Joint Encryption/Multiple Access for Body Area Sensor Networks

Walter D. Leon-Salas
CSEE Department
University of Missouri-Kansas City, USA
leonsalasw@umkc.edu

Yugyung Lee
CSEE Department
University of Missouri-Kansas City, USA
leeyu@umkc.edu

Deep Medhi
CSEE Department
University of Missouri-Kansas City, USA
dmedhi@umkc.edu

ABSTRACT

This paper addresses the security of the radio link in body area sensor networks (BASNs). Given that the well being of a person or its privacy can be compromised, security in a BASN is of utmost importance. In this work, we take a joint encryption/multiple access approach. We use a direct-sequence spread spectrum (DSSS) multiple access technique to share a radio channel between multiple sensor nodes. Unlike standard DSSS techniques, in this work, the pseudo-noise (PN) code employed to spread the transmitted signal is changed on a bit-by-bit basis. This new PN code is generated by a non-linear feedback register. The register is initialized with a secret key. Not two radio links may use the same key at any given moment. The nodes begin communication with each other by employing a publicly known PN code assignment. They exchange keys using the public PN codes and then switch into the non-linear, non-repeating PN code generation. The proposed method has the advantage of simultaneously securing the radio link and providing a means for different sensors to share the same radio channel. This joint approach results in circuit complexity and power savings.

Keywords

Body area sensor networks, security, spread spectrum.

1. INTRODUCTION

Advances in wireless communications, networking, electronics, and sensor technologies have made possible the design and implementation of wearable sensor networks. Wearable sensor networks, also known as body area sensor networks (BASN), are a collection of wearable, ingestible, or implantable wireless miniature sensors. These sensors can collectively monitor physiological and activity signals of a person. BASNs can be employed in hospitals to monitor at-risk or chronically ill patients, at home to monitor elderly people, or in the battle field to monitor the soldiers' vital signals [1].

To be widely accepted by the public, wearable sensor nodes have to have a small form factor, i.e., have low circuit complexity and consume minimum energy. Reduced energy consumption will allow the sensor nodes to be powered up by small batteries that do not have to be replaced frequently. Moreover, they can be powered by energy harvested from body heat or body motion.

Security is an important issue in a BASN. As the sensor nodes communicate wirelessly with each other, an eavesdropper equipped with an antenna and a tunable receiver can easily record physiological information from users without their permission. Moreover, he can launch different attacks on the BASN such as jamming the radio channel, inserting fake data packets, flooding the network with traffic, or altering the contents of packets as they move through the network. Given that the failure of a BASN might compromise the well being of a person, security is of utmost importance.

At the same time, a BASN has to have a mechanism to allow multiple sensor nodes to exchange information without interfering with each other. A first approach to this problem will be to assign different transmission and reception frequencies to each node. However, as the number of sensor nodes increases, the required frequency band becomes too large and could conflict with other wireless standards. Other ways to share a radio channel are time division multiple access (TDMA) and code division multiple access (CDMA). In TDMA, each sensor node is assigned time slots for transmission and reception. The sensors are required to have precision clocks to maintain synchronization with each other.

In CDMA, each sensor node is assigned a unique code that is used to distinguish its transmitted signals from the others. The CDMA scheme considered here is known as direct-sequence spread spectrum (DSSS). In DSSS, a unique pseudo-noise (PN) code is assigned to each sensor node. The node multiplies the data to be transmitted with the PN code and transmits the result. Due to the correlation properties of the PN codes, the transmissions from different nodes can be separated. DSSS has the added advantage of being robust against narrow band radio jammers and interferences.

In this work, we propose to employ a DSSS scheme to provide nodes with a multiple access mechanism. At the same time, we secure the radio transmission by changing the PN code for every bit of information. To keep intruders from fig-

BodyNets 2008, March 13-15 Tempe, Arizona, USA
Copyright © 2008 ICST 978-963-9799-17-2
DOI 10.4108/ICST.BODYNETS2008.2993

uring out how the PN codes are changed, a non-linear shift register is employed to generate these codes. This approach results in savings in hardware complexity since the hardware utilized to provide multiple access to the nodes is also utilized to encrypt the data. The reduced hardware will also consume less power than a separate encryption and multiple access implementation. Thus, the proposed solution is suitable for wearable sensor nodes.

2. PROPOSED SOLUTION

We propose a hybrid solution that combines the one time tape cryptographic technique with a DSSS system. The one time tape technique is an unconditionally secure system in which the plaintext is combined with a totally random sequence of the same length. If the plaintext is represented as a n-bit binary string, it can be combined with the random sequence by performing a bitwise XOR operation. The random sequence has the same length as the plaintext. As the name suggests, the random sequence, which is also referred to as the key, is never used again [2].

On the other hand, a DSSS system works by multiplying each bit of information with a PN sequence. Because the PN code or sequence has a wider bandwidth than the data, the spectrum of the original signal is spread over a larger frequency band. At the receiver, the spread signal is multiplied by a replica of the PN sequence. Assuming that the PN sequence at the receiver is correctly aligned to the incoming signal, the original data can be recovered. In a DSSS system, the cross-correlation of PN sequences of different users have values close to zero. At the same time, a single PN sequence has low auto-correlation values with shifted versions of itself. This feature allows to differentiate the transmitted signal of one user from others and to synchronize the PN sequence at the receiver with an incoming signal.

The multiplication operation in a DSSS systems is carried out by XORing the data bits with the PN sequence. The length of the PN sequence, L, is a function of different parameters like the number of users, the available spectrum, and the targeted performance of the system. Typical values of L range from 16 to 256. Because the same PN sequence is used to spread every bit of information, an intruder can figure out, without too much effort, the sequence employed by listening to the transmissions.

In both the one time tape and in DSSS a XOR operation and the generation of random sequences are required. Since in a BASN a multiple access mechanism like the DSSS is needed regardless of what type of security is employed, we exploit the common hardware with the one time tape technique to provide security and multiple access simultaneously. However, notice that unlike DSSS, in the one time tape technique the random sequence is never used again.

We employ a different PN code for different bits of the data. In other words, the PN codes are changed from bit to bit. To accomplish that, a very long pseudo-random sequence of length $N \times L$ is generated. The first L bits are used to encode the first bit of data, the second L bits to encode the second bit of data and so on. After N bits of data the random sequence will repeat itself. The repetition of the pseudo-random sequence is unavoidable and stems from the fact the practical random sequence generators are digital and therefore have a finite number of states. However, by making N very large, attempts to figure out the pseudo-random sequence become impractical.

Arbitrarily long pseudo-random sequences can be generated by a number of different techniques like linear and non-linear feedback shift registers. The drawback of linear feedback shift registers (LFSR) is that a relatively small portion of the output sequence can be used as the seed of the generator to produce the rest of the sequence. We propose to employ a non-linear generator due to its clear security advantages. Different non-linear generators have been proposed in the literature [3], [4].

Here we refer to the seed of the random sequence generator as the key. Before establishing a secure communication link, a pair of nodes have to agree on a key. The problem of key management and distribution in sensor networks has been addressed extensively in the literature. Suitable key management for BASNs have been proposed and include random key predistribution (RKP), structured key-pool random key predistribution (SK-RKP), shared key discovery, among others [5]. These methods have the advantage of requiring reduced memory space making them a good option for BASNs.

3. CONCLUSIONS

This paper addressed the security of the radio link in a body area sensor network. We took a joint encryption/multiple access approach. Multiple access to the radio channel is provided by a DSSS technique. The PN code employed to spread the transmitted signal is also used to provide security. This has the advantage of simultaneously securing the radio link and providing a means for different sensors to share the same radio channel. This joint approach results in circuit complexity and power savings.

4. REFERENCES

[1] E. Jovanov, A. Milenkovic, C. Otto, and P. C. de Groen, “A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation,” *Journal of NeuroEngineering and Rehabilitation*, vol. 2, no. 6, 2005.

[2] W. Diffie and M. E. Hellman, “Privacy and authentication: an introduction to cryptography,” *Proceedings of the IEEE*, vol. 67, no. 3, pp. 397-427, March 1979.

[3] E. L. Key, “An analysis of the structure and complexity of non-linear binary sequence generators,” *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732-736, Nov. 1976.

[4] D. Leon-Salas, S. Balkir, M. W. Hoffman, and L. C. Perez, “Pseudo-noise sequence generator circuits for spread spectrum communications,” *IEE Proceedings on Circuits, Devices and Systems*, vol. 151, no. 6, December 2004.

[5] D. Huang and D. Medhi, “Secure pairwise key establishment in large-scale sensor networks: an area partitioning and multigroup key predistribution approach,” *ACM Transactions on Sensor Networks*, vol. 3, no. 3, article 16, Aug. 2007.