Privacy-Preserving Telecardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign

Fei Hu, *Member, IEEE*, Meng Jiang, *Member, IEEE*, Mark Wagner, *Member, IEEE*, and De-Cun Dong, *Senior Member, IEEE*

***Abstract*—Recently, a remote-sensing platform based on wireless interconnection of tiny ECG sensors called Telecardiology Sensor Networks (TSN) provided a promising approach to perform low-cost real-time cardiac patient monitoring at any time in community areas (such as elder nursing homes or hospitals). The contribution of this research is the design of a practical TSN hardware/software platform for a typical U.S. healthcare community scenario (such as large nursing homes with many elder patients) to perform real-time healthcare data collections. On the other hand, due to the radio broadcasting nature of MANET, a TSN has the risk of losing the privacy of patients' data. Medical privacy has been highly emphasized by U.S. Department of Health and Human Services. This research also designs a medical security scheme with low communication overhead to achieve confidential electrocardiogram data transmission in wireless medium.**

***Index Terms*—Cardiac monitoring, medical privacy, telecardiology, wireless sensor networks.**

I. Introduction

OVER 20 million people worldwide have abnormal electrocardiogram (ECG) signals, i.e., arrhythmias, each year [1]. Most of the cardiac patients are elders. The worldwide population of those over 65 years of age is predicted to reach 761 million by 2025, more than double than what it was in 1990 [2]. If the proportion of elders with arrhythmias remains constant, and they increasingly move to nursing homes, it is a necessary tendency to reduce the medical labor cost by deploying self-organized wireless cardiac-monitoring hardware/software systems in an area with a radius of hundreds of feet. Such medical information networks could allow the doctors to immediately capture the arrhythmia events of any patient without leaving their offices. An added benefit is the freedom of movement for patients due to the wireless networking technologies.

Some cardiac remote-sensing systems have been built in academia and industries. Among commercial telemetry systems, *CardioNet* is the first provider of mobile cardiac outpatient telemetry (MCOT) service in USA for continuous monitoring of patient's ECG and heartbeat at home, at work, or while traveling[1]. A wearable wireless biomedical sensor system has been developed in [3]. A wireless and wearable ECG monitoring system has been proposed in [4]. It continuously measures and transmits the sampled ECG signals to the patient's personal digital assistant (PDA) using a built-in radio-frequency (RF) radio transmitter. The PDA automatically connects to a cellular network to transmit data to the health provider. A real-time patient-monitoring system that integrates vital signs sensors, location sensors, ad hoc networking, electronic patient records, and Web-portal technology was designed and developed in [5]. Most of those cardiac remote-sensing systems are based on cellular networks that can achieve long-distance ECG transmission but need to use expensive cellular network infrastructure (such as large base stations and complex cell management/bandwidth allocation systems).

It has been shown that remote sensing through the wireless interconnection of ECG sensors is a promising approach to perform "automatic" heart beat anomaly detection [6]. CodeBlue [7] is a typical example. Today, many ECG machines, both standard and continuous ones, are marketed as "portable," but this does not always indicate that they are small and unobtrusive. In contrast, most such appliances receive power from an electrical outlet and are sufficiently heavy such that they must be mounted on a cart and wheeled from one location to the next. Low-power *Telecardiology Sensor Networks* (TSNs) consisting of large-scale low-cost micro-ECG sensors attached to the patients' bodies, if deployed in nursing homes, will have the potential to significantly improve the ECG portability and timeliness. The tiny ECG sensors (weight <0.5 lbs; size is comparable to a few coins) are particularly advantageous because of their low cost, radio communication capability, rapid deployment, and ease of integration with existing hospital computer systems. In the next decade, we could even use microelectromechanical system (MEMS) technology to make an ECG sensor smaller than a coin [8].

In a typical TSN, each patient's ECG signal could be automatically collected and processed (such as analog-to-digital conversion) by a small ECG sensor, and then be wirelessly sent to an ECG server for analysis (such as using data classification to find out arrhythmia). If an ECG sensor reports any abnormal heart-beat signals, an emergency communication channel

Manuscript received October 7, 2006; revised February 27, 2007. This work was supported in part by the Cisco University Research Program and in part by the National Science Foundation (NSF) under Award 0716455.

F. Hu and M. Jiang are with the Department of Computer Engineering, Rochester Institute of Technology, Rochester, NY 14623 USA (e-mail: fei.hu@rit.edu).

M. Wagner is with Sensorcon, Inc., Reading, MA 01867 USA (e-mail: mark.wagner@sensorcon.com).

D.-C Dong is with the Transportation Engineering Institute, Tongji University, Shanghai 200092, China (e-mail: ddc58@sohu.com).

Digital Object Identifier 10.1109/TITB.2007.894818

[1][Online]. Available: http://www.cardionet.com/

established between the physician's office and the patient's wireless device such as a beeper or cellular phone will be used to send out alerts to provide the patient some medical suggestions such as taking drugs or performing other further processing. In a more advanced TSN, a patient's ECG sensor can even use a neighbor sensor to relay its data if his/her distance is too far away from the ECG server. This communication mode is called "multihop" wireless transmission. Multihop TSN not only extends the communication distance but also saves the energy consumption of an ECG sensor, since direct sensor–server long-distance wireless communication is avoided through hop-to-hop relay.

Although the proposed TSN runs in a nursing home that is different from a long-distance remote ECG monitoring scenario, the *hop-to-hop wireless data relay* nature (among patients' sensors) has the potential to be applied to a remote monitoring case.

Our main contributions in this research include the following three aspects.

1) *Low-Cost*, *Low-Power TSN Hardware Design* (see Section II): Our TSN hardware mainly includes tiny ECG sensors and RF communication boards. The manufacturing cost for all the components (such as resistors, amplifiers, etc.) is less than \$80 each. If produced in large amount ($>$1000), the cost will be less than \$50. We are in the process of using very large-scale integration (VLSI) to redesign those units, which can largely decrease the entire cost (below \$10 each). Because of our low-power design (through voltage scaling, low duty cycle, less RF collisions, and sleep control), the two AA batteries could provide the entire ECG sensor board 13 months of lifetime. Compared to the current commercial ECG measurement devices, our design is much lighter ($<$0.5 pounds), much cheaper ($<$\$80), more portable, and more power-efficient (no ac power outlet is needed). Moreover, our TSN includes a new RF board design, which saves more manufacturing cost than the current sensor networks such as CodeBlue [7].
2) *Integrated RF Communication/ECG Signal Processing Software Design:* Our TSN has more advanced ECG transmission/processing software than current sensor networks such as CodeBlue [7]. For instance, our TSN software can classify different types of heart beats at greater speed and higher accuracy. We have also built an ECG sensor control software.
3) *Less-Complex End-to-End TSN Security Scheme* (see Section IV): Many hospitals hesitate to use advanced remote-sensing systems, because they are not sure of the privacy-preserving capability of such systems. We have, thus, designed a cluster-based end-to-end TSN security scheme in our TSN software modules in order to keep confidentiality during the patient–doctor ECG transmission. Our security algorithm considers the low-cost low-memory characteristics of tiny ECG sensor boards. We, thus, designed a low-communication-overhead low-complex encryption and decryption scheme.

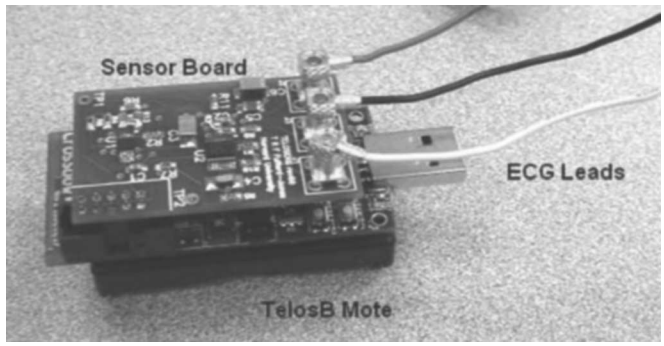

Fig. 1. Mobile platform appearance (includes ECG sensor + RF Mote) [7].

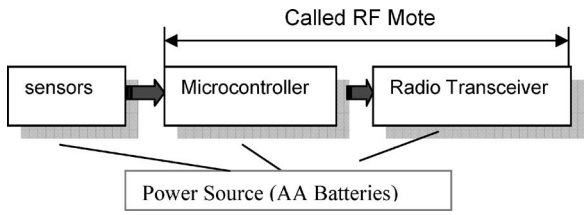

Fig. 2. TSN mobile platform: Logic architecture.

II. TSN Hardware Platform

Our TSN consists of large amount of wireless ECG communication units. Each unit is called a "mobile platform." These mobile platforms are essentially the wearable ECG devices that would be distributed among cardiac patients in order to offer continuous monitoring of the patients' vital signs. As shown in Fig. 1, each platform is composed of a customized ECG sensor board providing connections to a three-lead ECG monitoring system, which is housed on a wireless communication board (also called RF motes). CodeBlue [7] conducted pioneering ECG sensing research through this architecture. While the ECG sensor board gathers useful patient ECG data, the RF mote provides limited local signal-processing capabilities (such as ECG noise filtering) and, more importantly, wireless communication for transmitting the ECG signals back to the server for feature extraction. Fig. 2 shows the logic of the architectural components of the TSN mobile platform.

Our original RF mote (see Fig. 1) was based on TelosB motes from Crossbow, Inc.[2] The TelosB mote is also referred to as the Tmote Sky. It is an ultralow power wireless module intended for sensor networks applications. Regarded as the next-generation mote platform, it offers the on-chip RAM of 10 kB and also provides IEEE 802.15.4 Chipcon radio[3] with an integrated onboard antenna providing up to 125 m of range. Constructed around a TI MSP430 microcontroller[4], the TelosB worked for this project for its onboard analog-to-digital converter (ADC) peripherals with expansion bays, which connects the customized sensor board.

However, we found out a few problems when using TelosB: First, the unit price of TelosB is high in terms of large-scale

[2][Online]. Available: http://www.xbow.com
[3][Online]. Available: http://www.chipcon.com
[4][Online]. Available: http://www.ti.com

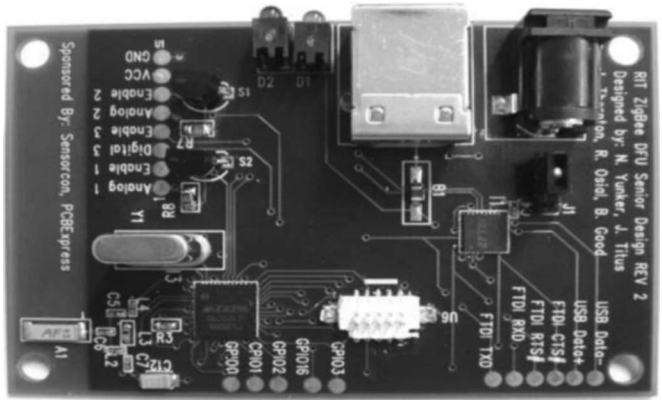

Fig. 3. RF board built by us.

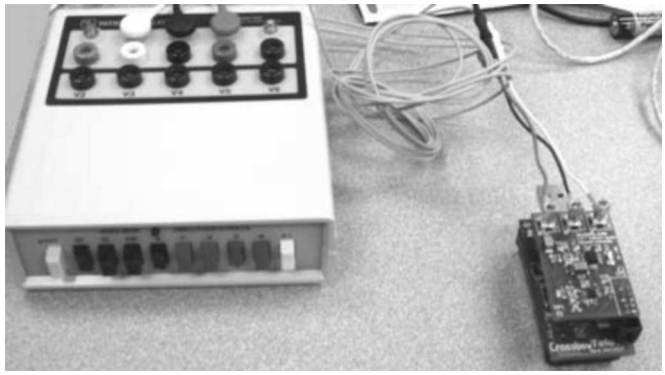

Fig. 4. Mobile platform patient simulation.

TSN deployment. Currently, the TelosB RF mote is around \$150 each[2], and there is no discount for educational purposes. Because we needed to use the TSN platform (with at least 30 motes in each TSN network) to train a large number of computer engineering/science students, we decided to build our own RF boards. Second, its power lifetime is around 3–6 months depending on how often the ECG signal is transmitted back to the server, which is somewhat short for medical applications. Ideally, we wish that the cardiac patient could carry such a low-cost ECG sensor for at least one year without worrying about power exhaustion. Third, its radio components cannot be enhanced; we cannot use a better radio transceiver to reach a longer distance.

Due to the above reasons, we have used Ember CPU-RF chips[5] to build our own RF motes. As shown in Fig. 3, it is also driven by AA battery. The RF mote is a little larger than two AA batteries. The cost for electronic parts is \$11.06 per board. The estimated quote of printed circuit board (PCB) fabrication (mass production) is \$1.93 per board. The estimated cost for board assembly is \$5.00 per board. This gives a total cost of *only* \$17.99 *per mote* (mass production). The heart of the RF board is the micro central unit (MCU)/ZigBee[6] transceiver unit. Multiple options and configurations were considered before selecting the final option. The two options that resulted from it were using a separate MCU and transceiver or using a system-on-chip (SoC) that incorporates the two devices together. The SoC option was chosen, as it would be cheaper to implement, would decrease programming complexity, and create an easier PCB layout, as there will be fewer parts to the layout.

Our ECG sensor board design is assisted by the Harvard University CodeBlue team [7]. The ECG lead extensions from the sensor board are pin-compatible and color coded to standard three-lead ECG monitoring systems. While there are different flavors of physiological chest leads, this system was designed to match any three-lead ECG snap set lead wires. The snap set may be used to collect data by attaching to it the appropriate jellied ECG conductive adhesive electrodes, if real people were to be used for testing purposes.

An alternative would be ECG signal simulators. The testing simulator chosen for this project is Model 430B, 12-lead ECG simulator that can provide a complete PQRST waveform at six preset rates (60, 75, 100, 120, 150, and 200 BPM) as well as six preset amplitudes (0.1, 0.2, 0.5, 1.0, 2.0, and 5.0 mV). It is also capable of generating square waves using its five ECG snaps plus ten banana jacks. This would provide a good testing interface even if this project is adapted into a 12-lead monitoring system in future. Fig. 4 shows the connection between 430B ECG simulator and our designed RF communication boards.

III. TSN Software Architecture

After the explanation of our TSN hardware devices, we will describe our TSN software architecture that includes two major modules: 1) TSN *wireless communication control software* that collects ECG data, and then transmits data through a patient-to-patient relay mode, until finally reaching the *medical server* that has ECG display software, medical database management, and ECG feature extraction functions and 2) *ECG Feature Extraction/Classification software*, which can classify heart beats with high accuracy.

A. ECG Sensor Mote Wireless Communication Software

All of our TSN RF mote control software runs in a special *operating system* called TinyOS[7]. Developed primarily by the University of California, Berkeley, in cooperation with Intel Research, TinyOS is an open-source embedded operating system designed for wireless sensor networks. Written in NesC programming language[7], TinyOS offers a component-based architecture and is able to operate within the severe memory constraints posted by sensor networks. The copy of TinyOS used in this research is Version 1.1.15, released in December 2005. NesC is a programming language designed for applications targeting the TinyOS platform. It is an extension to the C programming language that is component based as the TinyOS operating system. The most important feature of this programming language is that it produces fairly small-sized code to be able to load on to sensor network nodes.

[5][Online]. Available: http://www.ember.com
[6][Online]. Available: http:// www.zigbee.org
[7][Online]. Available: http://www.tinyos.net

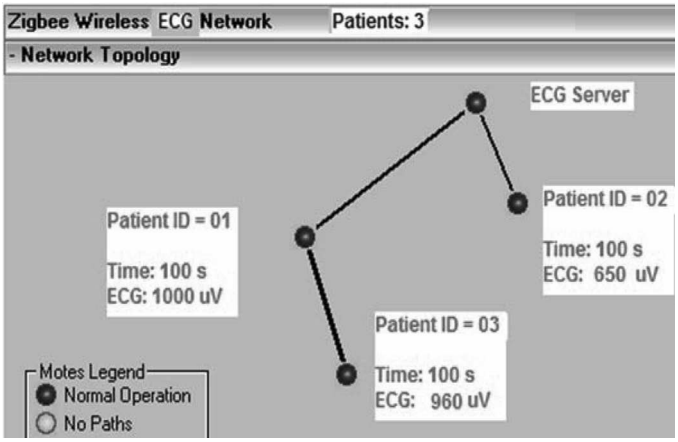

Fig. 5. Cardiac monitoring software for a simple case with three patients.

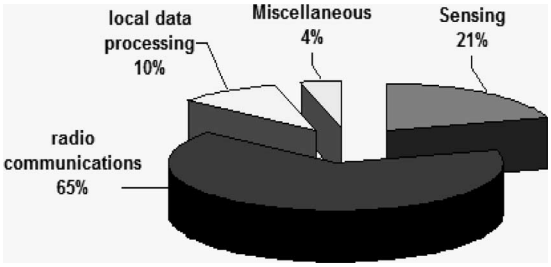

Fig. 6. Energy consumption of TSN.

In our medical server that receives all patients' ECG data, we can monitor the entire TSN network topology. As shown in Fig. 5, each patient's ECG data can be collected remotely. If two patients are close enough, a radio link will be shown between them to indicate the possibility of transmitting ECG data between them (in Fig. 5, ECG RF motes in Patient ID $= 1$ and ID $= 3$ can talk with each other).

An important feature of our TSN software is that we are able to control the ECG sensors' performance parameters (such as ECG detection threshold) through the command transmission from the server to any ECG sensor. We can set up the ECG server (i.e., the TSN workstation) *control parameters* to change the sensors' *detection frequency* (i.e., how many ECG values should be collected in each second). As we know, a higher detection frequency can bring higher ECG signal quality. However, it also causes the higher power consumption in each sensor and more memory storage overhead in each RF board. A good balance is needed. Here, we collect ECG values every 0.01 s, which is good enough to capture each change of heart beats.

The software used to govern the sensor network communication and displaying the received patient data on the workstation is based on a program called *VitalDust Plus* [7]. This software is essentially a stripped-down version of the CodeBlue [7] software that provides a simple demonstration of its wireless pulse oximeter and wireless eck devices. The software has two parts, the TinyOS software for the mobile platforms to sample and transmit vital sign data over the radio, and a Java GUI application to display the vital signs in a graphical form.

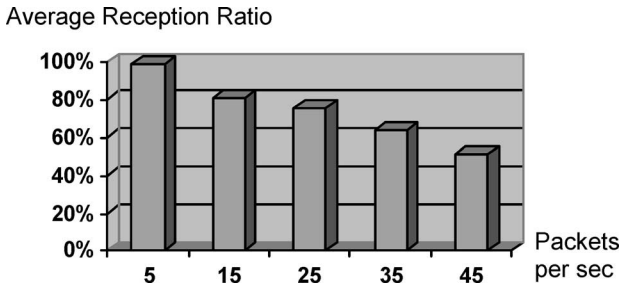

Fig. 7. Reception ratio for different sending rates.

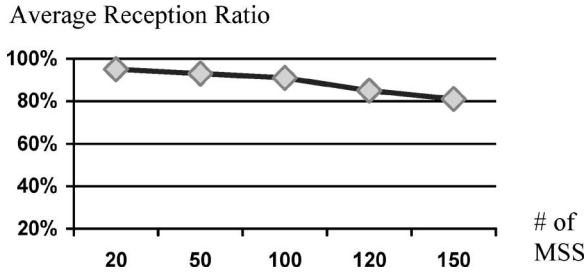

Fig. 8. Reception ratio for different number of MSS.

B. TSN Wireless Communication Performance Evaluation

1) *On the Energy Consumption of TSN Operations:* A major concern in TSN networking design is energy consumption. Our experiments have shown that most of the sensor battery is consumed in radio communications instead of in local data processing (such as ECG compression) or sensing (see Fig. 6). Therefore, any TSN networking protocols (such as finding optimal route) should be of low complexity to save energy consumption.
2) *Effect of Increasing the Data Sending Rate in Each Sensor:* For a better observation of a patient's health condition, a sensor can send out data at high reporting frequency, and then use a high data rate to send out the large amount of sensed data wirelessly. Fig. 7 shows the packet reception ratio (the number of "received" packets divided by the number of "transmitted" packets) for different sending rates (number of network packets per second). We can see that the TSN performance drops sharply if the sending rate is higher than 25 packets/s. Thus, it is important to use a reasonable reporting frequency in each sensor.
3) *Effect of Increasing the Number of Sensors*: We have investigated the TSN performance by increasing the number of sensors (it also means more patients, since each patient carries one sensor). Our TSN system can maintain good performance (reception ratio $>80\%$) even with a large number of multispectral scanners (MSS; see Fig. 8). It indicates that our TSN will be suitable to a large nursing home.
4) *The Effect of Increasing the Patients' Mobility Speed:* We have tested the TSN delay performance under users' mobility behaviors. Currently, our system cannot achieve real-time data collection (delay >10 s) if the users move quickly (such as at 30 mi/h) (see Fig. 9).

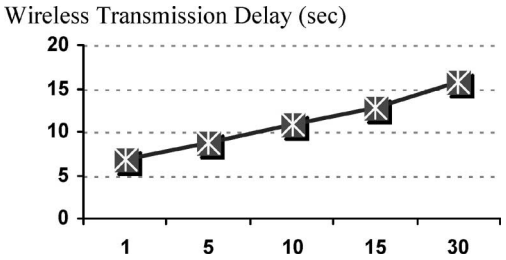

Fig. 9. End-to-end delay for users' mobility speeds.

C. ECG Feature-Extraction Software

Feature extraction is a commonly used term in image processing and pattern recognition. It is a form of dimensionality reduction that locates points of interest from a multidimensional space. In the scope of this research, feature extraction is conducted by applying wavelet analysis techniques to patient data, thus, providing ECG characteristic point-detection capabilities. To improve the *ECG classification* accuracy in terms of identifying different types of abnormal heart beats, we have investigated the theory of *support vector machine* (SVM), which has been proven to be able to minimize the probability of misclassifying yet-to-be-seen patterns [9], [10].

Our SVM algorithms are based on the biology signals data mining principle in [11]. The basic procedure of SVM algorithm is as follows [11], [12]. Considering the problem of separating the set of training vectors belonging to two separate classes, we have

$$S = \left\{ (x,y) \left| \begin{array}{l} \{(x_1,y_1),(x_2,y_2)\cdots,(x_L,y_L)\}, \\ x \in R^n, y \in (-1,1) \end{array} \right. \right\}. \quad (1)$$

The above vectors are said to be optimally separated by the hyperplane, if they are separated without error and the distance between the closest vector to the hyperplane is maximal. We can then transform the input data into a higher dimensional *feature space* to enable linear classification. Specifically, we can define an appropriate *kernel function* in the input space in place of the *dot product* in the high-dimensional feature space. Next, we can formulate the *dual of the convex quadratic programming* problem to obtain the unique global solution for the classifier. To apply the above SVM theory, we need to extract some dominant features from ECG data to serve as the SVM classification vectors. Wavelets analysis is well known for its feature-extraction efficiency. The wavelet transform of a function f is a convolution product of the time series with the scaled and translated kernel, and is given by

$$W_{S,x_0} = \int_{-\infty}^{+\infty} \frac{1}{s} \bullet \Psi\left(\frac{x-x_0}{s}\right) \bullet f(x)dx \quad (2)$$

where S is a scale parameter and x_0 is a space parameter.

To find out the "features" (i.e., the *singularity points*) of the above wavelet function, we introduce the concept of "local holder exponent (LHE)" [9], [11]. The LHE of a function $f(\bullet)$ at the point x_0, denoted as $h(x_0)$, is defined as the largest exponent such that there exists a polynomial $P_n(x)$ of order n satisfying the following condition for a in a neighborhood of x_0:

$$|f(x) - P_n(x-x_0)| \le C \bullet |x-x_0|^h . \quad (3)$$

Based on the Log-Log plot of the wavelet "amplitude *versus* scale a," we can then extract the local LHE $h(x_0)$. In fact, it has been shown that wavelets can remove polynomial trends that could cause the previously used box-counting techniques to fail to quantify the local scaling of the signal [11], [13].

Definition 1: Wavelet Transform Modulus Maxima (WTMM): To reduce the regular wavelet analysis redundancy and calculation complexity, WTMM [11] proposes to change the "continuous" sum over space (2) to a "discrete" sum over the local maxima of $|W_{s,x_0}(f)|$. Denote $Z(s,q)$ as a *partition function*, and $\Omega(s)$ as the set of all Maxima [9] at scale S, then WTMM can efficiently use the following "space-scale" partitioning:

$$Z(s,q) = \sum_{\Omega(s)} |W_{s,x0}(f)|^q \quad \text{and} \quad Z(s,q) \propto s^{\tau(q)} \quad (4)$$

where $\tau(q)$ represents a scaling range. We have the following relationship between the singularity strength $h(q)$, the spectrum of singularities $D[h(q)]$, and $\tau(q)$ (using the Legendre transformation theorem in [9])

$$h(q) = \frac{d\tau(q)}{dq} \quad D[h(q)] = q \bullet h(q) - \tau(q). \quad (5)$$

The importance of WTMM lies in its *maxima lines* (MLs). For any LHE $h(x_0)$, there is at least one ML that points toward x_0. For any fractal signals, the number of MLs will diverge in the limit $s \to 0+$ [16].

Although WTMM provides efficient estimation for "global" scaling of ECG time series, it has been shown that the "local" scaling analysis could provide more relevant information on feature extraction [14]. The idea of "local" scaling analysis can be summarized as follows (for details, see [14]).

First, let us define a function $G(s)$ as follows [through the partition function $Z(s,q)$; see (4)]

$$G(s) = \sqrt{Z(s,2)/Z(s,0)}. \quad (6)$$

Then, the mean LHE (denoted as $\bar{h}$) is determined by

$$\bar{h} = \frac{\log[G(s)] - C}{\log(s)} \quad (7)$$

where C is a constant depending on the ECG amplitude normalization ratio.

Through the Struzik multiplicative cascade model [14], and using $s = 1$ in the wavelet analysis, we can estimate the LHE (denoted as $\hat{h}(x_0)$) at singularity x_0 as

$$\hat{h}(x_0,s) = \frac{\log\left(|W_{s,x_0}(f)|\right) - (\bar{h} - \log(s) + C)}{\log(s) - \log(s_L)} \quad (8)$$

where S_L is the length of the entire wavelet ML tree.

Wrapper Algorithm for ECG Feature Reduction: Even though the wavelet analysis and LHE can provide us a series of ECG features, it is necessary to increase the accuracy of the induction algorithms through the reduction of parameters. Here, we use Wrapper approach in [9] to conduct a search in the wavelet space. Our Wrapper algorithm [9] includes a "state" that is a

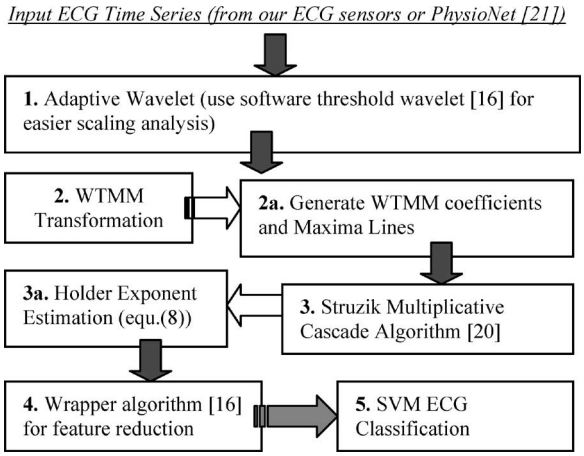

Fig. 10. ECG data series feature extraction software components.

vector of LHE, an initial state (we set to empty), a heuristic evaluation through five-fold cross validation (repeated multiple times with a small penalty for every ECG feature), and a hill-climbing search algorithm.

To validate our LHE/WTMM-based feature extraction and classification, we have used the following ECG data sets: 1) 50 *normal sinus* rhythms (NSR) recorded from real ECG sensors and 2) other Arrhythmia coming from PhysioNet [15], which provides a set of databases that groups records of one or more digitized ECG signals, as well as a set of their corresponding beat and rhythm annotations. Especially, we have used: 1) PhysioNet MIT-BIH noise stress test database that contains typical noises in ambulatory ECG recordings and 2) PhysioNet MIT-BIH Arrhythmia database, which is used to study the different types of arrhythmias.

Regarding Arrhythmia, we have chosen the following five types of rhythms: 1) normal rhythm; 2) *paced* rhythm; 3) *atrial fibrillation*; 4) *nodal (A-V junctional)* rhythm; and 5) *ventricular fibrillation*. For each of the five rhythms (i.e., normal (NSR), paced, A-Fib, nodal, and V-Fib), we have used the following procedure (see Fig. 10) to extract the WTMM LHEs that will be used for the input vectors of SVM model.

Please note that Step 3a in Fig. 10 does not directly use the "single-value" holder exponents, since we have used statistical analysis based on large amount of MIT-BIH arrhythmia record flows (each record flow has 10-s of ECG data series). Thus, we have calculated the probability densities of different LHEs and then fitted those densities into a Gaussian model. The LHEs for the five rhythms were found to be in the range of $(-0.5, 1.5)$. We then divided this range into ten subranges and took the ten mid-points of those ten subranges in the probability density function. We have used multiple runs of five-fold cross validation in Step 4.

Our SVM-based classification results are shown in Fig. 11, where we have also compared our classification performance to two of the best ECG classification algorithms, i.e., Bayesian Classifier [16] and Decision Tree [17]. Although the accuracy for NSR is similar between ours and others, the accuracy to identify arrhythmia is higher in our scheme. More importantly,

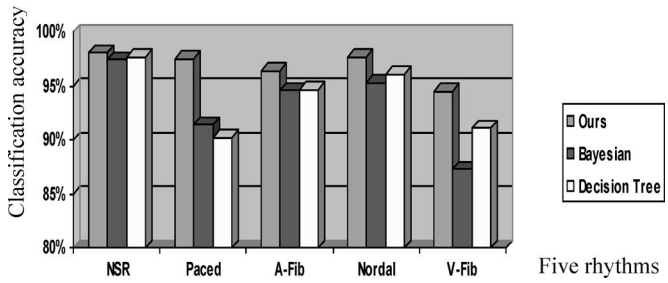

Fig. 11. Normal/Arrhythmia classification accuracy.

our algorithm can use WTMM/Wrapper to efficiently extract multiple features from a "large-scale" ECG database within a reasonable small calculation time.

Equation (9) shows the confuse matrix (for all Arrhythmia, not including NSR), where the WTMM coefficients were computed at scale [1:20] and the LHEs were estimated at scale 1. Both the leads were used for classification purpose. We can see that there are very few nondiagonal numbers present. The diagonal values represent the correct identification of the respective rhythms. Another important observation is that all the arrhythmia rhythms are very well separable. In the right-bottom (6×6) matrix, all the nondiagonal numbers are zero (or negligible).

$$\text{Confuse\_Matrix} = \begin{bmatrix} & \text{NSR} & \text{Paced} & \text{A–Fib} & \text{Nodal} & \text{V–Fib} \\ \text{NSR} & 67.3 & 0.89 & 0.13 & 1.12 & 0.89 \\ \text{Paced} & 0.77 & 19.35 & 0 & 0 & 0 \\ \text{A–Fib} & 1.31 & 0 & 9.98 & 0 & 0 \\ \text{Nodal} & 0.91 & 0 & 0 & 20.14 & 0 \\ \text{V–Fib} & 1.11 & 0 & 0 & 0 & 3.41 \end{bmatrix}. \tag{9}$$

IV. Privacy-Preserving Wireless ECG Transmission

A. Security Requirements in MANET-Based Telecardiology Networks

Medical security is important in healthcare organizations all over the world. For instance, U.S. HHS issued patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [18]. HIPAA included provisions designed to encourage electronic transactions, and also required new safeguards to protect the security and confidentiality of health information. Most health insurers, pharmacies, doctors, and other healthcare providers were required to comply with these federal standards beginning April 14, 2003 [18]. To protect the two important aspects of cardiac patient "privacy" in TSN systems: 1) *confidentiality*, i.e., only the source/destination can understand the medical data through cryptokeys and 2) *integrity*, i.e., no data falsifying during transmission, we need to apply strong end-to-end security mechanisms to the cardiac data packets that are transmitted between any two network entities (such as between a patient's sensor and a physician's server). On the other hand, in a practical community/hospital telecardiology system that is based on sensor network architecture, we

should consider the following two constraints when designing privacy-preservation mechanisms.

1) *Low-Energy/Low-Overhead Security Protocols*: A major concern in medical security protocols design is *energy efficiency*. Our experiments [19], [20] have shown that most of the sensor battery is consumed in radio communications instead of in ECG signal processing or sensing (see Fig. 6). Therefore, the security protocols should not use too many message exchanges between patients' sensors and network. Moreover, the security schemes should be of low complexity. Therefore, symmetric crypto could be a better choice than traditional asymmetric crypto based on public/private keys having high computational overhead.
2) *Multihop Versus Single-Hop Security:* We should use multihop wireless relay among patients instead of single-hop communications (i.e., direct patient–doctor wireless forwarding) due to the following reasons. First, by deploying a multihop data forwarding network, packets can be routed around radio obstructions in a community. While in a single-hop, i.e., long distance (>100 m), line-of-sight radio communications may not be possible. Second, packet forwarding via multiple short links requires less energy than a single long-link transmission for radio communications [21], [22]. The energy savings afforded by multihop forwarding would help conserve sensor batteries.

B. Security Design for "One-Hop" ECG Data Transmission

Security in each individual hop is the prerequisite of the multihop TSN security. As the starting point of our security research, we have implemented a low-energy low-overhead security scheme for one-hop (e.g., patient-to-doctor) wireless communications [22], [23].

Our one-hop security mechanism uses the following two security primitives.

1) *Initialization Vectors (IVs)*: One implication of semantic security is that encrypting the same plaintext two times should give two different cyphertexts. The main purpose of IVs is to add variation to the encryption process when there is little variation in the set of messages.
2) *Block Cipher Choice*: Triple-DES [23] is too slow for software implementation in embedded medical PDAs or sensors. We found RC5 [23] and SkipJack[8] to be most appropriate for embedded microcontrollers. Although RC5 is slightly faster, it is patented. Also, for good performance, RC5 requires the key schedule to be precomputed, which uses 104 extra bytes of RAM per key. Because of these drawbacks, we selected Skipjack.

It is difficult to directly measure energy consumption of security mechanisms from sensors. We have, thus, resorted to an accurate simulator called Power Tossim [24], where hardware peripherals (such as the radio, EEPROM, LEDs, and so forth) are instrumented to obtain a trace of each device's activity during the simulation run. Through the obtained real-time traces of the current drawn in our SkipJack-based symmetric crypto and RSA-based symmetric crypto [23], we have computed the energy consumption of major components (such as CPU idle, CPU active, radio, etc.) in sensors (see Table I). From Table I, we can see that for the two most important components, i.e., CPU active and radio transmission, our proposed security scheme shows significant power-saving improvements over RSA security scheme (the energy efficiency is improved by 92% and 154%, respectively).

TABLE I
SECURITY ENERGY CONSUMPTION COMPARISONS

(in milli-joules *mJ*)	RSA	Skipjack
CPU active data processing	51	26
Radio communications	2542	1002
Memory access	25	11
Total	2618	1039

C. Wireless Cardiac Data Transmission Security: "Multipatient" Case

To get closer to the real telecardiology MANET scenario, we have extended the above single-patient transmission security to a multipatient case. It is challenging to securely deliver data from an ECG sensor to an Internet Gateway through multihop transmission, as it requires integration of the security scheme with energy-efficient TSN routing protocols.

In our security scheme, we partition patients' sensors into a number of "clusters." In each cluster, exactly one sensor is chosen as the cluster head (CH). Thus, each sensor only needs one-hop communication to send the ECG signals to its CH, which searches for a neighboring CH for data relay to the Gateway. This cluster-based concept has also been used in many hierarchical routing TSN protocols to save energy. To avoid the battery overusing in a CH, the selection of CH could be rotated periodically among the sensors belonging to the same cluster.

We have used the aforementioned SkipJack to achieve *Intra-cluster Security* (i.e., inside each cluster). For secure data transmission between clusters, an *Inter-Cluster Session Key* (*SK*) is used (see Fig. 12). A new *SK* is periodically distributed to all CHs by the Gateway. All new *SK*s are derived from a *one-way hash function* $H(\cdot)$. The Gateway first precomputes a long one-way sequence of keys: $\{SK_M, SK_{M-1}, \ldots, SK_n, SK_{n-1}, \ldots, SK_0\}$ (size $M \gg n$), where $SK_i = H(SK_{i+1})$. Initially, only SK_n (instead of the whole M-size key sequence) is distributed to each CH. Then, a CH can utilize $H(\cdot)$ to figure out $SK_{n-1}, \ldots, SK_0$. The n keys $\{SK_n, SK_{n-1}, \ldots, SK_1\}$ are stored in a local *key buffer*. However, SK_0 is not in the buffer because it is used for the *current* data packet encryption/decryption. After the initial SK_n delivery, the Gateway periodically sends $SK_{n+1}, SK_{n+2}, \ldots, SK_M$ (one key distribution in each period) to all CHs.

After receiving a new *SK*, the CH keeps applying $H(\cdot)$ to it for some time, in order to find a key match in its *key buffer*. For instance, assume that a CH receives a new key SK_j and its *key buffer* already holds n *SK*s as follows: $\{SK_i, SK_{i-1}, \ldots, SK_{i-n+1}\}$. If $H(H(H \ldots (H(SK_j))) \notin \{SK_i, SK_{i-1}, \ldots, SK_{i-n+1}\}$, the authentication fails and the SK_j will be discarded. Otherwise, if the authentication is

[8][Online]. Available: http://jya.com/skipjack-spec.htm

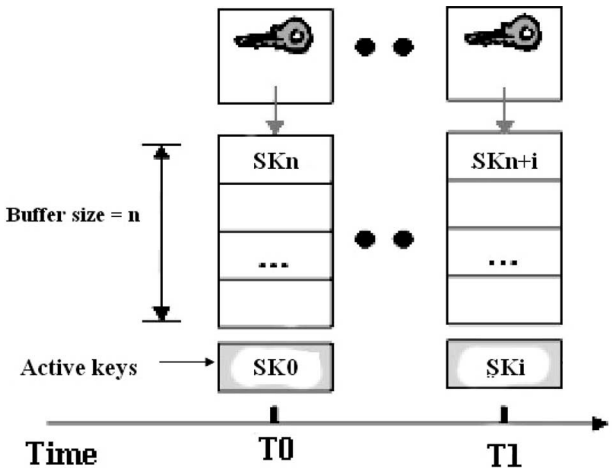

Fig. 12. Key-chain among CHs.

successful, the *key buffer* is shifted one position, and the *SK* shifted out of the buffer is pushed into the "active key slot" to be used as the current *SK* (Fig. 12). The empty position is filled with a new key SK', derived from the received SK_j through H, which meets the following two conditions:

$$SK' = H(H(H(\ldots H(SK_j))) \quad \text{and} \quad H(SK') = SK_i. \tag{10}$$

D. Security Analysis

1) Gateway Attacks: Because the distribution of new *SK*s is managed by the Gateway, it is possible for an attacker to compromise the Gateway and, thus, attack any future *SK* disclosures. Owing to the *SK* buffer, there is a delay between receiving the new *SK* and actually using it. If the distribution interval is Δ' (i.e., the rekeying period) and n is the buffer length, the new *SK* will not be used until $n \times \Delta'$ later. As long as we can detect the Gateway compromise within $n \times \Delta'$ time interval and renew *SK*s, the cardiac data packets will maintain security performance.

2) SK Attacks Among CHs: The attacker may modify the transmitting *SK*, inject phony *SK*, or use wireless channel interference to damage security packets. Our scheme can easily defeat these attacks. Owing to the one-way characteristics of the hash function keys, any false *SK*s cannot pass the *authentication test*, i.e., after L times ($L \leq n$) of using hash function, if we still cannot satisfy the following formula, we will regard that it is a false *SK*:

$$\underbrace{H(H(\ldots(H}_{L}(\mathrm{SK_{FAKE}})\ldots))) = \mathrm{SK_{NOW}}. \tag{11}$$

where $\mathrm{SK_{FAKE}}$ is a false *SK*, and $\mathrm{SK_{NOW}}$ is the currently used *SK*.

3) Cardiac Packet Attacks (such as faking the ECG data): Our scheme defeats it through *SK* rekeying every Δ', and inclusion of *Sensor_ID* and per-packet *IV* (which will also be updated from packet to packet) in the generation of key-streams to counter the key-stream reuse problem.

4) Main-in-the-Middle Attacks: Our scheme can also defeat main-in-the-middle attacks (where an attacker fools the CHs as if he/she were a legal CH). Our strategy is to perform a transmission of ***MAC*** in the rekeying procedure as

$$\text{Gateway} \rightarrow CH: E(\Delta'|n|SK_0|MAC(\Delta'|n|SK_0)). \tag{12}$$

V. Conclusion

The objective of this research was to take advantage of the modern low-cost low-power sensor and wireless communication technology to create a TSN for ECG monitoring purposes. Our TSN system has the potential to provide continuous vital sign monitoring capabilities without the exhaustion of any manpower. In fact, it is intended to give support to the current healthcare environments and free medical professionals for more urgent functions. By automating the vital sign monitoring process, the most updated information for all patients is made available *at all times*. Based on wireless sensor network technology, wearable *mobile platforms* are distributed to the patients of concern. These mobile platforms are responsible for gathering patient vital sign using a three-lead ECG monitoring system. The gathered data are transmitted wirelessly over radio to the receiving station connected to a workstation where the data are processed. ECG feature-extraction/classification techniques are applied to the patient data, and the characteristic points of interests extracted. These data provide meaningful information for the diagnosis of possible cardiovascular diseases. This is especially useful for extended recordings of ECG signals where human processing is not only time consuming for some tasks such as analyzing nonlife threatening rhythms (for example, the frequency and duration of A-Fib), but also error prone. In addition to these functionalities, the system is designed to also provide security measurements against malicious attacks and stealing of patient information.

References

[1] M. G. Hunink, L. Goldman, A. N. Tosteson, M. A. Mittleman, P. A. Goldman, L. W. Williams, J. Tsevat, and M. C. Weinstein, "The recent decline in mortality from coronary heart disease, 1980–1990. The effect of secular trends in risk factors and treatment," *J. Am. Med. Assoc.*, vol. 277, pp. 535–542, 1997.

[2] L. A. Short and E. H. Saindon, "Telehomecare rewards and risks," *Caring*, vol. 17, no. 42, pp. 36–40, 1998.

[3] R. Fensli, E. Gunnarson, O. Hejlesen *et al.*, "A wireless ECG system for continuous event recording and communication to a clinical alarm station," in *Proc. IEEE EMBS*, vol. 1, San Francisco, CA, Sep. 1–5, 2004, vol. 1, pp. 1–4.

[4] R. Fensli, E. Gunnarson, and T. Gundersen, "A wearable ECG-recording system for continuous arrhythmia monitoring in a wireless tele-home-care situation," in *Proc. IEEE Int. Symp. Comput.-Based Med. Syst.*, Dublin, Ireland, Jun. 23–24, 2005, pp. 407–412.

[5] T. Gao, D. Greenspan, M. Welsh, R. R. Juang, and A. Alm, "Vital signs monitoring and patient tracking over a wireless network," in *Proc. 27th Annu. Int. Conf. IEEE EMBS*, Shanghai, China, Sep. 2005, pp. 102–105.

[6] T. Martin, E. Jovanov, and D. Raskovic, "Issues in wearable computing for medical monitoring applications: A case study of a wearable ECG monitoring device," in *Proc Int. Symp. Wearable Comput.*, Atlanta, GA, 2000, pp. 43–50.

[7] M. Welsh B. Chen *et al.*, "CodeBlue: Wireless sensor networks for medical care," Div. Eng. Appl. Sci., Harvard Univ. Cambridge, MA, 2006.

[8] MEMS technology. (2006). [Online]. Available: http://www.memsnet.org/mems/ what-is.html

[9] A. J. Joshi, "Data mining of biomedical signals," Ph.D. Study Progress Rep., Indian Inst. Technol., Mumbai, India, Aug. 27, 2005.
[10] C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Min. Knowl. Discovery*, vol. 2, no. 2, pp. 121–167, 1998.
[11] A. J. Joshi, "Data mining of biomedical signals," Ph.D. Study 2nd Progress Rep., Indian Inst. Technol., Mumbai, India, Aug. 27 2005.
[12] S. R. Gunn, "Support vector machines for classification and regression," Support vector machines for classification and regression, Southampton, U.K., Tech. Rep., May 1998.
[13] A. Arneodo, E. Bacry, and J. F. Muzy, "The thermodynamics of fractals revisited with wavelets," *Physica A*, vol. 213, no. 1, pp. 232–275, 1995.
[14] Z. R. Struzik, "Determining local singularity strengths and their spectra with the wavelet transform," *Fractals*, vol. 8, no. 2, pp. 163–179, 2000.
[15] The research resource for complex physiologic signals (Sep. 8, 2004). PhysioNet. [Online]. Available: http://www.physionet.org
[16] T. M. Mitchell, *Machine Learning*. New York: McGraw Hill, 1997.
[17] R. Le Blanc, "Quantitative analysis of cardiac arrhythmias," *CRC: Crit. Rev. Bioeng.*, vol. 14, no. 1, pp. 1–43, 1986.
[18] Office for Civil Rights—HIPAA. (2006). Medical privacy—National Standards to protect the privacy of personal health information. [Online]. Available: http://www.hhs.gov/ocr/hipaa/finalreg.html
[19] F. Hu, Y. Wang, and H. Wu, "Mobile telemedicine sensing sensor networks with low-energy data query and network lifetime considerations," *IEEE Trans. Mobile Comput.*, vol. 5, no. 4, pp. 404–417, Apr. 2006.
[20] S. Lakdawala, "Low-power wireless sensor hardware/software platform for heart disease monitoring: an intelligent data processing interface" Master's thesis, Dep. Comput. Eng., Rochester Inst. of Technol., Rochester, NY, May 2005.
[21] L. Kleinrock and J. Silvester, "Spatial reuse in multihop packet radio networks," *Proc. IEEE*, vol. 75, no. 1, pp. 156–167, Jan. 1987.
[22] M. B. Srivastava, "Tutorial 7: Energy efficiency in mobile computing and networking," presented at the ACM Mobicom, Rome, Italy, Jul. 2001.
[23] Bruce Schneier, *Applied Cryptography*, 2nd ed. Hoboken, NJ: Wiley, 1996.
[24] V. Shnayder *et al.*, "Simulating the power consumption of large-scale sensor network applications," in *Proc. SenSys*, Baltimore, MD, Nov. 2004, pp. 188–200.

Fei Hu (M'99) received the first Ph.D. degree from the Department of Telecommunication Engineering, Shanghai Tongji University, Shanghai, China, in 1999 and the second Ph.D. degree from the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, in 2002.

He is currently an Assistant Professor with the Department of Computer Engineering, Rochester Institute of Technology, Rochester, NY. His research interests include wireless telemedicine, cognitive radios, ad hoc sensor networks, 3G wireless and mobile networks, and network security.

Meng Jiang (M'06) is currently a Graduate student in the Department of Computer Engineering at Rochester Institute of Technology, Rochester, NY.

His research interests include wireless telemedicine and wireless sensor networks.

Mark Wagner (M'07) received the M.S. degree from the Department of Mechanical Engineering, Clarkson University, Potsdam, NY, in 1998.

He was with IBM, Inc., in 1999. He is currently the President of Sensorcon, Inc.,˜Reading, MA. His research interests include low-power sensors and wireless communications.

De-Cun Dong (M'90–SM'99) received the Ph.D. degree from Northern Jiaotong University, Beijing, China, in 1996.

He is currently the Dean of Transportation Engineering Institute at Tongji University, Shanghai, China. His research interests include computer applications for the blind, transportation information automation, computer networking database, and digital signal processing for telemedicine.

Dr. Dong has received five awards of the Shanghai Frontier Computer Scientists in the last ten years.