Implantable Medical Device Communication Security: Pattern vs. Signal Encryption (Position Paper)

Fei Hu Qi Hao
Electrical and Computer Engineering
University of Alabama
Tuscaloosa, AL 35487
{ fei, qh} @ eng.ua.edu

Marcin Lukowiak
Computer Engineering
Rochester Institute of Technology
Rochester, New York
mxleec@rit.edu

A tele-healthcare system consists of the interconnections of medical sensors and implantable medical devices (IMDs). The tele-healthcare system needs *secure* medical signal acquisition because there are network attacks that could fail the medical signal collection tasks. For instance, an adversary can insert bad commands to IMD-doctor data communication channels in order to make the IMD operate incorrectly. A pacemaker can make the heart stop beating if it receives the "sleep" command by mistake. Although medical security has been studied [1, 2, 5, 6], very little work has investigated the following issue: *how do we utilize the special medical signal time/frequency domain characteristics to improve medical security efficiency? Can we design an ultra-low-energy medical data encryption scheme that is suitable to resource-constrained implantable medical devices?* Currently, most of conventional medical security schemes focus on the key management, and try to use a low-complexity approach to distributed keys to different medical sensors / IMDs. Some schemes try to simplify the encryption algorithms by reducing some operations such as bit permutations.

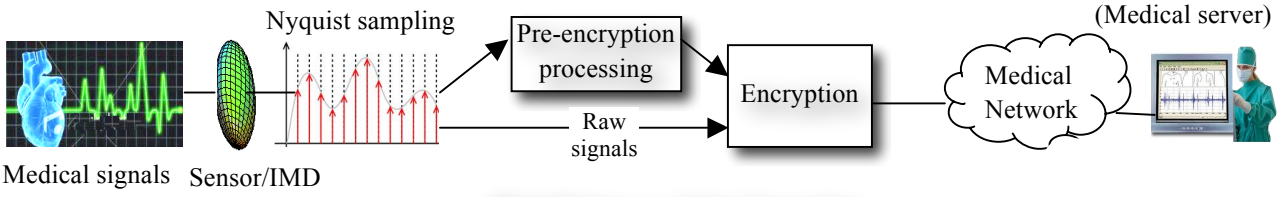

Fig.1 Pattern vs. Value Encryption

In this research, we investigate the energy-saving medical signal security issues from a new perspective: should we encrypt the *original* medical signals (which are collected at Nyquist sampling rate), which is called *value encryption*, or encrypt signals' pattern coefficients (called *coefficient encryption*), in order to achieve ultra-low-power medical signal encryption? As shown in Fig.1, in "value encryption", we take the raw signals from the Nyquist sampler (located in a sensor or an IMD), and perform encryption for each signal sample. In "coefficient encryption", we perform a special signal processing, which is typically some sort of signal transform such as wavelet, to generate a series of coefficients. We then take those coefficients to the encryption module. In the receiver side, we need to recover the original signals based on the received coefficients. Our research attempts to find an efficient *signal transform* to achieve the following purposes:

(1) The transform should be able to significantly compress the medical signals. In other words, the generated coefficients should be much less than the Nyquist samples. Based on our previous experiments [3], the RF transmission consumes most of the sensor's energy compared to other operations such as local sensor data calculation. Therefore, by encrypting much less data, we could significantly save sensor's energy.

(2) The transform should have a conjugate inverse transform that has a satisfactory medical signal recovery in the doctor's server side. If the transform's coefficients could be used to well reconstruct the original medical signals (without losing important statistical characteristics such as non-smooth values), the doctor will still be able to make a correct disease diagnosis.

(3) The transform should favor medical signals' special characteristics. Medical signals have low frequency (<1KHz). The transform should have good resolution in low-frequency band. Thus wavelet is a better choice than DCT (Discrete Cosine Transform) although both of them have good compression and signal recovery functions. Fourier is not a good choice either because they cannot handle the non-stationaility of medical signals. Moreover, besides noise, medical signals often have artifacts which mix with the original signals. For instance, in EEG signals, the movement of eyeballs causes special signal component embedded into the EEG waveform. General signal transform (such as wavelet) may be able to filter noise. However, they cannot remove those artifacts.

In this research, we have found such a good transform, which is *Hidden Markov Tree (HMT)* based signal processing, to generate a tree-shaped wavelet coefficients. Unlike general wavelet transform, the HMT captures not only low-frequency medical signals' characteristics by generating discrete wavelet

transformation (DWT) coefficients. Moreover, it organizes all coefficients through a tree structure. Besides medical signal transform, the HMT has another advantage: it could overcome the impacts of noise and artifacts on the medical signals. For example, it could recover the original EEG signals from a noisy EEG stream with the electric pulses from the eye blinks. *To the best of our knowledge, we are the first researchers to apply HMT to medical signals to achieve not only low amount of coefficients but also anti-distortion signal recovery.* Many other signal transform schemes (such as general wavelet) do not have good medical signal recovery capability when there are strong artifacts and distortions in the noisy medical data.

To further save security energy consumption, we enhance our previously proposed NTRU-based (initially proposed by Ntru Cryptosystems, Inc.) medical data encryption scheme [4] through Karatsuba Algorithm (KA), which can reduce the execution rounds of polynomial star multiplication. Such a NTRU simplification greatly saves local CPU energy consumption.

In summary, our research has two novel contributions: (1) *Pre-encryption medical data transform*: Instead of directly encrypting the medical signals, we adopt signal transform to pre-process the signals before encryption. Based on special medical signals' characteristics (low-frequency, artifacts-distorted, non-stationary), we propose a HMT-based signal transform to generate small amount of coefficients in a tree structure. It has the capability of "one stone hits two birds": it not only compresses the signals, but also identifies and removes the artifacts and noise. (2) *Low-energy encryption based on an enhanced NTRU*: NTRU has lower calculation overhead than ECC and RSA due to its simple polynomial operations. To reduce security energy overhead, we further improve our previously designed NTRU algorithm through KA optimization. We will use detailed experiments to demonstrate the efficiency of our *coefficient encryption*.

Experimental Results: We have observed the use of HMT for *1-D signals (heart beat rates) processing.* Our experiments show that even an ECG signal sequence is damaged by communication channel noise, the HMT model can still well recover the original signals. Security performance: Our NTRU-based HMT coefficient encryption scheme has shorter encryption / decryption time than ECC although the initialization takes more time. In coefficient encryption case, our results show that the percentage of energy for RF transmissions is smaller than value encryption case. This indicates that coefficient encryption significantly reduces energy consumption.

Unsolved Issues: In this position paper, we introduced the importance of "coefficient encryption" here in order to encourage the readers to pursue some unsolved issues in this field:

(1) Symptom-focused medical encryption: First, since the purpose of medical signals is for disease diagnosis, it is unnecessary to encrypt 100% medical signals before wireless transmission. Instead, we can just extract the **symptom-oriented** features for encryption. Some signal projections could be used to find only the signal segments with important symptoms. Normal signals could be filtered before encryption.

(2) **Integrating encryption with medical signal processing:** Integrate signal processing with encryption: currently medical encryption and medical signal processing are two separate processes. We argue that such a separate scheme could waste CPU time and cause high memory overhead. Recently, some signal processing schemes allow the use of a seed-like computing control, which uses a special key (called seed) that could be generated from humans' body signals (such as ECG peaks), to control the signal distortion and receiver recovery. Such a scheme finishes medical data compression and encryption in ONE process. Thus it is very difficult for an attacker to figure out the original medical signals.

(3) **Achieving implantable device security in physical layer instead of in medical data layer**: In the medical device communication layer, some radio signal fingerprints could be used to hide medical data. The OFDM signal decomposition and modulation provide some opportunities for encryption. The implantable device has special RF modulation constellation diagram, which can be used to achieve secure device access.

REFERENCES:

[1] A. B. Waluyo, I. Perk., Chen, and W. Yeoh, "SLIM: A secured lightweight interactive middleware for wireless body area network," 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 1821 – 1824, Aug. 2008.

[2] Y. Cai, J. Tan, "Secure Group communication in Body Area Networks," International Conference on Information and Automation, pp. 555 – 559, June 2008.

[3] Fei Hu, Yang Xiao, Qi Hao, "Congestion-aware, Loss-Resilient Bio-monitoring Sensor Networking," IEEE Journal on Selected Areas in Communications (JSAC), VOL. 27, NO. 4, MAY 2009. Pages 450-465.

[4] Fei Hu, Kyle Wilhelm, Michael Schab, Marcin Lukowiak, Stanislaw Radziszowski, Yang Xiao, "NTRU-based Sensor Network Security: A Low-power Hardware Implementation Perspective," International Journal of Security and Communication Networks (Wiley), Volume 2, Issue 1, Date: January/February 2009, Pages: 71-81.

[5] Fengyuan Xu, Zhengrui Qin, Chiu C. Tan, Baosheng Wang, Qun Li. *IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian.* The 30th IEEE International Conference on Computer Communications (INFOCOM 2011), Shanghai, P.R.China.

[6] hyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: Non-invasive security for implanted medical devices. In *Proceedings of ACM SIGCOMM*, August 2011.