International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 8– No.6, April 2015 – www.ijais.org

Medical Heed Sensors

Aiman J. Albarakati,
Department of Computer Engineering,
College of Computer and Information Science,
Majmaah University, Majmaah, Saudi Arabia

ABSTRACT

Up to date progress in embedded computing systems have led to the appearance of wireless sensor networks, consisting of small, battery-powered "motes" with restricted computation and radio communication competences. Sensor networks authorize data congregation and computation to be severely embedded in the physical environment. This technology has the prospective to blow the deliverance and study of resuscitative heed by allowing imperative cryptogram to be routinely collected and completely incorporated into the patient care/heed record and utilized for real-time triage, association with hospital records, and enduring surveillance. Medical Agents (Chemical, Biological, and radiological) can mess about with the activities of medical care suppliers, patient samples/trials, and drug management. This fallouts/leads in a shut down of all medical heed/care, leave-taking patients at a foremost jeopardy. The scientific defy is to build up sensors to identify and keep an eye on any infringements in the medical care environment prior to hazard to life occurs. Wireless devices have to communicate multimedia data such as patient information, laboratory results/trials, prescriptions, and EKG and X-ray reports. The consistency, protection, and truthfulness of these wireless devices and sensors can influence the aptness entrée to information for patient monitoring/supervision. Furthermore, data can be despoiled, computer information systems (I.S's) can be unsuccessful, and communication networks may possibly practice denial of service attacks direct to absolute collapse of an appropriate patient care/heed. In this article, we confer protection and safety concerns in medical environment, and distinctiveness of sensors, the technology/expertise, categories and research issues/agenda's in denial of service, smart antennas, fault tolerant authentication, privacy issues, and energy contemplations. A dialogue of sensors in patient rooms, wards/clinics, hospitals, and dimensions of safety and security is offered. The on hand devices for sensor and wireless communication are also briefly included.

Keywords

Sensors, WSN, IoT, Medical Care Sensors

1. INTRODUCTION

Medical care/heed related environments can be defenseless to malevolent actions and unfriendly settings/setup. In temporary or Ad Hoc hospital setups for natural disasters, military operations and terrorist attacks; wireless communication is required in an aggressive environment that consists of deserts, mountains, jungles, and be deficient in of any unchanging infrastructure. Everything is on the shift together with users, base stations and mobile units. The distributed control environment nodes may possibly be malevolent, egotistical, compromised and out of order. Reliability of data communication, Authentication, key management, flexibility to timing/duration/ type /extension of breakdowns is foremost scientific defies. Unchanging/fixed infrastructures in recognized hospitals with, the panorama of a fanatic assault on the water supply, food supply, electric grid, and the surroundings can cause chaos. During a disaster upturn, the dealings amongst government/community, law enforcement agencies, emergency personal (firemen, police), healthcare providers, leaders and pharmacies are obliged to ensure all the way through a wireless network. Such vibrant alliance ought to be sheltered, correct/consistent, sometimes anonymous, reliable and private.

2. KNOW-HOW

It has been that WSN consist of a huge number of devices and each one competent of a number of communication and sensing, restricted computations operating in an unattended mode with restricted energy. As the nodes will frequently maneuver with predetermined battery resources and restricted recharging so in this regards Sensor networks are distinguished by strict energy constraints. Various energy apprehensions are being outlined at the architecture and hardware level. So far the physical layer is concern so at present a considerable body of work on diminishing energy outlays by regulating the transmit power of nodes whereas attaining comprehensive network properties such as connectivity. Various works has been focused on energy-efficient media access schemes at the link layer. Inexpensive, large-scale wireless sensor networks usage is expected to result in privileged rates of provisional or durable breakdowns for individual nodes.

3. DISTINCTIVENESS

Sensors distinctiveness/characteristics to be well thought-out are mass/size, energy level, battery consumption, movement (whether the sensor is mobile or must remain stationary), lifetime, position (the sensor may possibly be implanted or may perhaps be autonomous of its environment), redundancy (for read-through reliability), and malfunction modes. The breakdowns may possibly point towards sensor failure, is mortifying leisurely, or possesses Byzantine/tortuous actions "goes up and down arbitrarily". Expediency and cost are also two incredibly key properties of sensors to be scrutinized.

4. CATEGORIES

Integrated circuits technology progression has made possible mass production of petite, energy-efficient and lucrative wireless sensor devices with dispensation potential. Lets start with a micro-sensor, which is a device that is outfitted with a sensor module that sense via electromagnetic/ electrical fields, chemicals, movement, biological agents, optical, environmental factors such as humidity, temperature, radiation, acoustics, etc. [4] At present micro-sensors usually consist of 8-bit 4-MHz processors. [5] with dawdling 10-Kbps communication and 8-Kbyte read-only memory and a 512-byte RAM [6]. Numerous kinds of biosensors are being developed for the discovery of perilous materials at

Purdue University Center for Sensing Science and Technology (CSST). A sensor to perceive Anthrax utilizes chips roofed with various microscopic squares layered with antibodies that exert a pull on an explicit biological agent [7]. A scanner that passes on images of surface to a computer incessantly keeps an eye on the chip surface. Pattern identification computer software agrees on if any amendments are stirring on the squares that restrain the antibodies [7]. Study on proteins that dish up as biomarkers for classification of toxins, bacteria and viruses brings into play an ion entrap mass spectrometer which abets in tracing the fingerprints of proteins. A protein database can be used to identify this fingerprint [8]. Biological agents, chemicals and nuclear materials can be detected through Neutron-based detectors [9]. Scanning tunneling microscope (STM) device can be used to measure the changes in electrical conductivity when a foreign molecule is introduced [7] [1] described Electronic sensors. The wireless communication problems are conferring in [10]. Wireless sensor networks (WSN) have been conferred in [11]. Research is in progress on WSN's and micro-sensor systems that comprise appraisals/analysis [12][13] on networking negotiation based protocols [14], distributing queries [15], sensor fusion [16], [14], localized algorithm [17], simulation [18], topology management [19], scalability, and smart dust [20], [21], [22].

5. SENSORS DEPLOYMENT SCENARIOS

5.1 Computer and Network System Security

Patient's records of privacy and classification have to be sealed according to authority regulations. Modifications to a patient record to shun grievance or to deliberately amend a patient's treatment/care/heed are instances of assaults. The automated sensor network exercised for treatment/care and be in charge of patient's fitness ought to be sheltered against assaults such as switching off or deafening computer systems, putting monitoring devices out of action, hindering of sending & receiving information and setting up of inconsistent software. Issues regarding quality of service (QoS) arise when transmission of multimedia data occurs. E.g. frame rate, the color, resolution and size might be compromised. For the sheltering the seclusion and protection of computer systems sensors can also be brought into play. Wireless communication entails protocols such as IEEE 802.11 and its siblings. IEEE 802.11 consent to make use of either the IR or RF mediums. When utilizing RF, IEEE 802.11 brings into play the Frequency Hopping Spread Spectrum wideband system with bandwidth restriction of 3 Mbps. IEEE 802.11b exercises the Direct Sequence Spread Spectrum wideband system with bandwidth up to 11 Mbps. IEEE 802.11 use a shared key having size 40 or 64 bits and IEEE 802.11b use key of having size in and 128 bits to endow with encryption and endorsement of data. Nevertheless, these protocols are susceptible to a broad range of attacks/assaults and an assailant can easily jam/squeeze all frequencies employed by wireless network. Liabilities take in decrypting traffic and inoculation of new-fangled traffic from unconstitutional mobile devices. Security concerns and faults in IEEE 802.11 based networks are argued in [23], [3] in the particular issue of Communication of ACM, May 2003.

5.2 Hospital Security

Sensors are also capable to be used for supervision of temperature, air quality and moisture. By embedding the sensors into floor tiles to detect the circumstances or obstructions. E.g, a red light can be stimulated if the floor is dicey or damp. Sensors can also be exercised to shelter entrée to FDA controlled narcotics, hazardous drugs and products. This can also look after meddle with medicine, scam in recommendations or assault by a peeved staff or patient. Exterior aspects that preserve constructing jeopardy are expulsion of power outages, biological agents, or electromagnetic molests. Sensors can also be brought into play to lend a hand in determining validation of a healthcare supplier who is sanctioned and refute entrée to others. Communication patterns with the patient can be appraised. Every offensive pattern/prototype of actions such as not retorting to patient requests can be shunned. For the protection of person and visitors alongside malevolent bustle and movement, sensors can also provide such support all the way through an automated sensor-based network.

5.3 Patient's Room Security

For monitoring entrance and access to patient's room a sensor can be brought into play. Frequency of communication and the periods of in and out movement could be kept under observation. The outline of action in a patient's room with respect to the patient's schedule of medicine, devices linked to the patient is capable of endowing with a constructive tool to guarantee patient protection and Intravenous supervision. Patient can also be sheltered from pass over, ill-treatment, damage, fiddle, and unintentional movement of the patient external protection region. Sensors are capable of brought into play for patient classification band for the movement. Sensors can also be affixed to visitor's hospital outfits to pledge deterrent dealings.

6. SECURITY APPRAISAL

The protection and safety measures/appraisal of the medical care/heed environment ought to be appraised and put a figure on. This is imperative if a programmed sensor based environment is brought in hospitals. Several recommended appraisals are:

-Incorrect information, data values, misplaced or deferred messages

-Break down of machinery such as controllers, sensors, network, computers, smoke detectors, pagers, fire alarms.

-Number of confrontations per day in patient room, ward, or hospital

- Truthfulness, aptness, exactitude, and other excellence of service strictures.

-Calls to doctors and nurses that are not remedial crisis's, but may possibly be due to break down, collapse, or infringement in the sensor network

7. RESEARCH PROSPECTS

To bring sensors into play for monitoring/supervising entails study in database systems, security, energy aware computing and communication. In security [24] [25] working on jam resistant antennas. [3] Working on fault tolerant authentication, [26] on denial of service attacks and privacy and anonymity issues. In communications, researchers are investigating communication delays, bandwidth utilization congestion. So far database systems are concern so studies are underway on data aggregation techniques such as pattern matching, summarization, energy saving query processing and integrity checking [27]. Research is in progress on compilation and communication techniques in energy aware computing. In the near future we will try to explore upon these areas and expands results that can direct to a sheltered sensor based wireless network for medical care/heeds.

7.1 Fault-Tolerant Validation

Each and every sensor is ought to validate/authenticate with the controller "base station" prior to the data received can be utilized so-called fault tolerant validation. A back-up controller in the immediate/pressing/instant neighborhood can authenticate/validate the sensor's signals and data incase of controller breakdown. A pecking order of base stations is possibly utilized for validation. A virtual controller is required in first scheme that holds primary and back-up controllers. Manifold keys will be obligatory for the hierarchical format. [2] Has been presented the design analysis and experimental evaluation.

7.2 Smart and Jam Defiant Antennas

Well-groomed antenna scheme has been presented in [3]. Information can be transmitted unvaryingly in all directions by means of Omni directional antenna. There is no chance for broadcasting of neighboring devices concurrently because it can cause overcrowding. The transmissions facilitate rivals to spy/snoop the communication, examine the pattern of the traffic, and position the dispatcher. One way out to the dilemma is the practice of smart antennae [3] In view of the fact that transmissions are directed, remote stations can be attained with inferior power utilization, and snooping turns out to be more knotty. Manifold sub-antennas and switches consist by a smart antenna. Several forms of Smart antennae are on hands [28] phased-array, adaptive array and sectorized. Phased-array antennae can maneuver a focal lobe in whichever direction, but are not proficient of forming premeditated nulls. Adaptive arrays can shape not only manifold main lobes, but also steerable nulls in the direction of interferers [28]. Sectorized antennae consist of individual sector elements intended in dissimilar directions, where merely one sector at a time is energized with Radio Frequency (RF). Beam can also be directed in a specific direction by using switch. It enhances safety measures and save power. A number of antennas on manifold devices can be communicating with devices in diverse directions. One more plan is the utilization of jam resistant antennas. The idea is to bring into play two antennas on each device and utilize polarization in a way to entertain signals from single direction. The achievement of the semi-blind technique "cross relation scheme and utilization of the training sequence" and a method based only on the training sequence has been demonstrated. The simulation illustrates that sequence-based training-based act upon superior [24] One can exercise semi-blind or blind algorithms for channel assessment as long as there are two discrete antennas on hand having either significant spatial separation for diversity sake or dissimilar polarizations The notions of channel assessment and equalization for GSM with manifold antennas are outlined in "VTC, 1999".

7.3 Confidentiality and Ambiguity

Confidentiality/Privacy concerns turn out to be very significant when an outsized hospital and all its maneuvers are being supervised by sensors. The Ambiguity/anonymity of the source of supervising data and the position of the sensor calls for fortification/safety from illicit entrée. In view of the fact that sensors will be organized in hospital wards/clinics, rooms, and attached to hospital personnel, the confidentiality concerns and bogus classification of misconduct calls for additional study. The medical care/heed suppliers have to shelter health information as mandatory by HIPPA rules. The patient's right to request a constraint or restriction on the revelation of protected health information (PHI) for the rationale of healing, monetary accountability, or health care/heed operations are supposed to be retained.

7.4 Energy Preservation

The sensor may possibly be in snooze mode or vigorous mode for energy conservation. The communication and computation by each sensor has to be vigilantly controlled. Given that sensors can be component of a direction to the controller, the routing systems calls for energy efficiency. If the data from preceding sensors desires to be cumulative or patterns require to be acknowledged, the algorithms obliged to be work out to diminish computation as discussed in [10] [27].

7.5 Denial of Service Assaults and Intruder Detection

Sensors and controllers communication may possibly influenced by denial of service attacks [26] set off by an interloper/Intruder. Instances comprise malevolent device flooding, imitation, gang assault where manifold devices either play up or deliberately generate a tortuous conduct. At controlling device the supervision of superiority of data and patterns can make out the attack/assault and the impostor too. Black lists and Mistrust lists can be fashioned to pay no heed to sensors concerned in denial of service attack/assault [29].

8. REFERENCES

[1] Introduction to Wireless and Mobile Systems. Brooks/Cole Thompson Learning, 2002.

[2] Fault Tolerant Authentication in Mobile Computing" , International Conference on Internet Computing, June 2000.

[3] Smart antenna for handsets. DSPS Fest, 2000, ''Security Flaws in 802.11 Data Link Protocols," CACM. May 2003.

[4] Advances in Distributed Sensor Integration: ''Applications and Theory''. Prentice Hall, New Jersey, 07458, 1995, pp. 273.

[5] Tennenhouse, ''Embedding the Internet: Proactive Computing''. Communications of the ACM. Vol. 43, No. 5, pp. 43-50, 2000.

[6] SPINS: ''Security protocols for sensor networks''. 7th Annual International Conference on Mobile Computing and Networks (MobiCom), pp. 189-199. 2001.

[7] ''Protein Microarray Fabrication for Immunosensing''. 224th American Chemical Society (ACS) National Meeting, Aug. 2002.

[8] Top Down'' Protein Characterization by Tandem Mass Spectrometry." Journal of Mass Spectrom. 2002, 37, pp. 663-675.

[9] ''Integrated Detection of Hazardous Material'', Proceedings of American Physical Society, 2003.

[10] ‘’Distributed Sensor Networks.’’ CRC Press, Inc. 2003

[11] Estrin, ’’Instrumenting the World with Wireless Sensor Networks (WSN)’’ (ICASSP 2001) International Conference on Acoustics, Speech, & Signal Processing, Utah, May 2001.

[12] Khan,’’Emerging Challenges: Mobile Networking for Smart Dust’’, (IJCN) International Journal of Communication Networks, Vol. 2, No. 3, Sept. 2000.

[13] Khan, M, ’’Next Century Challenges: Mobile Networking for Smart Dust’’, Mobicomm 99, 1999, pp. 271-278.

[14] Kulik, ‘’Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks,’’ Wireless Networks, Vol. 8, 2002, pp. 169-185.

[15] Krishnamachari, ‘’The Impact of Data Aggregation in Wireless Sensor Networks (WSN’s)’’ International Workshop on Distributed Event Based Systems (DEBS), Austria, 2002.

[16] Iyenger, ‘’Computational Aspects of Sensor Networks’’, I-SPAN’02, May 2002.

[17] Meguerdichian,’’Localized Algorithms in Wireless Ad-hoc Networks: Location Discovery and Sensor Exposure,’’ MobiHOC, 2001.

[18] Park, ‘’Simulating Networks of Wireless Sensor Networks,’’ Winter Simulation Conference, 2001.

[19] Schurgers, ‘’Topology Management for Sensor Networks: Exploiting Latency and Density,’’ ACM MobiHOC 2002.

[20] Doherty, ‘’Energy and Performance Considerations for Smart Dust.’’ International Journal of Parallel and Distributed Systems and Networks, Vol. 4, No. 3, 2001.

[21] Warneke, ‘’Smart Dust: Communicating with a Cubic Millimeter Computer’’, 2001.

[22] Housley, ‘’Security Problem in 802.11 based networks,’’ CACM. May 2003.

[23] Zoltowski, ‘’Jam-proof Area Deniable Propagation: Anti-jam Protection for GPS via Robust, Computationally Efficient Space-time Adaptive Processing. Technical Report, 2000.

[24] Xu, ‘’Diversity Assisted Channel Estimation and Multiuser Detection for Downlink CDMA with Long Spreading Codes’’, IEEE Transactions on Signal Processing, 2003.

[25] Habib, ‘’Detecting Service Violations and DoS Attacks’’, NDSS '03, San Diego, Feb 2003.

[26] Khan, ‘’Self-configuring Node Clusters and Data Aggregation in Micro-sensor Networks.’’ Technical Report, College of Computing, Purdue University, July 2002.

[27] Zoltowski, M. Recent advances in reduced-rank adaptive filtering with applications to high-speed wireless communications, Conference of the International Society for Optical Engineering, 2001.

[28] Wang, ‘’Intruder identification in Mobile Ad Hoc Networks.’’ Conference on Pervasive Computing, Dallas, IEEE, 2003.