2012 International Conference on System Engineering and Modeling (ICSEM 2012)
IPCSIT vol. 34 (2012) © (2012) IACSIT Press, Singapore

Using Wireless Sensor Networks for Managing Telemedicine Applications

Adnan .I. Al Rabea

Prince Abdullah Ben Ghazi College for Science and Information Technology
Al Balqa Applied University, Al Salt, Jordan
E-mail: adnan_alrabea@yahoo.com

Abstract. One of modern telecommunications and information technologies is Telemedicine that now used to provide a clinical care and help to many peoples that located at a distance, and to encourage the transmission of information needed to supply that care. The telemedicine can be sub-divided into 'live' and 'store-and-forward'. Live telemedicine needs both parties at the same time using audio-visual communications over high-bandwidth and so low-latency connections. Nearly all specialties of healthcare are able to make use of this kind of consultation. There are many circumferential devices which Linked to computers as aids to a reactivate examination. On the other hand, Store-and-forward telemedicine included the acquisition of data, images and/or video content and transmission to a medical specialist at an appropriate time for estimate off line. In this paper, we Sheds light on managing the wireless sensor networks in telemedicine applications. There are many management tasks that are reported covers: topology management, privacy and security issues in WSN management, topology management algorithms, and route management schemes. The major design issues facing WSN management was touched in a separate section.

Keyword: WSN, IATV, MRI, ECG, CT.

1. Introduction

1.1. Telemedicine and Its Relationship to Wireless Sensor Networks

The advances in the growth of medical sciences, biomedical engineering, communications and information technologies have enabled the growth of telemedicine to provide effective, efficient and improved health care. Medical care generally relies on the face-to-face encounter between patients and doctors. In places where face-to-face encounters are not possible telemedicine links are relied upon to link patients to specialist doctors for consultation for obtaining opinion. The advantages of telemedicine is in providing improved health care to the underprivileged in inaccessible areas, reduce cost and improve quality of health care and more importantly reduce the isolation of specialists, nurses and allied health professionals.

The term telemedicine refers to the use of telecommunications and computer information technologies with medical expertise to facilitate remote health care delivery, medical services to remote areas or across great distances on the globe. It also covers any form of communication between health workers and patients through electronic equipment from remote locations. Telemedicine applications are either based on store and forward or two-way interactive television technology. The store and forward method is used for transferring medical data and digital images from one location to another. Medical data like ECG, heart rate, oxygen saturation, respiratory rate, blood pressure, etc., and images like CT, MRI, ultrasound, etc. Two-way interactive television (IATV) is used when there is a need for a 'face-to-face' consultation between the patient and specialist doctor in another location. In telemedicine, a typical scenario is two doctors are involved with the patient: a local attending doctor and a remote tele doctor who is engaged to do one or more of a variety of services ranging from tele-consultation, or performing a tele-surgery, as well as tele-diagnosis where a doctor tele-diagnoses a sickness. The recent advances in telemedicine applications are propelled by two converging trends, which are the advances in Internet and telecommunications technologies and the increasing demand for access to high-quality medical care irrespective of location or geographical mobility. Wireless telemedicine is a new and evolving research area that exploits recent advances in wireless telecommunication networks.

The conventional telemedicine systems using the public switched telephone network (PSTN) and Integrated Services Digital Network (ISDN) are available for doctors to deliver the medical care and education remotely. The introduction of wireless telemedicine systems will provide further flexibility, wider coverage and new applications for telemedicine. The wireless telemedicine systems can provide better healthcare delivery, regardless of any geographical barriers, time and mobility constraints.

A wireless sensor network (WSN) is a communication network composed of wireless sensor devices. These devices essentially are low cost, low power, multi-functional, small sized and communicate over short distances [6]. Typically these devices serve as nodes in a wireless network and are deployed randomly in a given area. Nodes establish connectivity with each other dynamically after deployment and do not follow a pre-determined topology. Therefore WSN are self-organizing in nature and are suitable for military surveillance, control communication and monitoring disaster areas. One application of WSN is in remote healthcare monitoring of patients. Wireless Sensor nodes are placed on patients and thus acquire critical data for remote monitoring by health care providers. Significant amount of research has been done in the area of Wireless Body Area Sensor Networks (WBASN) with many researchers proposing various types of sensor nodes.

Wireless sensor networks (WSN) consist of many small sensors that are limited in resources, particularly processing power and battery life. These networks are used in many different applications, including environment sensing, military scenarios, habitat monitoring, structure monitoring, and first responder situations. There are many challenges associated with sensor networks but the primary challenge is energy consumption. Sensor networks are typically have little human interaction and are installed with limited battery supplies. This makes energy conservation a critical issue in deployed WSNs. All types of networks require monitoring and maintenance. A service that supplies a set of tools and applications that assist a network manager with these tasks is network management. It includes the administration of networks and all associated components.

While all networks require some form of network management, different types of networks may stress certain aspects of network management. Some networks may also impose new tasks on network management. There are different types of network management architectures: centralized, hierarchical and distributed. In a centralized approach, one central server performs the role of the network management application. A hierarchical architecture will include multiple platforms, typically one server and several clients, performing network management functions. This type of architecture helps to distribute the functions thus eliminating the bottleneck at the one central server. In order to distribute network management functions even more would be to move to a distributed architecture. This type of network management architecture utilizes multiple peer-to-peer platforms sharing all management tasks. This provides better scalability, availability, reliability and modularity.

2. Wireless Sensor Networks Structure

Wireless sensor networks (WSNs) have promised us a new monitor and control model over the distributed computing environment. In general, these networks consist of a large number of sensor nodes densely distributed over the region of interest for collecting information or monitor & track certain specific phenomena from the physical environment. As shown in Fig.1, each sensor node is typically battery-powered, and consists of a processor, sensor, transceiver and other modalities. As sensor nodes are always designed with small dimensions, the size imposes restrictions on its resources (e.g. energy, communication, and processor capacities), and consequently limits sensor nodes to undertake too much complex tasks.

Management of WSNs is a new research area that only recently started to receive attentions from the research community. It has already presented a set of significant management challenges. The operation of a WSN is greatly affected by different inter-related factors such as network traffic flows, network topologies, and communication protocols. The interactions among those factors are still not clear yet. The environment also imposes a deep impact on the wireless network performance. As a result, the unique features of WSNs make the development of management architecture significantly different enough from traditional computer network.

This paper summarizes some unique features, which are most likely to be considered in design of management architecture in WSNs. Also, this paper highlights some management features from current state of researches, which support WSN operation in various aspects.

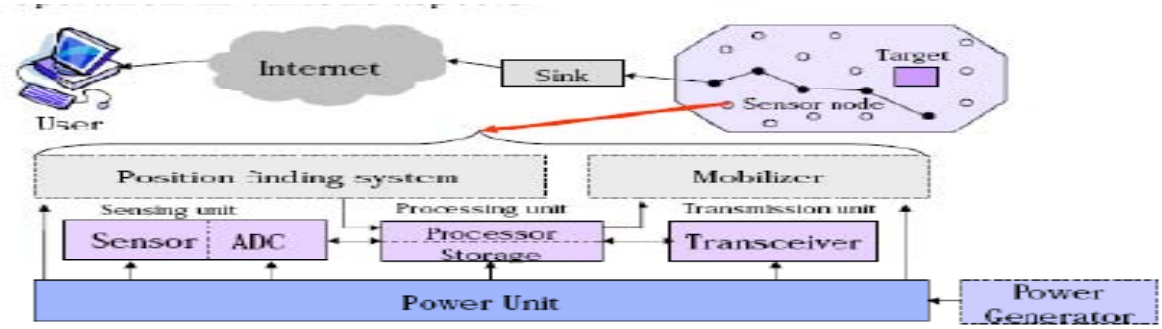

Fig1. The structure of sensor nodes.

3. Network Management Functionalities

3.1. Traditional networks.

Network management of traditional, wired networks includes five functional areas, as identified by the International Standards Organization or ISO. These five areas are: fault management, configuration management, security management, performance management and accounting management. Fault management deals with the process of finding problems in the network. This process involves finding the problem, isolating the problem, and fixing the problem if possible. Faults should be reported in some manner, such as a log file, E-mail message to the network manager, or an alert on the network management system.

The process of setting up, monitoring and controlling network devices is configuration management. An inventory of all network devices should be maintained which should include the current configuration of each device. The information about the current network environment should be collected on a periodic basis, either manually or automatic. Reports should be generated that includes this information. A common collection method is called auto discovery, which is a process that runs on a network management system and will detect all installed network devices and possibly their current configuration.

3.2. Sensor networks

Network management in sensor networks is comparable to traditional network management. Sensor network management will include the five functional areas identified by ISO, although perhaps in a different manner. For instance, performance management would also include monitoring to ensure network coverage and connectivity. Security management in sensor networks is difficult due to the ad hoc nature of these networks, the use of wireless communication and the inherent resource limitations of the sensors.

One primary goal of network management in sensor networks is that it be autonomous. This is especially important in fault and configuration management. Configuration management includes the self-organization and self-configuration of the sensor nodes. Since WSNs involve very little human intervention after deployment, it is imperative that the areas of fault management be self-diagnostic and self-healing. Another important issue to consider in fault management of WSNs is that a single node failure should not impact the operation of the network, unlike a traditional network device failure causing impact to several users to potentially the entire network.

There are several new functional areas of network management in sensor networks. These new functional areas introduced for network management of WSNs are topology management, energy management and program management. One of these jobs is energy management. Recall that energy conservation is a critical aspect of sensor networks. Saving energy can be done at many different levels and in many different ways and is thus a separate area of network management. The most common way to conserve energy in WSNs is to power off a node when idle, but there have been many proposals in existing algorithms and protocols as well as establishing new protocols in order to be more energy efficient.

4. Network Management Models And Types.

4.1. Topology management

There are three basic ideas of topology management in WSNs: topology discovery, sleep cycle management, and clustering. According to [33], there are six properties that should exist in the topology of WSNs: 1) symmetry, 2) connectivity, 3) spanner, 4) sparseness, 5) low degree, and 6) low interference. Consider two nodes in a WSN, x and y. If the network is symmetric, then x is a neighbor of y and vice versa. Two nodes in a network are connected if there is a path, which may be multiple hops, from one node to the other.

4.2. Topology discovery

Topology discovery involves a base station determining the topology or organization of the nodes in the sensor network. The physical connectivity and/or the logical relationship of nodes in the network are reported to the management station which maintains a topology map of the WSN. The base station or network management station will send a topology discovery request to the network. The nodes in the network will respond with its information. There are two basic approaches taken for topology discovery. The first one is a direct approach. In this approach a node will immediately send a response back upon receiving a topology request. The node's response will contain information about that particular node only. The other approach is an aggregated approach in which a node will forward the request but will not respond immediately.

4.3. Sleep cycle management

Another idea of topology management is to eliminate redundancy by allowing some redundant nodes to sleep for periods of time. Topology management protocols are used to manage the sleep-wake cycle for nodes. The goal is to conserve energy in each node while continuing to maintain network connectivity. One disadvantage of most sleep cycle management protocols is that many of them trade routing latency for energy conservation. There has been research on the possibility of turning off nodes at the MAC layer when the radio is not being used. Other algorithms have been developed to conserve energy but rely on location or geographic information.

5. Privacy and Security Issues in WSN Management.

In a healthcare monitoring system security of data is of utmost importance. From acquiring data from medical measurement sensors, to data transmission over a network, to the data storage and analysis, patient data needs to be protected at all stages. It is therefore important to secure data at physical layer from signal jamming and noise, network layer from routing errors and denial of service and at application layer from unauthorized data manipulation of patient records . A security consideration for the proposed system in was classified to three levels of implementation as follows:

5.1. Data privacy at acquiring level (Non invasive)

At this level the Sensor nodes would acquire medical measurement and send these data to the sink device (SD). Also if there is any data to be sent to any of the sensor nodes such as configuration settings for a sensor, it can be done at this level. Any data that has been acquired must be done in a non-invasive manner and must not be accessed by sensor devices on a different user. This can be achieved by authentication at the MAC layer level for a particular user. When the WSN is deployed all sensors can be identified and their distinct MAC addresses stored in the sink device. Whenever a sensor needs to send some data it can request connection by sending a request with its own MAC address. The sink device can identify the incoming request by matching MAC address with the ones stored in its memory.

5.2. Data security at transmission level

At this level all data collected by the SD and is ready to be transmitted was assumed. A users SD is assumed to be roaming in a foreign network and therefore needs to connect to the healthcare provider's device (HD) by either accessing the Home Authentication Server (HAS) or the Foreign Authentication Server (FAS) depending on its current location, either in home network or a foreign network. In either case it will authenticate with the required server using a challenge/ response mechanism by encrypting all correspondence with mutual sharable keys. If the HD allows the user to be registered it will authenticate the session for further data transmission. Figure 2 shows the proposed model.

5.3. Security areas in transmission

In the proposed model, a patient is considered to be moving from an area to another physical locality. Therefore a route needs to be established to the healthcare provider's locality. Two cases for providing security in home service were considered, when the user is part of the same network as healthcare provider; and Foreign Service, when the user is the part of a different network as of the healthcare provider.

5.4. Security in home service

In this scenario the user is part of the same network as of the healthcare provider. To initiate the service user needs to authenticate himself with the home authentication server by sending a service request. The local Cell Access Point (CAP) would forward the request to the Home Authentication Server (HAS). The

HAS would generate a challenge request for the user . The user will respond to the request, the HAS would authorize access only if the challenge/response mechanism succeeds as shown in Fig.2b. When authenticated the user can establish connection with the healthcare provider.

5.5. Security in foreign service (Phase:I).

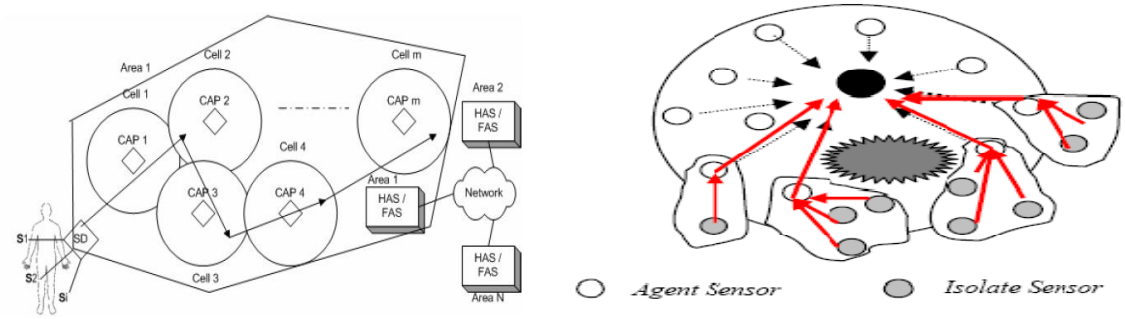

Fig. 2 Secured System Models, HAS: Home Authentication Service, FAS: Foreign Authentication Service, CAP: Cell Access point, S1..Si are Sensor devices, SD- Sink Device Arrows show movement direction.

In this scenario the user is not a part of the same network as of the healthcare provider possibly because the user has moved to a different location. A secure route needs to be established for communication to the healthcare provider. For seamless connectivity a Foreign Authentication Server (FAS) exists which provides challenge response condition on behalf of the HAS was assumed. User sends a request to the local CAP which in turn forwards the request to the FAS.

5.6. Security in foreign service (Phase:II)

When the user is authenticated by the healthcare provider a registration and authorization response is generated for FAS. FAS would then send the approval to the user and a secure connection is established.

6. Challenges And Design Issues

The primary goal of many WSN protocols and algorithms is energy conservation. This is true of topology management algorithms. Energy conservation is one of many design goals that should be considered when designing or evaluating topology management algorithms. Along with conserving energy among the nodes, the algorithm should minimize the energy required for running. While doing this, another primary goal is to maximize the network lifetime. Many times these two goals work concomitantly .If the algorithm can be distributed and not centralized, it would be beneficial. This would lessen the communications required. Also, there are often multiple sinks or base stations, so nodes only have to communicate with the closest one. Having a centralized solution might require some nodes to communicate long distances.

The maintenance overhead of the algorithm should be kept to a minimum. This would require less energy consumption for the algorithm. It would also require less processing power, which is often limited as well in sensor nodes. If the algorithm can be developed requiring no location information or time synchronization, that would be advantageous. Requiring such information again requires additional communication. The protocol or algorithm should be developed so it is robust to node mobility and node failures. Many applications or sensor node deployment have node mobility; some by design and some just by the nature of the application (nodes may shift or move accidentally. WSNs are prone to node failures. This may be due to running out of energy, hardware failures or simply the node being destroyed due to harsh conditions. The algorithm will be more successful if it is robust to node failures.

7. Conclusion

Network management is a critical function in all types of networks. In a traditional wired network, network management is typically a centralized architecture with a primary server controlling most network management functions. There are five primary functional areas of traditional network management: fault management, configuration management, security management, performance management and accounting management.

Wireless sensor networks are networks consisting of many sensor nodes, which are constrained by power and energy. Network management is critical in WSNs but is more practical implemented as a distributed architecture, with different tasks being performed by different nodes in the network. There may still be a

primary base station or sink that collects and stores the network management data. The functional areas for network management in WSNs include the five functional area of traditional network management plus the following areas: energy management, program or code management, and topology management.

There are three primary tasks of topology management. These tasks are to determine the network topology, allow some nodes to sleep and management when nodes sleep, and cluster the nodes of the network. There are several existing algorithms that have been developed in each of these areas of topology management with research in each area ongoing.

8. References

[1] H S Ng et al,"Wireless Technologies for Telemedicine",BT Technology Journal,Vol 24 No 2,April 2006

[2] Poondi Srinivasan et al, "Store and Forward Applications in Telemedicine for Wireless IP Based Networks", Journal of Networks, Vol.2, No.6, December 2007

[3]B. Jeffrey and M. Ringel, "Telemedicine and the Reinvention of Healthcare", New York: McGraw-Hill, 1999.

[4] C. S. Pattichis, et al, "Wireless Telemedicine Systems: an Overview", IEEE Antennas & Propagation Magazine, vol. 44, pp. 143-153, 2002.

[5]S. Laxminarayan and R. H. Istepanian, "Unwired e-Med: The Next Generation of Wireless and Internet Telemedicine Systems [Editorial] ", IEEE Transactions on Information Technology in Biomedicine, vol. 4, 2000, pp. 189-193.

[6] A. Akyildiz et al, "A Survey on Sensor Networks", IEEE Communications, pp.102-114, August 2002

[7] http://www.sensatex.com

[8] K. M. Sungmee Park and S. Jayaraman. "The Wearable Motherboard: a Framework for Personalized Mobile Information Processing (PMIP).Proceedings of 39th ACM/IEEE Design Automation Conference, pages 170-, 2002.

[9] J. G. R. DeVaul et al "Mithril 2003: Applications and Architecture", 7thInternational Symposium on Wearable Computers, pages 4-11, 2003.

[10] J. E. T. Martin, M. Jones and R. Shenoy. "Towards a Design Framework for Electronic Textiles", 7th IEEE International Symposium on Wearable Computers, pages 190- 199, 2003.

[11] http://lifeguard.stanford.edu .

[12] S. Krco, V. Delic, "Personal Wireless Sensor Network for Mobile Healt Care Monitoring", Proceedings of IEEE TELSIKS 2003, Serbia Montenegro, pp.471-474, Oct 1-3, 2003.

[13]. G. J. Mandellos et al, "A Novel Mobile Telemedicine System for Ambulance Transport Design and Evaluation", Proceedings of the 26th Annual International Conference of the IEEE EMBS San Francisco, CA, pp.3080-3083, September 1-5, 2004.

[14]M. Rasid and B Woodward, "Bluetooth Telemedicine Processor for Biomedical Signal Transmission via Mobile Cellular Networks", IEEE Transactions on Information Technology in Biomedicine, Vol. 9, No. 1, March 2005.

[15] Mengjie Yu et al, " A Survey of Network Management Architecture in Wireless Sensor Network"www.cms.livjm.ac.uk/pgnet2006/Programme/Papers/2006-93.pdf

[16] Lisa Frye et all, Network Management of a Wireless Sensor Network www.lehigh.edu/images/userImages/jgs2/Page_7287/LU-CSE-07-.pdf

[17] J. E. López de Vergara et al "Semantic Management: Application of Ontologies for the Integration of Management Information Models". Proceedings of the Eighth IFIP/IEEE International Symposium on Integrated Network Management, Colorado Springs, Colorado, 24-28 March 2003

[18] X. Hong and Q. Liang. "An Access-Based Energy Efficient Clustering for ad hoc Wireless Sensor Network". 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2004.(PIMRC 2004). 5-8 Sept. 2004. Volume: 2. page(s): 1022- 1026.

[19] D.D.Kouvatsos, G. Min and B. Qureshi, " Performance Issues in a Secure Health Monitoring Wireless Sensor Network, www.comp.brad.ac.uk/het-net/tutorials/WP01.pdf

[20] J. Galego et.al. , "Performance Analysis of Multiplexed Medical Data Transmission for Mobile Emergency Care

over UMTS Channel," IEEE Transaction on Information Technology in Bio medicine, Vol.9, No. 1, pp.13-22, March 2005.

[21]. W. Stallings, Network Security Essentials, Applications and Standards,Prentice Hall, Upper Saddle River, NJ, 2000

[22] R. Rajaraman. "Topology Control and Routing in ad hoc Networks: a Survey". ACM SIGACT News. Volume 33 , Issue 2 (June 2002). Pages: 60 – 73.