Wireless Sensor Networks In Health Care – an architectural approach

Sandor Rozsa, Vasile Teodor Dadarlat, Emil Cebuc
Technical University of Cluj-Napoca
sandor@net.utcluj.ro, vasile.dadarlat@cs.utcluj.ro, emil.cebuc@cs.utcluj.ro

Abstract

This paper presents best practices in wireless sensor network design for health care applications. Based on the most important aspects like power efficiency and security which guide the development of a wireless sensor network based e-health applications, we introduce novel system architecture for health care WSNs.

Keywords – wireless sensor networks, power efficiency, security, e-health

1. Introduction

Wireless sensor networks (WSN) represent a new research area. This domain is characterized by low computation power microcontrollers equipped with radio modules. The main usage domains of these systems are: monitoring of the industrial processes, environmental monitoring, military application, medical applications. In the area of wireless sensor networks for medical applications there are three main research directions: power consumption optimization, security method development for medical data transmission, management of the wireless sensor networks.

Power consumption reduction (power efficiency method development) is achieved by using stand-by methods and low power listening methods. The importance of the power consumption reduction is given by the fact of limited power resources (batteries) in each of the sensor motes, and the high cost of the battery replacement in wireless sensor applications.

The data transmitted on the wireless sensor network have to be secured. Security features like encryption and authentication must be provided. Wireless sensor networks with a huge number of components also need an active monitoring. The current tendency is to perform WSN monitoring using modular approaches.

There are several wireless sensor networks – health care projects worldwide: WBAN from University of Alabama from Huntsville [4], CodeBlue from Harvard University [5] , WSHM from University of Virginia[6][7].

This paper focuses on best practices in wireless sensor network development in an architectural approach and will present the proposed wireless sensor network architecture for health care applications.

Section 2 will present the theoretical background about power consumption optimization like “sleep mode“, and ADFC (Adaptive and Distributed Flow Control) with sleep mode [1] and security solutions [2] [3].

Section 3 will present the existing architectures of wireless sensor networks used in an e-health system [4].

In section 4 our proposed architecture will be presented, the architectural layers and the requirements which guided the architectural design.

Section 5 presents the next steps in the development process and conclusions

Section 6 lists the bibliographical references.

2. WSN optimization

There are several optimization directions in wireless sensor networks. In this section power efficiency methods and security methods are presented which guide the development of reliable, wireless sensor network based, e-health solution.

2.1. Power efficiency methods

Due to the fact that wireless sensor motes have limited power resources (batteries) power efficiency

optimization is required to maximize the lifetime and reliability of the wireless sensor network.
The general "sleep mode" [1] method is characterized by the existence of an "always power on" sensor node, the cluster head (CH). After a period of inactivity the RF (radio frequency) and computational circuits of the sensor motes other than CH are disconnected. CH is unable to initialize a communication channel to a sensor mote. There are two possibilities to create a sensor mote – CH bidirectional communication channel:

- Event based – initialized by data transmissions from sensor to CH. Data from CH to sensor does not initialize an event based communication channel.
- Periodical – permits the data transfer from CH to sensor when there are no data transmissions from sensor to CH to activate an event based communication channel.

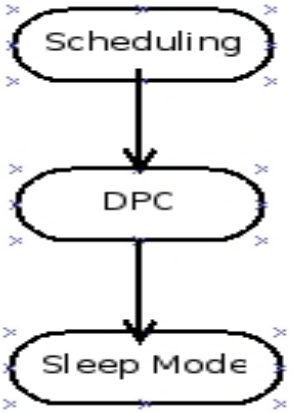

Figure 1.
ADFC with sleep mode

The ADFC (Adaptive Distributed Flow Control) method with sleep mode [1] defines a complex pattern using three sub patterns:

- Fair scheduling algorithm – the packets are classified according to the traffic flow to which they belong. Weights are fixed values. ADFS (Adaptive and Distributed Fair Scheduling – a QoS method based on CSMA/CA communication paradigm) is used as scheduling algorithm.
- Distributed power control – defines a four steps acknowledge method (ReSeT – ClearToSend – DATA – ACKnowledge). In this section are defined the physical parameters such like retransmission power of the control signals mentioned.
- Sleep mode method – defines sleep mode intervals and acknowledgment attributes.

Figure 1. presents the scheme of an ADFC method with sleep mode.

2.2 Security in wireless sensor networks

Security requirements in wireless sensor networks must comply with [2]:

Access control and message integrity – should prevent unauthorized parties from participating in the network. Nodes should be able to identify messages from unauthorized nodes.

Confidentiality – only authorized sensor nodes will be able to access data from the network. This requirement is achieved using encryption. Several encryption were adapted to wireless sensor networks such like RC5 or skipjack.

Protection against replay attacks – is solved using monolithically increasing counter with every message and reject messages with old counter values [2]. The replay attack protection is not scalable at the link layer. For this reason this is solved at the application layer using topological information and traffic pattern information.

As a conclusion to the security requirements presented we can affirm that a security solution for wireless sensor networks must provide both encryption and authentication. TinySec is a link layer security mechanism. Its packet format permits authentication and encryption. Figure 2-1 presents the TinySec-AE packet format - Data field is encrypted and uses MAC (Message Authentication Code). Figure 2-2 – TinySec-Auth packet format – uses MAC (Message Authentication Code). Figure 2-3 presents the TinyOS packet format – does not use encryption nor MAC.

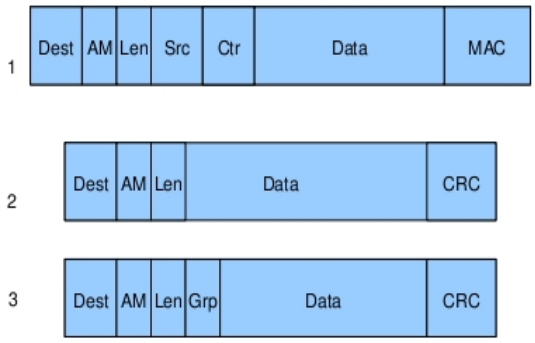

Figure 2. TinySec+AE (1), TinySec+Auth(2), TinyOS(3) packet format

3. WSN architectures for health care

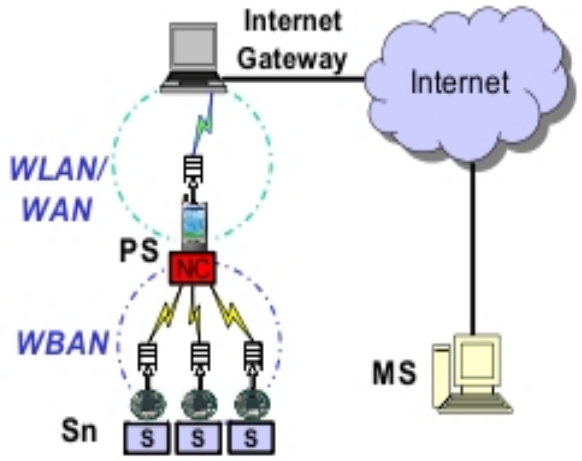

Figure 3. WBAN system architecture [4]

A WSN based e-health system architecture used in our system architecture development is presented in the WBAN project [4]. This architecture has 3 layers:

1. WBAN (Wireless Body Area Network) – at this layer are placed the sensor nodes interconnected with medical equipments
2. PS (Personal Server) – at this layer are placed data acquisition elements. Using this layer the WBAN and MS layers are connected. A PS application can be installed on PDAs or on mobile phones
3. MS (Medical Server) – at this layer are placed the medical data processing elements such like application servers, data base servers.

Figure 3 presents the WBAN (Wireless Body Area Network) system architecture [4].

4. Proposed solution

Our proposed solution is based on the WBAN architecture. Figure 4 presents the three-layered architecture of the e-health solution.

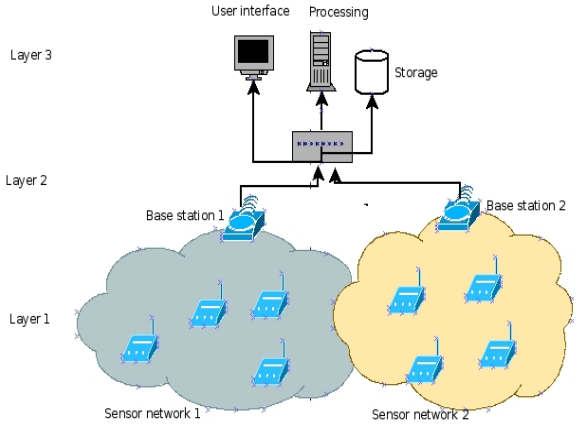

Figure 4. The proposed system architecture

Layer 1: sensor nodes layer

At this layer are placed the sensor nodes (Figure 5) connected with the medical equipments like electrocardiograms, pulse oxymeters, blood pressure meters. PAN (Personal Area Network) protocols will be used as link layer protocols (Bluetooth, IEEE 802.15, ZigBee). The sensor nodes will use an ADFC with sleep mode based solution for power saving. Because medical data are transmitted via the wireless sensor network a security solution have to be provided. The security solution will be based on TinySec+AE which permit both authentication and encryption.

Figure 5. An IEEE 802.15 sensor mote

Layer 2: interconnection layer

Base stations (BS) collect data from sensor nodes and transmit to the control and processing layer using LAN and WAN protocols. This layer consists of base stations and PAN-to-LAN or PAN-to-WAN converters (ZigBee to Ethernet Gateways, Bluetooth to Ethernet Gateways).

Layer 3: control and processing layer

Layer 3 contains the access, control and processing logic: medical storage servers, access control servers. Users will access the WSN based e-health solution through this layer. We intend to integrate at this layer a modular monitoring system for the wireless sensor network.

5. Future work

In this paper were identified the most important optimization directions in WSN infrastructures, and was described a novel architecture for a wireless sensor network based e-health system architecture.

Future work will contain the development of each layer from the proposed architecture presented in this paper. The first part of our research will focus on the implementation and adaptation of the presented power efficiency methods to our requirements.

The steps of the e-health system development process will be:

- Energy efficiency optimization of the wireless sensor network and development of the proper energy efficiency methods based on the requirements identified;
- Security method development for wireless sensor networks based on existing security methods, which will permit authentication and encryption;
- Modular management system development for wireless sensor networks;
- E-health data processing logic development.

6. References

[1] Jaganathan Sarangapani – Wireless Ad-hoc Sensor Networks – Protocols, Performance and Control, The University of Missouri Rolla, CRC Press, 2007

[2] C. Karlof, N. Sastry, D. Wagner – TinySec: A Link Layer Security Architecture For Wireless Sensor Networks, Sensys'04, November 3-5, 2004, Baltimore, Maryland, USA

[3] C. Karlof, N. Sastry, D. Wagner – TinySec: UserManual, http://www.cs.berkeley.edu/~ckarlof/papers/tinysec-user-manual.pdf

[4] E. Jovanov – Wireless Technology and System Integration in Body Area Networks for m-Health Applications, Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Shanghai, China, September 2005.

[5] D. Malan, T. Fulford-Jones, M. Welsh, S. Moulton – CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care, Internationa Workshop on Wearable and Implantable Body Sensor Networks, April 2004

[6] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T.Doan, Z. He, R. Stoleru, S. Lin, J. A. Stankovic – An Advanced Wireless Sensor Network for Health Monitoring, Transdisciplinary Conference on Distributed Diagnosis and Home Heathcare (D2H2), Arlington, VA, April 2-4, 2006

[7] J.A. Stankovic, Q. Cao, T. Doan, L. Fang, Z. He, R. Kiran, S. Son, R. Stoleru, A. Wood – Wireless Sensor Networks for In-Home Healthcare: Potential and Challenges, High Confidence Medical Device Software and Systems (HCMDSS) Workshop, Philadelphia, PA, June 2-3, 2005