment before threat to life occurs. Wireless devices must communicate multimedia data such as patient information, laboratory results, prescriptions, X-ray and ECG reports. The reliability, security, and accuracy of these sensors and wireless devices can affect the timeliness access to information for patient monitoring. In addition, data can be corrupted, computer information systems can fail, and communication networks may experience denial of service attacks leading to a complete failure of proper patient care.

During a disaster recovery, the interaction amongst healthcare providers, pharmacies, emergency personal (firemen, police), law enforcement agencies, and government/community leaders must be ensured through a wireless network. Such dynamic collaboration should be secure, private, reliable, correct/consistent, and sometimes anonymous.

I. TECHNOLOGY AND TYPES OF SENSORS

A. Technology

Wireless sensor networks are envisioned to consist of a large number of devices, each capable of some limited computation, communication and sensing, operating in an unattended mode with limited energy. Sensor networks are characterized by severe energy constraints because the nodes will often operate with finite battery resources and limited recharging. Some of the energy concerns are being addressed at the hardware and architecture level. At the physical layer, there is now a significant body of work on minimizing energy costs by adjusting the transmit power of nodes while achieving global network properties such as connectivity. At the link layer, some of the work has focused on energy-efficient media access schemes. The use of inexpensive, large-scale wireless sensor networks is likely to result in higher rates of temporary or lasting failures for individual nodes.

B. Types of Sensors

Advances in integrated circuits technology have enabled mass production of tiny, cost-effective, and energy-efficient wireless sensor devices with processing capabilities. A micro sensor is a device that is equipped with a sensor module that detects via electrical/electromagnetic fields, acoustics, optical, movement, chemicals, biological agents, radiation, environmental factors such as humidity, temperature, etc. [Iyengar, 1995.] Currently microsensors typically consist of 8-bit 4-MHz processors (80% of all microprocessors shipped in 2000 were 8-bit) [Tennenhouse, 2000] with slow 10-Kbps communication and 8-Kbyte read-only

memory and a 512-byte RAM [Perrig, 2001].

At Purdue University Center for Sensing Science and Technology (CSST), several types of biosensors are being developed for the detection of hazardous materials. A sensor to detect Anthrax uses chips covered with numerous microscopic squares coated with antibodies that attract a specific biological agent [Inerowicz, 2002.] A scanner that relays images of surface to a computer continually monitors the chip surface. Pattern recognition computer software determines if any changes are occurring on the squares that contain the antibodies [Inerowicz, 2002.] Research on proteins that serve as biomarkers for identification of viruses, toxins, bacteria uses an ion trap mass spectrometer which aids in locating the "fingerprints" of proteins. This "fingerprint" can be identified through a protein database [Reid, 2002.] Neutron-based detectors can be used to detect chemicals, biological agents, and nuclear materials [Koltick, 2003.] The changes in electrical conductivity when a foreign molecule is introduced can be measured with a device called a scanning tunneling microscope [Inerowicz, 2002]. Electronic sensors are described in [Agrawal, 2002]. The wireless communication issues are discussed in [Iyenger, 2003]. Wireless sensor networks have been discussed in [Estrin, 2001]. Varieties of sensors have been discussed in http://www.measure.com/sensors/sensor-other.html.

Research is underway on wireless sensor networks and microsensor systems that include surveys [Khan, 2000, Khan 1999] on networking negotiation based protocols [Kulik, 2002], sensor fusion [Iyenger, 2002, Kulik, 2002], distributing queries [Krishnamachari, 2002], localized algorithm [Meguerdichian, 2001], topology management [Schurgers, 2002], simulation [Park, 2000], scalability, and smart dust [Khan, 2000, Doherty, 2001, Warneke, 2001].

C. *Characteristics of sensors*

Characteristics of sensors to be considered are size, battery consumption, energy level, lifetime, movement (whether the sensor is mobile or must remain stationary), position (the sensor may be embedded or may be independent of its surroundings), redundancy (for checking integrity), and failure modes. The malfunctions may indicate that the sensor has failed, is degrading slowly, or possesses Byzantine behavior (goes up and down randomly.) Cost and practicality are also two very key properties of sensors to be examined.

II. RESEARCH ISSUES

Deploying sensors for monitoring requires research in security, communication, database systems, and energy aware computing. In security, we are working on jam resistant antennas [Zoltowski, 2000; Xu, 2003], fault tolerant authentication [Bhargava, 2000], denial of service attacks [Habib, 2003], and privacy and anonymity issues (http://www.CERIAS.purdue.edu, http://www.jrpit.flinders.edu.au/confpapers/CRPITV14Schadow.pdf). In communications, we are exploring communication delays, congestion, bandwidth utilization [www.cs.purdue.edu/people/bb.] In database systems, we are investigating data aggregation techniques such as summarization, pattern matching, integrity checking, and energy saving query processing [Khan, 2002.] In energy aware computing, research is underway in compilation and communication techniques [www.cs.purdue.edu/people/Li.] We are working closely with Dr. Clem McDonald at Indiana University Medical School in studying the research that applies to medical care [http://www.regenstrief.org/investigators/mcdonald.htm]. In the full paper, we will expand upon these results that can lead to a secure sensor based wireless network for medical care.

A. *Smart and jam resistant antennas*

The idea of smart antenna has been presented in [Biedka, 2000] Omni directional antenna transmits information uniformly in all directions. Neighboring devices cannot be broadcasting at the same time because it can cause congestion. The transmissions enable adversaries to eavesdrop the communication, analyze the pattern of the traffic, and locate the sender. One solution to the problem is the usage of smart antennae [Biedka, 2000]. Since transmissions are directed, remote stations can be reached with lower power consumption, and eavesdropping becomes more complicated. A smart antenna consists of multiple sub-antennas and switches. Smart antennae are available in several forms [Zoltowski, 2001]: sectorized, phased-array, and adaptive array. Sectorized antennae consist of individual sector elements aimed in different directions, where only one sector at a time is energized with Radio Frequency (RF). Phased-array antennae can steer a main lobe in any direction, but are not capable of forming intentional nulls. Adaptive arrays can form not only multiple main lobes, but also steerable nulls in the direction of interferers [Zoltowski, 2001]. A switch can direct the beam in a specific direction. It increases security and conserves power. Some antennas on multiple devices can be communicating with devices in different directions.

Another idea is the use of jam resistant antennas. The idea is to use two antennas on each device and use polarization in a way to receive signals from one direction. The success of the semi-blind method (cross relation method and exploitation of the training sequence) and a method based only on the training sequence has been demonstrated. The

simulation shows that training-based sequence-based performs better [Zoltowski, 2000] One can use blind or semi-blind algorithms for channel estimation as long as there are two distinct antennas available having either different polarizations or significant spatial separation for diversity sake [http://ece.purdue.edu/~mikedz/EDGE.] The ideas of channel estimation and equalization for GSM with multiple antennas are presented in [VTC, 1999].

B. Fault Tolerant Authentication

In fault tolerant authentication each sensor is supposed to authenticate with the controller (base station) before the data received can be used. In case the controller fails, a back-up controller in the immediate neighborhood can authenticate the sensor's signals and data. A hierarchy of base stations can also be used for authentication. The first scheme will require a virtual controller that contains primary and back-up controllers. For the hierarchical scheme, multiple keys will be required. The design analysis and experimental evaluation has been presented in [Bhargava, 2000].

C. Denial of Service Attacks and Intruder Identification

The communication among sensors and controllers could come under denial of service attacks [Habib, 2003] initiated by an intruder. Examples include flooding by a malicious device, impersonation, gang attack where multiple devices either malfunction or intentionally create a Byzantine behavior (sometimes act in normal mode, whereas at other times send errant messages.) The monitoring of quality of data and patterns at the controlling device's (base station) can identify the attack as well as the intruder. Suspicion lists and black lists can be created to ignore sensors involved in denial of service attack [Wang, 2003].

D. Privacy and Anonymity

Privacy issues become very important when a large hospital and all its operations are being monitored by sensors. The anonymity of the source of monitoring data and the location of the sensor needs protection from non-authorized access. The authenticated flow of information without the source can be achieved by using ideas discussed in [http://www.CERIAS.purdue.edu.] Since sensors will be deployed in hospital rooms, wards/clinics, and attached to hospital staff, the privacy issues and false identification of misbehavior needs further research. The medical care providers need to protect health information as required by HIPPA regulations. The patient's right to request a restriction or limitation on the disclosure of protected health information (PHI) for the purposes of treatment, financial liability, or health care operations should be maintained.

E. Energy Conservation

For energy conservation, the sensor could be in doze mode or active mode. The computation and communication by each sensor has to be carefully controlled. Since sensors can be part of a route to the controller, the routing schemes need to be energy efficient. If the data from previous sensors needs to be aggregated or patterns need to be identified, the algorithms have to be devised to minimize computation. This research is discussed in [Iyenger, 2003, Khan, 2002, www.cs.purdue.edu/people/Li].

III. UTILIZATION OF SENSORS IN A PATIENT'S ENVIRONMENT

A. Safety and Security of Patient's room

A sensor can be used to monitor the entrance and access to a patient's room. The frequency of interaction and the times of in and out activity could be observed. The pattern of activity within a patient's room with respect to the patient's intake of medicine, Intravenous administration, and devices connected to the patient can provide a useful tool to ensure patient safety. It can also protect the patient from neglect, abuse, harm, tampering, and unplanned movement of the patient outside the safety zone. Sensors can be utilized for patient identification band for the movement. Sensors can be attached to visitor's hospital clothing (i.e. gown, cap, gloves) to guarantee precautionary measures such as hygiene and prevention of infections.

B. Safety and Security of the Hospital

Sensors can be used to monitor temperature, humidity, air quality. They can be embedded in floor tiles to observe the conditions or obstacles for the mobile stretchers. For example, a red light can be activated if the floor is slippery or wet. Sensors can be used to protect access to FDA controlled products, narcotics, and dangerous drugs. This can also protect tampering with medicine, fraud in prescriptions, or attack by a disgruntled patient or staff. External factors that can create danger are discharge of biological agents, power outages, or electromagnetic attacks.

Sensors can help determine authentication of a healthcare provider who is authorized and deny access to others. The pattern of interaction with the patient can be assessed. Any unacceptable pattern of behavior such as not responding to patient needs can be avoided. Sensors can also provide safety of personnel and visitors against malicious activity and movement through an automated sensor-based network.

IV. PRIVACY AND SECURITY OF NETWORK AND COMPUTER SYSTEM

Medical research is being conducted at Indiana University Medical School [http://www.regenstrief.org/investigators/mcdonald .htm] in collaboration with five Indianapolis hospitals. The privacy of patients' records and identification must be preserved according to federal regulations. Changes to a patient record to avoid lawsuit or to intentionally alter a patient's treatment are examples of attacks.

The automated sensor network used for treatment and control of patient's health should be protected against attacks such as disabling monitoring devices, switching off or crashing computers, installation of flawed software, and disabling of sending/receiving messages. The quality of service issues come into play when multimedia data is transmitted. For example, the color, size, frame rate, and resolution may be compromised. Sensors can be utilized to protect the privacy and security of computer systems.

Wireless communication requires protocols such as IEEE 802.11 and its siblings. IEEE 802.11 allows for use of either the RF or IR mediums. When using RF, IEEE 802.11 uses the Frequency Hopping Spread Spectrum (FHSS) wideband system and has bandwidth limitation of 3 Mbps. IEEE 802.11b uses the Direct Sequence Spread Spectrum (DSSS) wideband system and can reach speeds up to 11 Mbps. A shared key of size 40 or 64 bits in IEEE 802.11 and 128 bits in IEEE 802.11b are used to provide authentication and encryption of data. However, these protocols are vulnerable to a wide range of attacks and an attacker can jam all frequencies in the band being used by the wireless network. Vulnerabilities include decrypting traffic and injection of new traffic from unauthorized mobile devices. Security problems and flaws in IEEE 802.11 based networks are discussed in [Housley, 2003, Cam-Winger, 2003] in the special issue of Communication of ACM, May 2003.

Another wireless technology being used in wireless communication is called Bluetooth. It is a low cost, low power short range radio link for wireless connectivity between sensors and mobile devices and access points. Similar to IEEE 802.11, Bluetooth is susceptible to physical threats and DoS attacks from jamming devices. Other problems include the inability to authorize users and susceptibility to eavesdropping and impersonation because of weaknesses with the cipher.

V. MEASURE OF SAFETY AND SECURITY

The safety and security of the medical care environment must be assessed and quantified. This is important if an automated sensor based environment is introduced in hospitals. Some suggested measures are:

- Number of incidents per day in patient room, ward, or hospital
- Calls to nurses and doctors that are not medical emergencies, but may be due to malfunctioning, failure, or intrusion in the sensor network
- Malfunctioning of components such as sensors, controllers, computers, network, fire alarms, smoke detectors, pagers
- Wrong information, data values, lost or delayed messages
- Timeliness, accuracy, precision, and other quality of service parameters

VI. SAMPLE OF AVAILABLE PRODUCTS

Communication protocols beyond 802.11 and Bluetooth include Wireless Fidelity which is becoming increasingly available for wireless networking [NY Times, 12/24/02.] Implantable devices are becoming available to build pacemakers for the brain. These can predict seizures and interrupt with jolts of electricity or tiny squirts of medication directly into the brain [NY Times, 2/18/03.] Systems to query tiny radio chips embedded in walls, shelves, packages, and sense the silence in case an item is removed. This technology known as radio-frequency identification---the same technology that enables an electronic sensor to record data from the E-ZPass tag or an office door to open with chip-equipped cards in their pockets is becoming available [NY Times 2/25/03.] Such radio chips can track inventories and thefts and are being built by Philip Semiconductor and Alien Technology. The tags unlike barcodes are programmable chips.

Technology is available to the terrorist who can use high energy systems that can kill all electronics, disrupt or destroy the digital devices that control the information flow used in the care of patients in the hospital. Directed energy and radio frequency weaponry can be used as a jamming technology according to John Arquilla, a professor of defense analysis at the Naval Postgraduate School in Monterey, CA [NY Times 2/20/03].

CONCLUSION

The reliability, security, and accuracy of these sensors and wireless devices can affect the timeliness access to information for patient monitoring. In addition, data can be corrupted, computer information systems can fail, and communication networks may experience denial of service attacks leading to complete failure of proper patient care. In this paper, we discuss security and safety issues in medical environment,

the technology, types, and characteristics of sensors, and research issues in smart antennas, denial of service, fault tolerant authentication, privacy issues, and energy considerations.

REFERENCES

1. Bhargava, B.; Kamisetty, S.; and Madria, S. "Fault Tolerant Authentication in Mobile Computing"in Proceedings of International Conference on Internet Computing (IC, 2000), Special Sessions on New Paradigms in Computer Security, pp. 176-185, June 2000.
2. Chessa, S.; Santi, P. "Crash Faults Identification in Wireless Sensor Networks." Computer Communications. Vol. 25, No. 14, pp. 1273-1282, Sept. 2002.
3. Costlow, Terry. "Despite Successes, Telemedicine's Future is clouded with Questions." Today's Engineer. Dec. 2002.
4. Estrin, D.; Girod, L.; Pottie, G.; and Srivastava, M. "Instrumenting the World with Wireless Sensor Networks." International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001), Salt Lake City, Utah, May 2001.
5. Grady, Denise. "Forgotten Surgical Tools 'Uncommon but Dangerous.'" The New York Times 21 Jan. 2003: D5.
6. Iyenger, S.S.; Brooks, R. Distributed Sensor Networks. CRC Press, Inc. 2003.
7. Iyenger, S. S.; Prasad, L., and Min, Hla. Advances in Distributed Sensor Integration: Applications and Theory. Prentice Hall, New Jersey, 07458, 1995, pp. 273.
8. Iyenger, S. S., Wu, Q. "Computational Aspects of Sensor Networks", International Symposium on Parallel Architectures, Algorithms and Networks, I-SPAN'02, May 2002. pp. 23-30.
9. Khan, M., Katz, R. H., Pister, K. S. J. "Emerging Challenges: Mobile Networking
10. Agrawal, D. P.; Zeng, Q. Introduction to Wireless and Mobile Systems. Brooks/Cole Thompson Learning, 2002. Pages: 450.
11. Krishnamachari, B., Estrin, D., Wicker, S. "The Impact of Data Aggregation in Wireless Sensor Networks," *Proc. Of the International Workshop on Distributed Event Based Systems (DEBS)*, Vienna, Austria, July 2002.
12. Min, R. Architecture for a Power-Aware Distributed Microsensor Node." IEEE Workshop on Signal Processing Systems (SiPS '00) October 2000.
13. Park, S., Savvides, A., Srivastava, M. B. "Simulating Networks of Wireless Sensor Networks," Proceedings of the 2002 Winter Simulation Conference, 2001, pp. 1330-1338.
14. Pottie, G. J.; Kaiser, W. J. "Wireless Integrated Network Sensors," Communications of the ACM. Vol. 43, No. 5, pp. 551-558, May 2000
15. Schurgers, C., Tsiatsis, V., Gaberiwal, S., Srivastava, M. "Topology Management for Sensor Networks: Exploiting Latency and Density," ACM MobiHOC 2002, pp. 135-145.
16. Tennenhouse, D. "Embedding the Internet: Proactive Computing. Communications of the ACM. Vol. 43, No. 5, pp. 43-50, 2000.
17. Wang, I., Jones, S. D. "The Scalability of a Class of Wireless Sensor Networks," Modeling and Design of Wireless Networks, Proceedings of SPIE, Vol. 4531, 2001, pp. 103-113.
18. Warneke, B., Liebowtiz, B., Pister, K. S. J., "Smart Dust: Communicating with a Cubic Millimeter Computer," Computer, 2001, pp. 2-9.
19. Zoltowski, M. Recent advances in reduced-rank adaptive fith applications to high-speed wireless communications. Proceedings of the Conference of the International Society for Optical Engineering, 2001.
20. http://www.measure.com/sensors/sensor-other.html
21. http://www.cs.ucla.edu/csd/CENS.html
22. http://www.ece.northwestern.edu/~pappas/nsf_workshop
23. http://www.nsf.gov/pubs/2003/nsf03512/nsf03512.htm
24. http://www.regenstrief.org/investigators/mcdonald.htm