Quick Prototying of Multifacete Interface for Healthcare Wireless Sensor Network

Rahul Dubey, Kalyani Divi, and Hong Liu

University of Massashusetts Dartmouth
Department of Electrical And Computer Enginering
285 Old Westport Road, North Dartmouth, MA 02740, USA
{rdubey,KDivi,hliu}@UmassD.edu

Abstract. This paper presents a quick prototyping of a mobile wireless sensor network (WSN) in healthcare applications that provides multiple interfaces with various access rights to different personnel involved in medical systems such as patients, healthcare providers, and system administrators. The prototype demonstrates a seamless access from constantly sensing patients' vital signs to long term medical records stored in central database. A quick prototyping approach facilitates communications and understanding of the system requirements among the stakeholders and is a cost-effective way to build a functioning massive ubiquitous healthcare infrastructure.

Keywords: Human-computer interface; Mobile Wireless Sensor Network (WSN); Healthcare Sensor Network (HSN); security and privacy of mobile and wireless systems.

1 Introduction

The National Vital Statistics of death rate in United States of America states that the two major causes of death are heart disease and stroke. According to it, the majority of the deaths due to heart disease were 26% and the Cerebrovascular diseases (stroke) were 23.1% [1]. To trim down the number of deaths due to heart disease, many measures were adopted. To comprehend about the ways and to improvise the quality of health care, Electronic Health Care system is introduced. Primarily, the system focuses on the elderly and physically disabled patients [2]. In the system, the doctors can follow the records of the patient and patient does not need to see a doctor whenever he/she requires doing so. In this kind of system, there is a very vast use of wireless sensor nodes. Wireless sensor network itself have very wide range of application. Sensor network, nowadays are very prominent in Surveillance, Health care, Traffic monitoring and Military. Sensor network has immense prospective in Medical Industry.

Many applications on wireless sensor networks (WSN) have been proposed, and medical healthcare is in particular interest of the nation. The first sensor network application designed for medical and healthcare industry is Codeblue [3]. Codeblue is for emergency medical care and is used to monitor a patient's heart rate, blood oxygen saturation as well as ECG through the use of Berkley MICA2 motes, a pulse oxygen meter, and an ECG mote. The vital signs from the patient can be either

Y. Cai et al. (Eds.): Mobilware 2010, LNICST 48, pp. 390–399, 2010.

transmitted via multi-hop communication to a wired base-station or to PDA devices carried by hospital staff or EMTs. The infrastructure incorporates routing, node naming and discovery. Codeblue uses an ad-hoc network to collect data from patients and then deliver the data to an information panel. However, security is not yet integrated. The researchers suggest using an ECC-based security protocol. The major drawback of Codeblue is its lack of security in its original architectural design.

Alarmnet [4] is another notable project that monitors assisted-living and residential patients. In terms of hardware, the infrastructure consists of several sensors (infrared, dust, integrated temperature, light, pulse, and blood oxygen), Star gateways, PDAs as well as computers. One of the major components of Alarmnet is the Star gateway, holding the code for the Alarm Gate module that handles most of the security functionality. The security services include the Secure Remote Password (SRP) protocol, authentication, and secure communication. It also takes care of message handling, query and report parsing, and database access. The main issue with Alarmnet is its platform-dependency.

Medical sensor network architecture called SNAP (Sensor Network for Assessment of Patients) [5] is proposed to address the security challenges of sensor networks. The infrastructure does not address routing, mobility or congestion issues. It deploys security mechanisms consisting of ECC-based secure key exchange protocol, symmetric encryption and decryption to protect data integrity, and two-tier authentication scheme using patient biometrics. SNAP uses two types of nodes: limited power node and unlimited power node. An unlimited power node would be active most of the times, and a limited power node goes into sleep state when inactive. Unfortunately, SNAP becomes ineffective due to its over-conservation of energy.

It is urgent to systematically address security issues in Healthcare Sensor Network (HSN) applications [6]. However, before a potential security mechanism can be integrated into a HSN, we must understand the measurement to assess and evaluate the security requirements and goals for the healthcare application and develop the architecture to house the security schemes/protocols. Divi et al have proposed a secure architecture for healthcare wireless sensor networks that put security in the design rather than patch work [7]. This paper shows a quick implementation that prototypes the architecture to demonstrate its feasibility and to study its efficiency.

2 Divi's Secure Architecture

In healthcare applications, sensor nodes are deployed to monitor patients and assist disabled. Our research is focused on designing a wireless sensor network that collects, transmits, and processes sensitive patient information for medical personals to monitor patients in real time. Since security is of significant challenge in transmitting data wirelessly and timely, we propose security architecture to support mobile healthcare infrastructure. Our approach is unique in that we place security in the center of the architectural design. The goals of our research are to

- Develop an architecture that positions security as a core component targeted to healthcare applications,
- Implement a security structure that provides low latency encryption and decryption, and
- Design security algorithms that are not resource intensive, permitting its deployment on sensor nodes.

2.1 Sensor Node Architecture

Our sensor node has five blocks: Controller, Sensors, Communication Device, Power Supply, and Memory. The sensors collect the data from the outside environment. The center component is the controller which processes the data (transfer data between a sensor and the memory as well as compute the data if necessary). The communication device transfers the data among the network. The Memory stores any short results or some important configuration information. The Power supply supports all these components. It is shown in Figure 1 below:

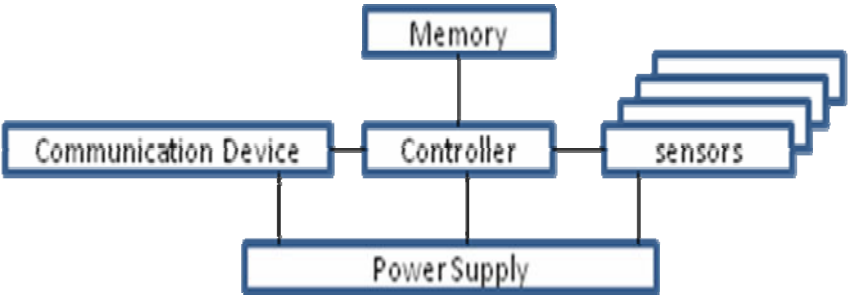

Fig. 1. Wireless Sensor Node Architecture

A wireless sensor network (WSN) has sensor nodes deployed in the environment strategically and communicating remotely as well as wirelessly to base station. Base station can be a router, a desktop, or another sensor node that communicates over the Internet to transfer data to different devices like PDA (Personal Data Acquisition) and laptops for data comprehension. For design considerations, the choice of base station effects cost and range of sensor node which in turn decides the structure of the network.

2.2 Patient Monitoring System (PMS)

The main design of the HSN architecture lies in the Patient Monitoring Network (PMN). The separate design of the PMN provides patient mobility. In the situations of emergency, the PMN can be set up in the ambulance and the aggregation node will be talking to the base station at the hospital. As the ambulance would be moving in and around the locations nearby to the hospital, the aggregation node can be maintained the same as for the body range. In the situations, like where a patient has to be monitored continuously, he can wear this PMN and keep contact with the base station even though he is moving around.

Our further research work has to be carried out on the choice of this aggregation node and the optimized design of a protocol so that this aggregation node utilizes less power. It makes the proposed architecture versatile in various conditions such as emergency or assisted living monitoring.

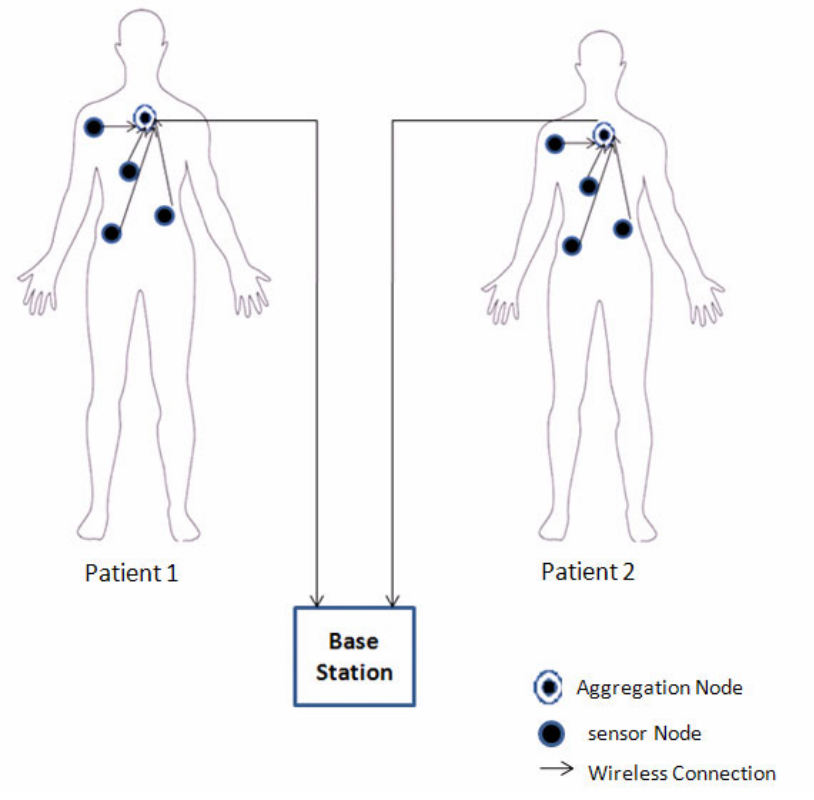

Fig. 2. Patient Monitoring Network (PMN)

2.3 Secure Architecture for HSN

In the secure architecture of a HSN, the PMN can be accessed in a variety of locations and each PMN has its own aggregation node identification. If the PMN is in the ambulance then the aggregation node uses the Internet or any WAN to transmit the patient data to the base station, which is (in most of the cases) located in the hospital. If the base station is in the hospital, then the aggregation node uses a LAN or a VPN to transmit the data. The base station collects information and stores in a database. In the database, each record might be stored with the aggregation node ID and patient ID for more confidentiality. Whenever a doctor or a care taker would like to go through the records of the patient, the doctor can access the data base directly using the local area network or VPN or directly access the database through the Internet.

The architecture shown is a three-tier architecture: Senor Nodes, Aggregation Nodes, and Base Station The communicating range of the sensor nodes is limited to body range, i.e., all the sensor nodes on the patient are always in the range of aggregation node by the patient body. The range of the aggregation nodes would be varying because it is the aggregation node that transmits the data to the base station.

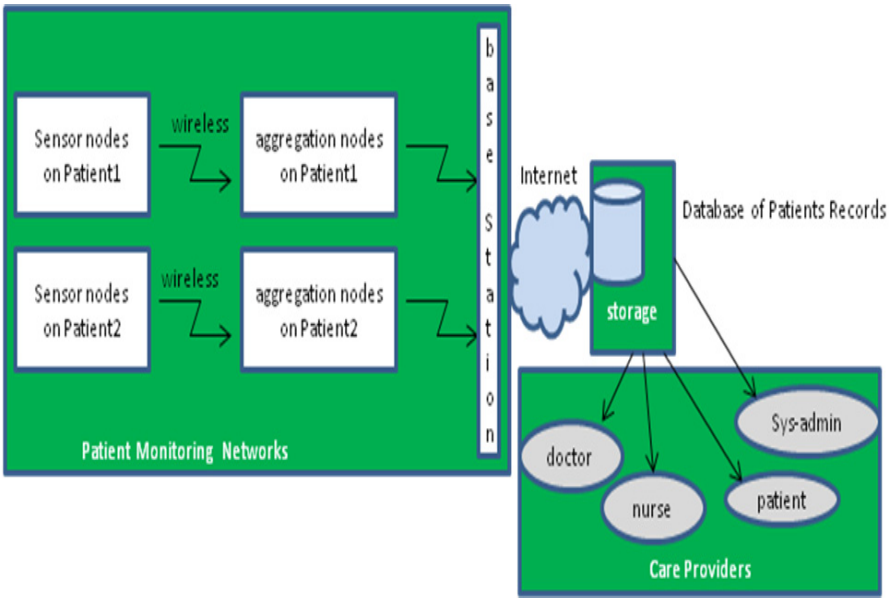

Fig. 3. Secure HSN architecture

Therefore, it is sufficient to have the aggregation node with varying range. The range of the aggregation node to the base station is local area for Region 1. For Region 2, the range for care providers would be wide area or via the Internet while Region 3 would be the databases. The secure architecture of HSN is shown in Figure 3.

The proposed architecture has many advantages when compared to the existing wireless sensor networks in healthcare application. As we have discussed in the state of art section, Codeblue, SNAP, and ALARMNET are the major existing wireless sensor architectures in healthcare sensor networks. Each of them does not include security in their architectural design; security is like an added-on feature. The proposed architecture has security built in it, and this comes with the features that the addition of aggregation node provides to us. The advantages of the proposed architecture over the existing architectures are:

- The architecture is designed for any type of application like for emergency purposes or assisted living and so on.
- The architecture has the security as a built-in feature rather than an additional feature.

3 A Quick Prototype

The main users of such system would be Care-Giver, patients and Administrators of the whole system. In the following approach the main concern is to make the health care system essentially mobile. Proceeding forward, system tries to focus on giving

privileges to the patients as well. Since foremost care seeker would be elderly and physically disabled person, so the system would be expected to have some kind of user interface where bedridden patient can see day to day reports of their health. Also, the system should allow them to make an appointment to the specialized doctors. At the same time, the proposed schema of the system is likely to provide the doctors to see the minute to minute updates of the critically unwell patients. According to the proposed health care system, the doctors can prescribe the patient if a doctor wishes to do so. To maintain functioning of the whole system, the administrator should be able to see the technical reports and the minute to minute update of each cluster. Administrator would be able to enable or disable any sensor node and that too wirelessly. To reduce the health casualties, the administrator should be able to track the sensor network traffic and can limit it. Chief issues that the administrator would deal with are interoperability of the network along with the data like personal information of the patient. The personal data would flow through the network. For this, the system should provide some kind of the security aspect so that the data can be encrypted and can travel through the network. The proposed system schema would be used by ordinary patient. Therefore, the primary concern of the design would be to make the user interface as uncomplicated as possible but, at the same time proficient.

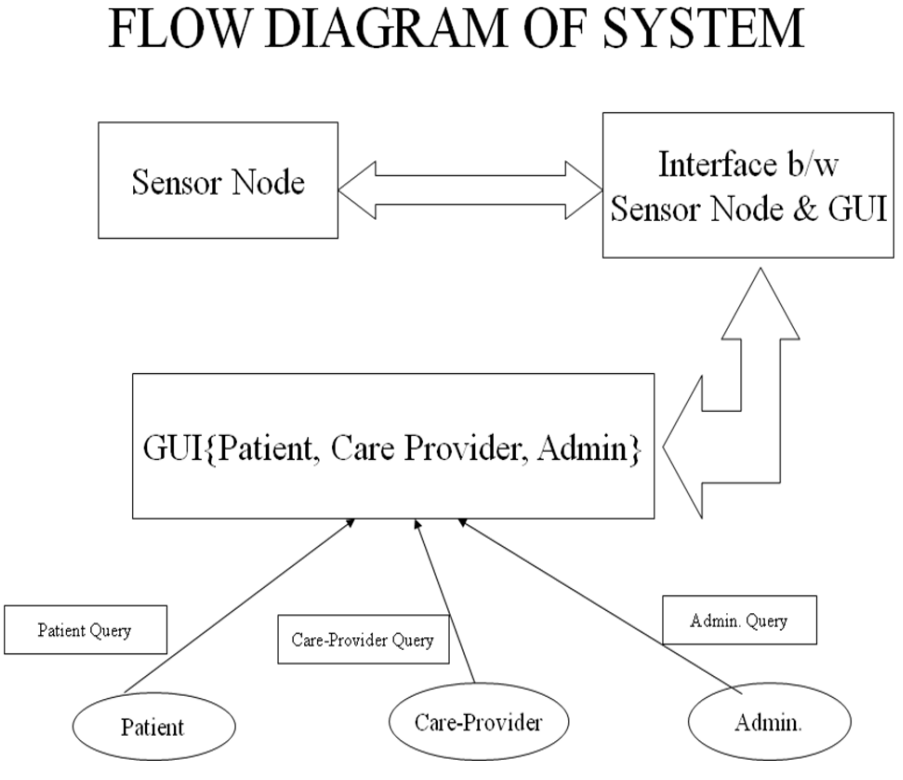

Fig. 4. Prototype Components

The anticipated scheme of the initial research-work allows clustering down the architecture. With the help of primary study and observation, we can think of three major sub-blocks- mainly the sensors (installed on the patient's body), GUI (user interface for the users of the system) and an interface (between the user interface and the sensors). The first task would be the collection of real time data from the sensor node and processing it at some base station. Then making the real time processed data readable to the user interface so that the users can easily read it. At transmitter end sensor node, the data has to follow some encryption method that allows secure data to stream across the network. At the user end, each patient and doctor would have their own login and password so that they can access their records only. To maintain the login, password details and to monitor the sensor nodes working, the administrator of the system would have access to the records.

- Data collection from Sensor nodes.
- Process entries at MOTE.
- Interfacing of MOTE and SQL server.

4 Our Proposed Workflow

In advancement of the initial studies, the workflow of the architecture would have a base station in between the user interface and the sensor nodes. The base station would be a programmable device which interacts with the sensors and the database server.

- Data collection from Sensor nodes.
- Process entries at a Base station; MOTE.
- Processing data at "TinyDB".
- Interfacing of "TinyDB" and SQL server.

The entire model provides an approach to make the health care system more secured and mobile keeping elderly and physically patient into consideration. The final outcome should provide a simple and operable user interface to the users and maintain the patients and doctor's data privacy and integrity. The proposed system should provide all the security requirements keeping all the data properties maintained. The model should provide the authentication at the time logging in and should be clear to read and understand by the patient and doctors. Model should be able to interact with the sensor nodes and should be able to communicate with the interfacing device, in this case MOTE. Along with this, the data streaming from the sensors should be able to follow the network protocols, as it would be flowing from one protocol to another.

Different users are presented with different interfaces. At the Log-In window as shown in Figure 6, user's credentials are checked, if user enters the correct login id provided manually/automatically to the user, a window will pop-up for the different type of function. Then the system gives different feature to the user; system would have different fields like foe patient, doctors, prescription and admin as shown in Figure 7. Here each tab would lead to a database where a record for each user is maintained. Figures 8 and 9 give the different user interfaces for patients verse doctors.

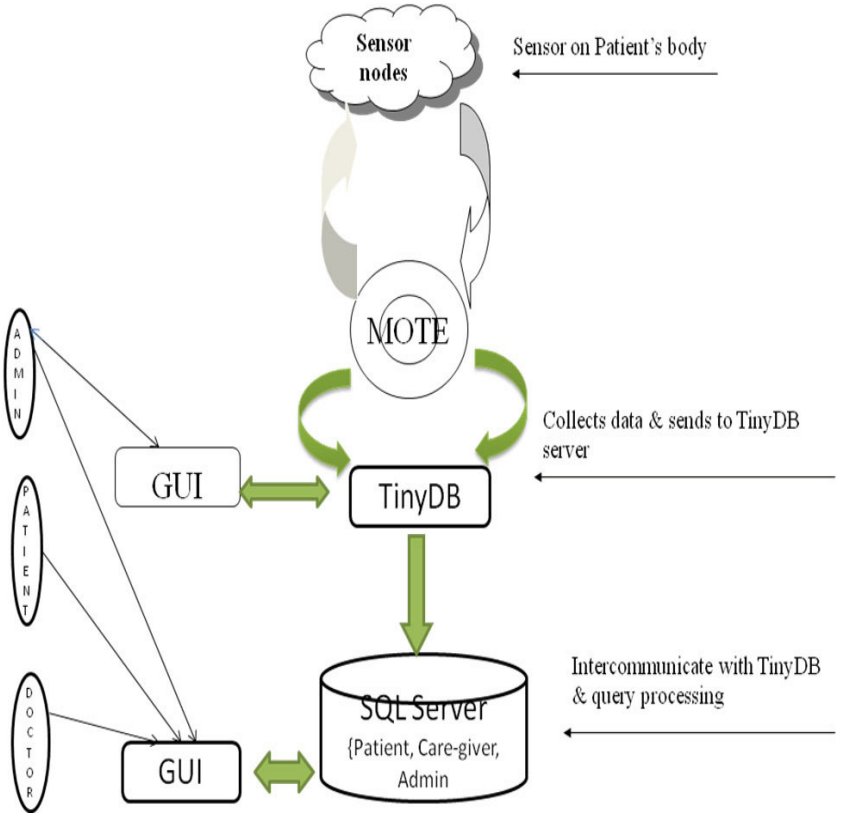

Fig. 5. Workflow Model

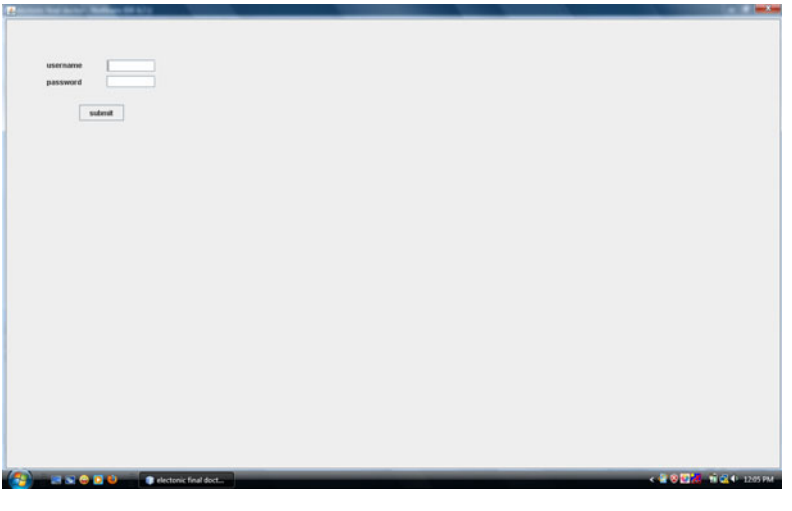

Fig. 6. Login In

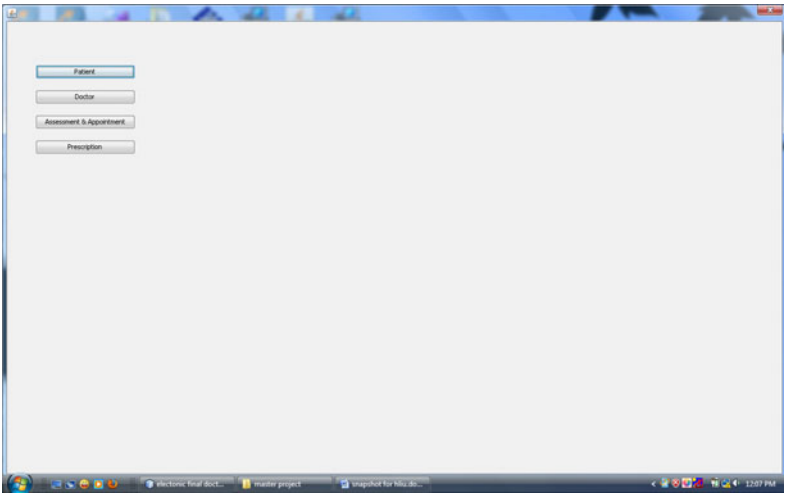

Fig. 7. Various User Interfaces

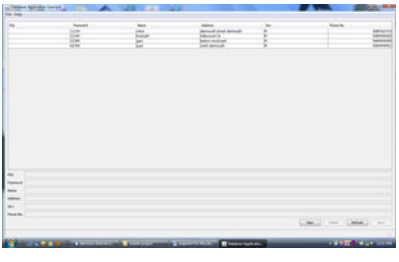

Fig. 8. Patient Interface

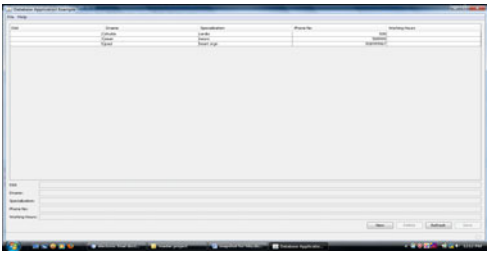

Fig. 9. Doctor Interface

5 Conclusion

This work demonstrates the feasibility of Divi's Secure Architecture for Healthcare Systems. Our further work includes validates the system's functionality and studies the efficiency issues.

References

[1] Lin, C.-C., Chiu, M.-J., Hsiao, C.-C., Lee, R.-G., Tsai, Y.- S.: Wireless Health Care Service System for Elderly With Dementia

[2] Gouaux, F., Simon-Chautemps, L., Adami, S., Arzi, M., Assanelli, D., Fayn, J., Forlini, M.C., Malossi, C., Martinez, A., Placide, J., Ziliani, G.L., Rubel, P.: Smart Devices for the Early Detection and Interpretation of Cardiological Syndromes. In: Proc. of the 4th Annual IEEE Conf. on Information Technology Applications in Biomedicine, UK

[3] Malan, D., Fulford-Jones, T., Welsh, M., Moulton, S.: Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In: International Workshop on Wearable and Implantable Body Sensor Networks (2004)

[4] Wood, A., Virone, G., Doan, T., Cao, Q., Selavo, L., Wu, Y., Fang, L., He, Z., Lin, S., Stankovic, J.: ALARM-NET: Wireless sensor networks for assisted-living and health monitoring, Technical Report CS-2006–01, University of Virginia (2006)
[5] Malasri, K., Wang, L.: Addressing security in medical sensor networks. In: Proceedings of the 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, San Juan, Puerto Rico, June 11-13 (2007)
[6] Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials 8(2), 2–23 (2006)
[7] Divi, K., Kanjee, M.R., Liu, H.: Secure Architecture for Healthcare Wireless Sensor Networks. In: Proceedings of the IEEE & ITSS Sixth International Conference on Information Assurance and Security (IEEE & ITSS IAS 2010), Atlanta, USA, August 23-25 (2010) (to appear in)
[8] Malan, D.J., Welsh, M., Smith, M.D.: Implementing public-key infrastructure for sensor networks. ACM Transactions on Sensor Networks 4(4), 22–45 (2008)
[9] Karlof, C., Sastry, N., Wagner, D.: TinySec: A link layer security architecture for wireless sensor networks. In: Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems, Baltimore, Maryland, USA (2004)
[10] Liu, A., Ning, P.: TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In: Proceedings of the 7th International Conference on Information Processing in Sensor Networks, April 22-24, pp. 245–256 (2008)
[11] Kurian, J., Sarac, K.: A security framework for service overlay networks: access control. In: BroadNets 2008, Internet Track 3: Overlays and Traffic Estimation, London, UK, September 8-11 (2008)
[12] Wang, Y., Ramamurthy, B., Xue, Y., Zou, X.: A key management framework for wireless sensor networks utilizing a unique session key. In: BroadNets 2008,Wireless Track 6: MAC and Key Management, London, UK, September 8-11 (2008)
[13] Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An architecture for differentiated services. RFC2475 (December 1998)
[14] Rajan, R., Verma, D., kamat, S., Felstaine, E., Herzog, S.: A policy framework for integrated and differentiated services in the Internet. IEEE Network, 36–41 (September 1999)
[15] Liu, H., Dempsey, H.H.: Multi-facet Internet resource management system. In: Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (IM), Boston, MA, USA, May 24-28 (1999)
[16] Yu, Q., (Liu, H., advisor): Denial-of-Service Countermeasure with Immunization and Regulation: Ph.D. Dissertation Dartmouth, MA: University of Massachusetts Dartmouth (2005)
[17] Ameen, M., Jingwei, L., Kyungsup, K.: Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of Medical Systems (March 2010)
[18] Dishman, E.: Inventing Wellness Systems for Aging in Place. IEEE Computer (May 2004)
[19] Tan, C.C., Wang, H., Zhong, S., Li, Q.: Body sensor network security: an identity-based cryptography approach. In: Proceedings of the 1st ACM Conference on Wireless Network Security, Alexandria, VA, USA, March 31-April 02, pp. 148–153 (2008)
[20] Karl, H., Willig, A.: Protocols and architecture for wireless sensor networks. Wiley, Boston (2007)