31st Annual International Conference of the IEEE EMBS
Minneapolis, Minnesota, USA, September 2-6, 2009

Low-power Secure Body Area Network for Vital Sensors toward IEEE802.15.6

Masahiro Kuroda[1], Shuye Qiu[2], and Osamu Tochikubo[3]

Abstract— **Many healthcare/medical services have started using personal area networks, such as Bluetooth and ZigBee; these networks consist of various types of vital sensors. These works focus on generalized functions for sensor networks that expect enough battery capacity and low-power CPU/RF (Radio Frequency) modules, but less attention to easy-to-use privacy protection. In this paper, we propose a commercially-deployable secure body area network (S-BAN) with reduced computational burden on a real sensor that has limited RAM/ROM sizes and CPU/RF power consumption under a light-weight battery. Our proposed S-BAN provides vital data ordering among sensors that are involved in an S-BAN and also provides low-power networking with zero-administration security by automatic private key generation. We design and implement the power-efficient media access control (MAC) with resource-constraint security in sensors. Then, we evaluate the power efficiency of the S-BAN consisting of small sensors, such as an accessory type ECG and ring-type SpO2. The evaluation of power efficiency of the S-BAN using real sensors convinces us in deploying S-BAN and will also help us in providing feedbacks to the IEEE802.15.6 MAC, which will be the standard for BANs.**

I. Introduction

Recently wearable sensors and their short-range wireless communication technologies have been applied to preventive medical/ healthcare environments. However, these devices are, however, still big and heavy to wear, it is cumbersome to setup the network, and they are not compatible among their interfaces. Users at home are less likely to tolerate the inconveniences of today's medical/healthcare devices and their wireless interfaces. Common network interfaces are also not provided in the devices. There are standardization activities, such as Medical Devices WG in Bluetooth SIG [1] and point-of-care medical device communications in the ISO/IEEE 11073 [2]; however, these standards are not targeted for small vital sensors, but for medical/healthcare equipments in hospitals/at home.

This paper discusses and evaluates a secure body area network (S-BAN) optimized for small vital sensors. The S-BAN provides vital data ordering among sensors in the network. It also provides privacy in the wireless data transfer under limited power supply, such as a coin-size battery. The S-BAN is also expected to configure many sensors automatically in it and simple setup an interface for users. We begin this paper by the S-BAN MAC protocol, logical channel assignment, MAC frame, and application data representation. We then discuss less-power consumption for time synchronization between an S-BAN management node, called as a coordinator and sensors having different timer precision in hardware. We confirm the implementation of S-BAN on real sensors and evaluate the power-efficient timing synchronization. Then, we discuss the standardization towards IEEE802.15.6 MAC. We conclude with directions for further works.

[1]M. Kuroda is with National Institute of Information and Communications Technology, 4-2-1 Nukui-Kitamachi, Koganei, Tokyo,184-8795 Japan (e-mail: marsh@nict.go.jp)

[2]S. Qiu is with Dairix Corporation, 1-10-2 Isago, Kawasaki-ku, Kawasaki, 210-0006 Japan (e-mail: shuye.qiu@dairix-net.co.jp)

[3]O. Tochikubo is with Graduate School of Medicine, Yokohama City University, 3-9 Fukuura, Kanazawa-ku, Yokohama, 236-004 Japan (e-mail: tocchi@med.yokohama-cu.ac.jp)

II. Secure Body Area Network

An S-BAN is a privacy-protected short-range network of wearable/implanted vital sensors in the human body and it consists of a coordinator and sensor nodes, as shown in Fig. 1. The coordinator is a gateway enabling secure data exchange between wide-area networks and the S-BAN.

The coordinator collects vital data securely from sensors and uploads them to a wide-area network through a wireless link. Otherwise, it securely downloads instructions to a sensor node such as an actuator.

The S-BAN is dynamically configured when a sensor is powered on and is associates with the coordinator. The sensor is disassociated from the coordinator when the power is off.

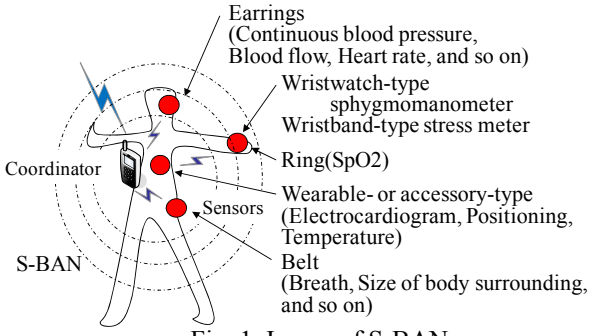


Fig. 1. Image of S-BAN

A. S-BAN Protocol Stack

An S-BAN protocol stack consists of three layers: the MAC security sublayer, MAC common part/management sublayer and PHY layer. The security sublayer is transparent to S-BAN applications via MCPS-SAP/ MLME-SAP interfaces (Fig. 2). Application data are protected by encryption and they prevent attacks using mutual authentication and fixed data size camouflaging.

The common part sublayer deals with data transfer and is expected to be simple and not have extra overhead in wireless communications. Once the S-BAN is configured using logical channels in the PHY layer, the MAC layer does not need to set addresses every time the sensor sends data. The address information is stored in the MAC information base (MIB) and reduces management works. The PHY-dependent information base (PIB) is also used to reduce the operations.

The S-BAN provides the semi-static configuration and the MAC, by default, is expected to ensure secure medical data transfer with less burden on sensor sides. The IEEE802.15.4 MAC [3], whereas, is flexible enough to represent various kinds of data transfer, such as CSMA/CA and TDMA.

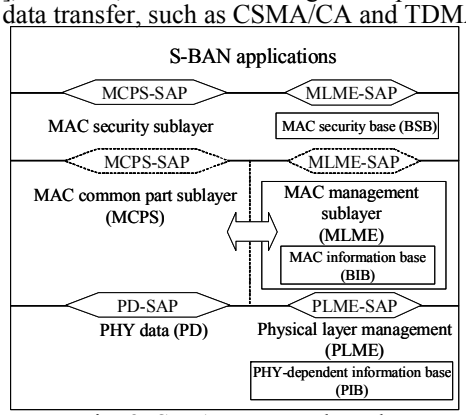


Fig. 2. S-BAN protocol stack

B. Logical Communication Channel

A coordinator and sensors are configured to have three logical conduits for different purposes of the MAC management: a random access logical channel (RALC), an MAC command logical channel (MCLC), and a data transfer logical channel (DTLC). First, a sensor registers itself with a coordinator via the common RALC and receives an acknowledgement with the data transfer timing and logical channel assignment from the coordinator (Fig. 3). Then, it sends vital data following the assigned time period to the coordinator via the DTLC. It does not wait for an acknowledgement from the coordinator. When the data transfer timing exceeds the assigned time duration, the sensor triggers a re-synchronization through the MCLC and adjusts the send-receive timing between the two. The trigger is generated by each sensor so as not to enter into the data receiving mode (RX), since the power consumption is proportional to the receive-wait duration.

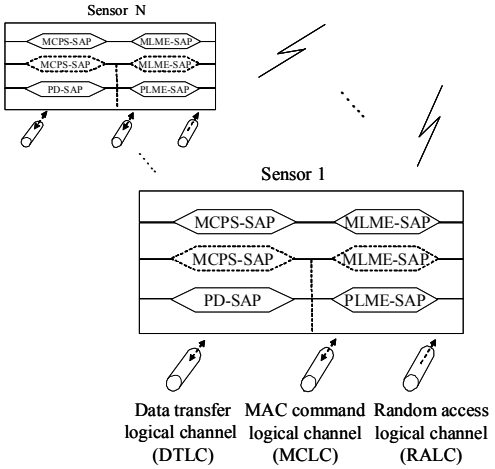


Fig. 3. Logical channel assignment in sensors

Logical channels are defined when a sensor node registers with the coordinator. Once the node is registered, the three conduits are configured between them. The coordinator only sets the destination address of the MCLC and the DTLC so as to reply to sensors.

C. MAC Protocol

1) Association and Disassociation

A sensor requests an association to a coordinator and receives an acknowledgement with an assigned sensor ID, which represents the slot offset in the guaranteed time slot (GTS) when it powers-on. Then, it initializes the security mechanism, such as a block cipher and key sharing protocol, followed by the security type in the MAC frame format shown in Fig. 7. After the initialization, it begins to send vital data to the coordinator via the secured data channel (DTLC).

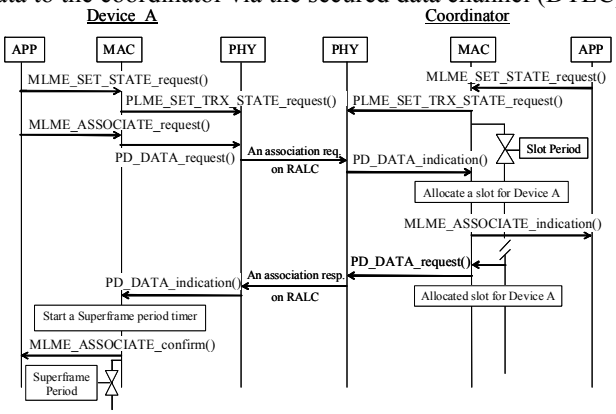


Fig. 4. S-BAN association

The sensor disassociates from the coordinator when the former sends a disassociation request to the latter. The sensor-ID and other related information is erased or the coordinator does not receive any data for several GTSs till the sensor information expires and is finally erased.

2) Security Initialization

The S-BAN security is the resource-constraint security of IEEE802.15.4 with an easy-setup mechanism. Wearable sensors have strong resource constraints not only on data storage and CPU power, but also on their weights.

The S-BAN solutions toward passive attacks are data encryption, mutual authentication and identity camouflaging. (1) All traffic including control and data packets should be well integrated and encrypted to the allowed maximum degree and well integrated. AES128-CBC is deployed and optimized for 8-bit sensors and their coordinator. (2) S-BAN nodes have intrinsic mutual authentication feature by generating a key separately in both sides. (3) S-BAN nodes provide sender/receiver camouflaging by deploying fixed-size packet transfers so that eavesdroppers can not identify senders/receivers.

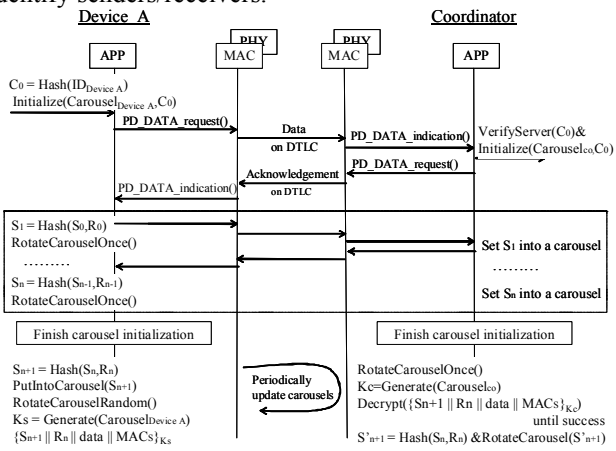


Fig. 5. Security initialization

The S-BAN security has three states: software reset, key generating, and ready. The software reset state initializes keying information on both a sensor and the coordinator. In this state, only a key seed is set on both sides and it is not strong enough to create a key from this data. In the key generating state, the key seed becomes unique for sharing between the two nodes by partially exchanging a subset of a key seed randomly for 35 times. Details are described in [4] and the protocol is shown in Fig. 5.

3) Data Transmission and Receive

A sensor sends vital data to the coordinator at the assigned slot offset via the DTLC. The coordinator enters the receive mode during the offset and receives data from the sensor. The same protocol is used when the coordinator sends data to the sensor.

Vital sensors such as ECG and SpO2 usually keep sending data to the coordinator; therefore, a GTS is required for each sensor. There are some sensors keeping data in their storages, but the privacy protection mechanism needs to comply with the personal information protection law and its guidelines. This privacy-protected function increases the complexity of sensors.

4) Synchronization

The communication is synchronized by a GTS. Each sensor knows how often and when to adjust the timing with the coordinator on the basis of the information exchanged between the nodes during the association. The sensor requests the coordinator to re-adjust the timer (RTC) via the MCLC using the slot, receives the response, and restarts the RTC for next synchronization. Less time synchronization reduces the RX state and saves the power consumption in the sensor node.

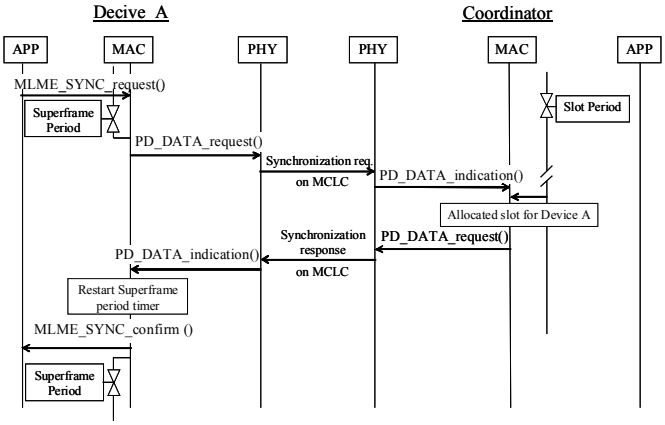


Fig. 6. Synchronization between a sensor and the coordinator

D. MAC Frame Format

An S-BAN does not require high-level protocols such as TCP/IP because of the peer-to-peer data exchange.

The MAC data format is defined in Fig. 7. The application data is divided into series of MAC frame data whose size is less than or equal to 16 × n bytes depending on the RF module and then put into the payload of PHY frames. The maximum data length is determined by the slotted time length, data size, and efficiency in a block cipher.

The format consists of frame control field, sequence number, destination/source addresses, security type, and frame payload with frame check sequence.

The frame control consists of frame type. security enabled, address compression, destination/source address mode, frame version, and frame check. When the security enabled bit is set, security type in the header is used to encrypt/decrypt the data. The frame format is optimized to the logical channel design that does not require to send a destination address each time called and to accommodate recent crypto technologies.

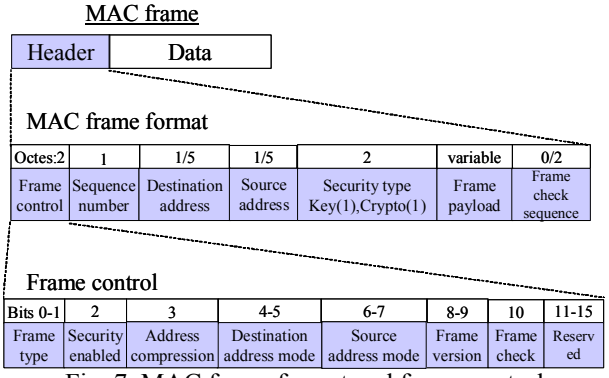


Fig. 7. MAC frame format and frame control

The MAC frame supports both the pre-configured MAC address mode and the usual dynamic address mode. Given below are the typical bit assignments in the frame control.

Destination address mode:
0x00 = No address, pre-configured, 0x01 = reserved, 0x02 = 16-bit short address
0x03 = reserved

……
Security type:
Key: 0x00 = reserved, 0x01 = carousel-type key v1.2, 0x02 = reserved
Crypto:0x00 = reserved, 0x01 = AES128-CBC, 0x02 = reserved

E. Application Data Representation Using TLV

The data representation is expected to be compact and extendable to accommodate new sensors. Currently the number of sensors targeted for regular/home medical examination systems is around 20 and the maximum number of organizations that manufacture sensors is expected to be less than one hundred. The data representation is optimized to the number less than 127 and is extendable to accommodate more than 127 manufacturers.

Each data is distinguishable by the TYPE field at a coordinator, as shown in Table 1. If the first octet in TYPE has 0 in the MSB, then following 7 bits identifier (1-127) represents a manufacturer. Beyond the identification number, the MSB of the first octet is set to 1 and the 2nd, 3rd, and 4th octets are filled with the value of the vendor's IEEE organizationally unique identifier (OUI).

Table 1 TYPE_VDE_VENDOR_ID

Type= TYPE_VDE_VENDOR_ID	Length= *Variable*
Sequence number	
Vender specific TLV data	

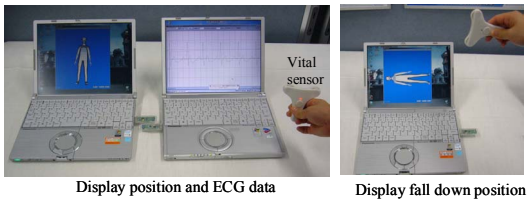
III. Evaluation

We evaluated the S-BAN from the viewpoint of implementation and the reduction of power consumption. Firstly, it is important to confirm that the S-BAN operates on real devices, such as an accessory-type ECG and a ring-type SpO2 sensor, because target sensors have severe restrictions in the RAM/ROM sizes, CPU clock, and real-timer precision/drift. Secondly, it is necessary to evaluate power consumption in sensor nodes. We mainly analyzed the reduction of the RX mode used in time synchronization.

A. *Secure BAN on ECG*

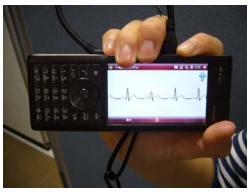
First, we confirmed that the S-BAN works on an accessory-type ECG sensor, as shown in Fig. 8 and 9. The BAN MAC/PHY and AES128-CBC with automatic key generation consumes 29KB ROM and 2 KB RAM in an 8-bit CPU C8051. We confirmed that 9 ECG sensors were associated with the same S-BAN and they operated properly. In the current GTS configuration, the number of sensors in an S-BAN is 24, which is based on the data sampling period/bandwidth. Logically, there is no limitation in the sensor management. IEEE802.15.6 is expecting more than 100 sensors in a BAN in future and this is also feasible in our design.

A medical sensor is required to have the ability of continuously sending vital data for 24 hours for clinical tests that comply with the Pharmaceutical Affairs Law in Japan. We confirmed that the S-BAN with the ECG sensors satisfy this requirement.



Display position and ECG data

Display fall down position



Display ECG and position in a coordinator (Cellular phone)

A coordinator and wearable vital sensor

Fig. 8. Secure BAN on accessory-type ECG

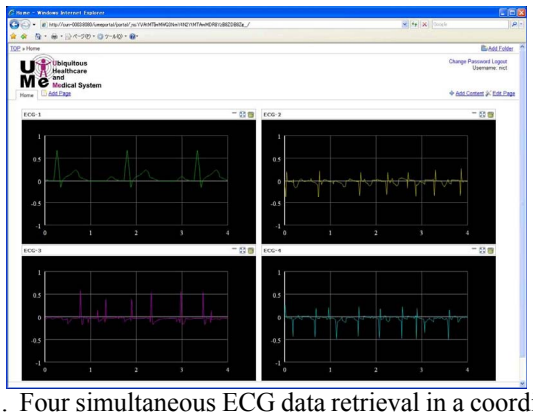


Fig. 9. Four simultaneous ECG data retrieval in a coordinator

B. *Power Consumption in Time Synchronization*

We measured the current draw of send/receive in the RF chip nRF2401. The C8051 CPU consumes 3.3mA. The current draw of data transfer in the RF is 11.3mA and its active time is 300 µs, whereas that of data receive is 11.8mA and the active time is 9.5ms. The average current draw of data transfer is 3.313mA, whereas that of data receive is 3.721mA. The relationship between the average current draw and the number of GTSs for timer re-synchronization expresses how short time a sensor needs to enter to the RX mode. Less time it enters to the mode, more efficient in sensor node power consumption. Fig. 10 shows that the average current draw is almost the same when the interval of the re-synchronization is more than 100 GTSs. It signifies that the reduction of the receive state in the sensor node is not so important for the reduction of power consumption, since the CPU consumes 3.3mA in data encryption and the MAC is considered as a baseline.

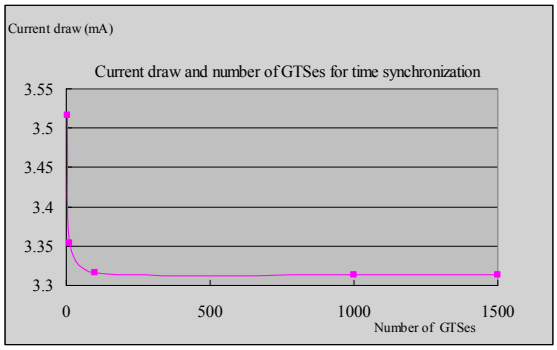


Fig. 10. Average current draw and GTS re-synchronization

The battery capacity in the ECG is around 230mAh and it satisfies more than 24 hours of continuous data retrieval; however, we need to investigate whether it operates as we expected it to. We have found extra power consumption in the MAC by looking at SYNC packet timing charts using a synchroscope and need to further investigate it.

IV. Conclusion and Future Work

In this paper, we proposed a power-efficient MAC protocol with resource-constraint security of the BAN. The S-BAN MAC provides vital data ordering among different types of vital sensors. We implemented the MAC in the real ECG sensors and evaluated the performance of the S-BAN from the view point of power consumption. The evaluation of power efficiency of the S-BAN helps us in deploying it and also provided feedback to the IEEE802.15.6 MAC proposal which will be the future standard for the BAN. We also have observed power consumption tendency in timing charts.

From now on, we will further investigate remaining issues, such as the detailed power-consumption ratios in data retrival and transfer, and work with medical people for conducting clinical evaluations in hospital settings. In the near future we will follow the IEEE802.15.6 specification with advanced low-power mechanism.

Acknowledgment

We would like to thank Mr. Changbin Zhang and Ms. Xiaoxue Liang of Dairix Corporation for deploying the S-BAN MAC. We also wish to thank Mr. Hiroshi Yoshizawa of RIE Inc. for providing a medical sensor device for analysis.

References

[1] http://www.bluetooth.org

[2] S. Gumudavelli, P. McKneely, and P. Thongpithoonrat,, "Medical Instrument Data Exchange," pp.1809-1812, IEEE EMBC 2008, Aug. 2008.

[3] http://www.ieee802.org/15/pub/TG4.html

[4] M. Kuroda, Y. Tamura, R. Kohno, and O. Tochikubo, "Empirical Evaluation of Zero-admin Authentication for Vital Sensors in Body Area Networks," pp.2349-2352, IEEE EMBC 2008, Aug. 2008.

[5] M. Kuroda, R. Nomura, and W. Trappe, "A Radio-independent Authentication Protocol (EAP-CRP) for Networks of Cognitive Radios," pp.70–79, IEEE SECON 2007, Jun. 2007.