Wireless Telemedicine System: An Accurate, Reliable and Secure Real-time Health Care

Huyu Qu[1], Le Yi Wang[2], Christopher M. Klaus[3], Qiang Cheng[4], Ece Yaprak[5] and Hong Wang[6]
[1]*Scanning and Mobility Division, Honeywell International Inc., Cupertino*
[2]*Department of Electrical and Computer Engineering, Wayne State University, Detroit*
[3]*Drighten Research Inc., DeKalb*
[4]*CS Department, Southern Illinois University, Carbondale*
[5]*Division of Engineering Technology, Wayne State University, Detroit*
[6]*Department of Anesthesiology, Wayne State University, Detroit*
USA

1. Introduction

Rapid development in telecommunication technologies, especially wireless communications, has made remote monitoring of patient vital signs feasible. When a signal is transmitted through a communication channel, accuracy of information transmission at the receiver is one of the most significant issues. For medical diagnosis, errors in signal processing and communications introduce substantial artifacts, making pattern recognition and diagnosis less reliable, leading potentially to an erroneous diagnosis. Consequently, when system resources are limited, such as transmission bandwidths, appropriate utility of available resources becomes imperative to ensure accuracy of information.

For a given communication bandwidth, the communication system can first process original medical signals by waveform transformation, data compression, and quantization to reduce the data size, which will result in a reduced rate of data transmission through communication channels, but introduce more information processing errors. This chapter analyzes fundamental relationships between accuracy of information exchange and available resources on a platform of wireless local area network (WLAN) systems that involve typical function blocks of discrete cosine transform, data compression, magnitude quantization, stochastic WLAN channels, and inverse discrete cosine transform. The main complexity relationships developed in this chapter provide a trade-off between resource consumptions and information processing errors, and a strategy for optimal allocation of resources.

An example of these relationships is simulated in a typical medical diagnosis problem using lung sounds. Respiratory sounds contain a rich reservoir of vital physiological and pathological information that is of critical importance for clinical diagnosis and patient management in operating rooms (OR). Several research groups have investigated potential computer-assisted sound analysis and classifications for asthma, cystic fibrosis, pneumonia, etc. (17; 19; 24). This chapter evaluates the impact of communication channels on diagnostic accuracy and the benefits of studying signal processing and communications in an integrated framework. The main findings of this chapter indicate that effective utility of communication resources is essential for tele-monitoring and telemedicine when the communication bandwidth is shared by many users, and hence is very limited for each connection.

There are extensive efforts in studying integrated information processing and communication systems, especially in feedback control. For example Firoozbakhsh et al. (7) provided a versatile framework for incorporation of sensing, monitoring, information processing and wireless communication devices. Sayeed (22) proposed a signal modeling framework for sensor networks that interact between space-time signal sampling, distributed signal processing, and communications. This chapter is focused on a stochastic analysis and simulation of complexity relationships among typical components on integrated medical information processing and communication systems. A stochastic optimization problem is formulated that explicitly relates communication resources to information transmission accuracy. Solutions to the optimization problem leads to a strategy of communication resource allocation. A typical medical diagnostic problem on lung sounds is used, in combination with a standard IEEE 802.11b WLAN network simulation model, to show the utility of this strategy by finding the optimal resource allocation between compression ratios (and/or quantization levels) and transmission rates.

WLAN standards allow freedom for laptops, computers on wheels, medical sensor nodes and other medical equipment to efficiently roam through hospitals, but encounter potential vulnerabilities of wireless beds, wireless medication robots, wireless I.V.s, wireless heart monitoring & medication devices, and various other wireless medical technologies. There are several common security threats to WLAN networks, such as eavesdropping, denial of service, theft of service, etc., revealing weakness of the current security methods (RADIUS servers, MAC filtering, etc.). Even proprietary systems have been shown to quickly succumb to attacks. Control systems, which are the basis for medical equipment, also have weaknesses that allow unauthorized control via these WLAN networks. As such, transmitting and receiving a medical signal via an open medium like Wi-Fi is a critical concern. Interference with these systems from congestion to outright manipulation of medical information can not only put private medical information (PMI) at risk but also patients' lives in peril. WiFi-based telemedicine systems need to be immune from deny of service attacks, and provide service all the time. Any kind of congestion is intolerable. Moreover, the privacy medical data should not be intercepted and eavesdropped. As such, it is essential to have a multi-layered defense starting with conventional security tactics to the implementation of more in-depth methods like wireless covert channel signaling and wireless self protection systems. By increasing wireless network security in this way, vulnerabilities of medical equipment and sensor nodes can be significantly reduced to help ensure medical services are secure and available when needed.

The remainder of the chapter is organized as follows. Section 2 introduces the basic system settings for an integrated wireless-based medical information system. The main mathematics models of the system modules are described. The trade-offs of compression errors and compression ratios, quantization errors and quantization levels, transmission errors and transmission rate as well as power levels are established in a stochastic framework. An optimization problem for resource allocations to achieve overall error reduction is presented. A standard IEEE 802.11b WLAN is used as a communication channel to illustrate the usefulness of optimal resource allocations. An example of uniformly distributed signals through a 1Mbps WLAN channel is employed to show the optimal choice of quantization levels. Section 3 focuses on the integrated medical systems for diagnosis. A lung sound signal is transmitted through a simulation model of WLAN-based medical information systems in three different scenarios. The trade-offs among compression ratios, quantization levels, transmission rates, and signal-to-noise ratios are demonstrated in a stochastic framework. The overall error reduction can be achieved by optimizing information and resource allocations. The impact of information processing and transmission errors on medical pattern recognition and diagnosis accuracy is discussed. Session 4 discusses security weakness and security enhancement methods in WLAN-based telemedicine system, and talks about the secure roaming among different access points. Session 5 briefly summarizes the findings of the chapter.

2. Integrated and wireless-based medical information systems

2.1 Mathematics models and error analysis of communication systems

A typical integrated system of information processing and wireless communications is shown in Figure 1. The input sequence $u = \{u_k : k = 1, \ldots, L_0\}$ belongs to an input ensemble $\mathbf{U}$. For system analysis, the length L_0 of $u \in \mathbf{U}$ is assumed to be fixed and known. This represents the size of a signal or the number of samples in a fixed time interval T. Hence, $f = L_0/T$ will be the data sampling rate. The probability of occurrence of a specific sequence $u \in \mathbf{U}$ will be denoted by $P\{u\}$. The following typical components of communications will be considered in this chapter, and their accuracy and complexity will be analyzed.

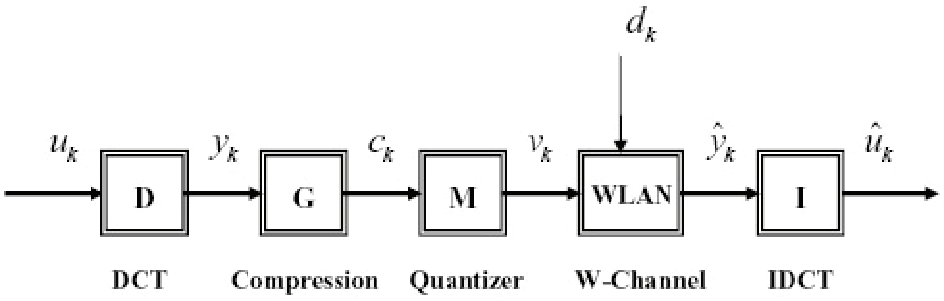


Fig. 1. System blocks

Discrete Cosine Transform

Several algorithms of transform data compression (TDC), such as fast Fourier transform (FFT), discrete sine transform (DST), discrete cosine transform (DCT), 2D discrete cosine transform (DCT2), etc., were compared in (29), showing that DCT has least compression errors in most cases for medical signals. As a result, the DCT algorithm is used in our system modeling.
The input data block $u = \{u_k : k = 1, \ldots, L_0\}$ of medical signals passes a DCT block to generate a coefficient sequence $y = \{y_k : k = 1, \ldots, L_0\}$.

$$y_k = D(u) = 2\sum_{n=0}^{L_0-1} a_n u_n \cos\left(\frac{\pi k n}{L_0 - 1}\right), \quad 0 \le k \le L_0 - 1, \tag{1}$$

where $a_n = \begin{cases} 1/2, & n = 1 \text{ and } L_0 - 1; \\ 2, & 2 \le n \le L_0 - 2. \end{cases}$

The DCT coefficient sequence $y = \{y_k, k = 0, \ldots, L_0 - 1\}$ belongs to an ensemble $\mathbb{Y}$, and $\mathbb{Y}$ is uniformly bounded by $\sup_{y \in \mathbb{Y}} \max_{k=0,\ldots,L_0-1} |y_k| \leq y_{max}$. The length of $y \in \mathbb{Y}$ is same as the input sequence u.

Data Compression

To reduce data sizes, y is first compressed. In this chapter, we will use the following scheme of truncation in data compression for concreteness of analysis, although the main tools of analysis can be readily extended to other data compression schemes. For a given threshold ε,

$$c_k = G(y_k) = \begin{cases} y_k, & \text{if } |y_k| > \varepsilon \\ 0, & \text{if } |y_k| \leq \varepsilon \end{cases} \tag{2}$$

The length N of c depends on y with $N \leq L_0$, and hence is a random variable. The average data compression ratio is defined as the expected value of N/L_0

$$\mu = E\left(\frac{N}{L_0}\right) = \sum_{y \in \mathbb{Y}} \frac{N}{L_0} P(y).$$

Observe that for any given $y \in \mathbb{Y}$, N is a monotone non-increasing function of ε. Namely, the larger the threshold ε, the shorter the compressed sequence. As a result, μ is a monotone non-increasing function of ε. This function will be denoted by $\mu = h(\varepsilon)$. $h(\varepsilon)$ represents the *compressability function* of the input ensemble $\mathbb{Y}$. The main information we need for subsequent complexity analysis, in terms of data compression, is this compressability function. Typical compressability functions are shown in Figure 2.

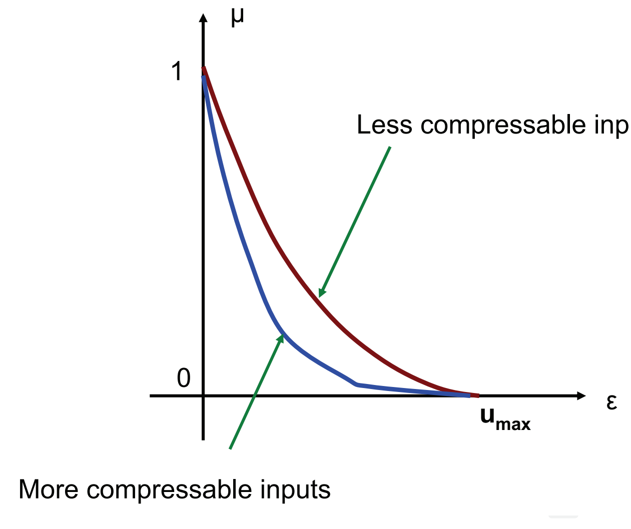


Fig. 2. Typical compressability functions

Data Quantization

Before transmission, c_k is first quantized. Suppose that the signal range $[-y_{max}, y_{max}]$ is divided into m equally spaced intervals of length $\delta = 2y_{max}/m$. Quantization output sequences take m possible values $Q = \{q_j : j = 1, \ldots, m\}$, defined by

$$q_j = -y_{max} + (j - 0.5)\delta, j = 1, \ldots, m. \tag{3}$$

The quantization maps $c_k \in [-y_{max}, y_{max}]$ into its nearest element in Q. The complexity of quantization is characterized by the size m of Q, or $l = \log_2 m$ in bits. The quantization errors are bounded by $\delta/2 = y_{max}/m = y_{max}/2^l$, hence is inversely proportional to m.

Data Transmission

The output of the quantization process is $v_k = M(c_k)$, which will be transmitted through a WLAN channel, whose output sequence will be denoted by w_k. At a system level, a DMC (discrete memoryless channel) can be modeled by its transmission conditional probability matrix:

$$\Phi = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & \cdots & & \vdots \\ p_{m1} & p_{m2} & \cdots & p_{mm} \end{bmatrix}. \tag{4}$$

where $p_{ij} = P\{y_k = q_i | v_k = q_j\}$, that is, the conditional probability of receiving q_i when q_j is transmitted.

It should be emphasized that this is a system-level representation of the communication channel. The physical-level channel may vary. For instance, if the underlying modulation scheme is a BPSK (bi-phase shift keying) modulation, then a binary memoryless channel model may be used in representing the physical-level channel, with a probability matrix

$$\Phi_0 = \begin{bmatrix} p_{11}^0 & p_{12}^0 \\ p_{21}^0 & p_{22}^0 \end{bmatrix}. \tag{5}$$

In this case, v_k, that takes m possible values, will be represented by a binary sequence of length $l = \log_2 m$ for transmission. The matrix Φ in (4) can be derived from Φ_0 as the l-tuple Cartesian product $\Phi = \Phi_0 \otimes \cdots \otimes \Phi_0$. Similar discussions (26) can be made for DBPSK (differential bi-phase shift keying), DQPSK (differential quandary phase shift keying) modulation, or other modulation schemes which are used in IEEE 802.11b WLAN.

Inverse Discrete Cosine Transform

The received sequence $w = \{w_k : k = 0, \ldots, N-1\}$ of the wireless channel are processed through the inverse cosine transform block to recover the original time-domain signal sequence $\widetilde{u} = \{\widetilde{u}_k : k = 0, \ldots, N-1\}$.

$$\widetilde{u}_k = I(\widetilde{y}) = \frac{1}{N-1} \sum_{n=0}^{N-1} a_n \widetilde{y}_n \cos\left(\frac{\pi k n}{N-1}\right), \quad 0 \le k \le N-1, \tag{6}$$

where $a_n = \begin{cases} 1/2, & n = 0 \text{ and } N-1; \\ 2, & 2 \le n \le N-2. \end{cases}$

2.2 Relations between errors and complexity: Analysis and optimization

2.2.1 Information accuracy and complexity

Assumption A: DCT and IDCT do not involve errors.

Under assumption A, only data compression, quantization, and communications introduce errors in information representation and transmission. The sizes of the errors depend on certain complexity measures of the operations. In particular, data compression introduces compression errors that increase when the compression ratio μ decreases. Quantization errors increase when the quantization complexity m decreases. Communication errors increase when the signal/noise ratio decreases, or the transmission rate increases, or the assigned bandwidth decreases. We shall start with a more precise description of these errors.

- **Compression Errors and Compression Ratios**

  Assume that y_k takes values in $[-y_{max}, y_{max}]$ with a probability density $f_c(x)$ that is an even function and the sequence $\{y_k\}$ is independent and identically distributed (i.i.d.). The compression error $e_k^c = y_k - c_k = y_k - G(y_k)$ has mean

  $$Ee_k^c = \int_{-y_{max}}^{y_{max}} (x - G(x)) f_c(x) dx = \int_{-\varepsilon}^{\varepsilon} x f_c(x) dx = 0,$$

  and variance

  $$\sigma_c^2 = E(e_k^c)^2 = \int_{-y_{max}}^{y_{max}} (x - G(x))^2 f_c(x) dx = \int_{-\varepsilon}^{\varepsilon} x^2 f_c(x) dx = S_c(\varepsilon).$$

  It follows that the variance is

  $$\sigma_c^2 = E(e_k^c)^2 = \int_{-y_{max}}^{y_{max}} (x - G(x))^2 \frac{1}{2y_{max}} dx = \int_{-\varepsilon}^{\varepsilon} x^2 \frac{1}{2y_{max}} dx = \frac{2\varepsilon^3}{3} \frac{1}{2y_{max}} = \frac{\varepsilon^3}{3y_{max}}.$$

  Combining the relationship between σ_c^2 and ε with the compressability function $\mu = h(\varepsilon)$, assuming $h(\cdot)$ is invertible in the range $[0, y_{max}]$, we have a complexity relationship

  $$\sigma_c^2 = S_c(\varepsilon) = S_c(h^{-1}(\mu)) := \lambda_c(\mu). \tag{7}$$

- **Quantization Errors and Complexity**

  The quantization error $e_k^q = c_k - M(c_k)$ is bounded by $|e_k^q| \leq \delta/2$. Suppose that e_k^q is i.i.d. with a density function $f_q(x)$ that is an even function on $[-\delta/2, \delta/2]$ (31). Then the mean and variance of e_k^q can be derived as $E(e_k^q) = 0$ and

  $$\sigma_q^2 = E(e_k^q)^2 = \int_{-\delta/2}^{\delta/2} x^2 f_q(x) dx = S_q(\delta) = S_q(2y_{max}/m) := \lambda_q(m), \tag{8}$$

  noting that $\delta = 2y_{max}/m$. The function $\sigma_q^2 = \lambda_q(m)$ defines the complexity relationship for quantization. For example, if e_k^q is uniformly distributed, then $f_q(x) = 1/\delta$ and

  $$\sigma_q^2 = \int_{-\delta/2}^{\delta/2} \frac{x^2}{\delta} dx = \frac{\delta^2}{12} = \frac{y_{max}^2}{3m^2} = \frac{y_{max}^2}{3} 2^{-2l}.$$

- **Transmission Errors and Communication Power and Bandwidth**

  The impact of signal power and bandwidth on the transmission channels is typically summarized in the normalized signal-to-noise ratio E_s/N_0, where E_s is energy per symbol and N_0 is average noise power per unit bandwidth. This parameter defines the communication complexity or resource requirements since signal power and bandwidth are the key resources in a communication system. For a given physical level modulation, the transmission matrix Φ defined in (4) depends on E_s/N_0 and may be expressed as

$\Phi(E_s/N_0)$. Intuitively, the larger the signal-to-noise ratio E_s/N_0 is, the closer the matrix Φ is to the identity matrix.

To understand the transmission errors, we note that if $v_k = q_j$ occurs with probability $p_j = P\{q_j\}$ and q_j is transmitted, then the output $\widehat{y}_k$ may take any values in Q with probability $P\{\widehat{y}_k = q_i | v_k = q_j\} = p_{ij}$ and error $e_k^t = q_j - q_i$. It follows that the conditional mean squares error $E[(e_k^t)^2 | q_j] = \sum_{i=1}^m (q_j - q_i)^2 p_{ij}$. Consequently, the overall mean squares error is $E[(e_k^t)^2] = \sum_{j=1}^m \sum_{i=1}^m (q_j - q_i)^2 p_{ij} p_j$. The last quantity depends on the input probability distribution $p = \{p_1, \ldots, p_m : p_j \geq 0 \text{ and } p_1 + \cdots + p_m = 1\}$. A characterizing quantity for the transmission error is the worst-case mean squares error

$$\sup_p E[(e_k^t)^2] = \sup_p \sum_{j=1}^m \sum_{i=1}^m (q_j - q_i)^2 p_{ij} p_j \leq \max_{j=1,2,..m} \sum_{i=1}^m (q_j - q_i)^2 p_{ij} := \sigma_t^2. \tag{9}$$

It is noted that since Φ is a function of signal-to-noise ratio E_s/N_0 and transmission rate which is determined by compression ratio μ and quantization level m, so is σ_t^2. This dependence will be denoted by

$$\sigma_t^2 = \lambda_t(E_s/N_0, \mu, m). \tag{10}$$

For some typical communication modulation schemes, we will derive explicit expressions for $\lambda_t(E_s/N_0, \mu, m)$ in subsequent sections.

2.2.2 Optimal resource allocations

Assumption B: Compression errors, quantization errors and transmission errors are independent.

Under assumption B, the overall errors in the integrated information processing and communication system can be derived as follows:

$$e_k = y_k - \widehat{y}_k = y_k - c_k + c_k - v_k + v_k - \widehat{y}_k = e_k^c + e_k^q + e_k^t,$$

where e_k^c is compression error, e_k^q is quantization error (31), and e_k^t is transmission error. Hence, under assumption B, and under the worst-case input distributions, the mean squares error is

$$\sigma^2 = \sup_p E e_k^2 = E(e_k^c)^2 + E(e_k^q)^2 + E(e_k^t)^2 = \sigma_c^2 + \sigma_q^2 + \sigma_t^2. \tag{11}$$

where σ_c^2, σ_q^2, and σ_t^2 is mean square errors for compression, quantization and transmission respectively. By substituting the complexity relationships (7), (8), and (10) into this expression, we obtain an overall complexity function

$$\sigma^2 = \lambda\left(\mu, m, \frac{E_s}{N_0}\right) = \lambda_c(\mu) + \lambda_q(m) + \lambda_t\left(\frac{E_s}{N_0}, \mu, m\right). \tag{12}$$

For a given communication resource, compression ratio μ and quantization level in bits $\log_2^m$ are inversely proportional to each other for a particular transmission rate, namely $\mu * \log_2^m = C$, and C is determined by the assigned channel bandwidth and the selected modulation method. In order to minimize the overall mean squares error, we shall minimize the following performance index:

$$\min_{\mu,m}\left[\lambda\left(\mu,m,\frac{E_s}{N_0}\right)\right]=\min_{m}\left[\lambda_c\left(\frac{C}{\log_2^m}\right)+\lambda_q(m)+\lambda_t\left(\frac{E_s}{N_0},\frac{C}{\log_2^m},m\right)\right]. \tag{13}$$

2.3 Mathematical analysis of WLAN-based medical information systems

2.3.1 Typical modulation schemes and channel models

In digital communication systems, popular modulation schemes include phase shift keying (PSK), frequency shift keying (FSK), amplitude shift keying (ASK), continuous phase modulation (CPM), and some hybrid combinations such as quadrature amplitude modulation (QAM). For every modulation scheme there are several sub-modulation methods, for example, PSK includes bi-phase shift keying (BPSK), quadri-phase shift keying (QPSK), multiple phase shift keying (MPSK), differential PSK (DPSK), etc.

Suppose that a memoryless symmetric binary channel transmits $x_k = a > 0$ for the bit $v_k = 1$ and $x_k = -a$ for the bit $v_k = 0$. The output of the channel is $w_k = x_k + d_k$, where d_k is the additive channel noise. The decoding scheme is that $\widehat{y}_k = 1$ if $w_k \geq 0$, and $\widehat{y}_k = 0$ if $w_k < 0$. d_k is assumed to be i.i.d., zero mean, and has finite second moments. The probability density function of d_1 is $f_d(x)$, which is symmetric to the origin. The accumulative probability distribution is denoted by $F(x)$. Consequently, the probabilities of transmission errors can be derived as

$$P\{\widehat{y}_k=0|v_k=1\}= P\{w_k<0|x_k=a\}=P\{d_k<-a\}=\int_{-\infty}^{-a}f_d(x)dx=F(-a):=p_e.$$

$$P\{\widehat{y}_k=1|v_k=0\}= P\{w_k\geq 0|x_k=-a\}=P\{d_k\geq a\}=\int_{a}^{\infty}f_d(x)dx=F(a):=p_e.$$

since $f_d(x)$ is symmetric.

For example, if the disturbance is Gaussian distributed with variance σ^2, its probability density function is

$$f_d(x)=\frac{1}{\sqrt{2\pi\sigma}}e^{-x^2/\sigma^2}. \tag{14}$$

It follows that $p_e = \int_a^\infty f_d(x)dx = Q(a/\sigma)$ where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\tau^2/2}d\tau$ is called the complementary error function.

In a typical BPSK modulation (11), $\sigma = \sqrt{\frac{N_0}{2T_b}}$, where $T_b = \frac{1}{R}$ and R is the transmission rate. In this case,

$$p_e=Q(a/\sigma)=Q\left(a/\sqrt{\frac{N_0}{2T_b}}\right).$$

For BPSK energy per symbol $E_s = a^2T_b$, and symbol error probability is

$$p_e=Q\left(\sqrt{\frac{2E_s}{N_0}}\right). \tag{15}$$

Consequently, the probability transition matrix Φ in (5) under BPSK modulation is $\Phi = \begin{bmatrix} 1-p_e & p_e \\ p_e & 1-p_e \end{bmatrix}$.

Similarly, the symbol error probability for differential binary PSK (DBPSK) modulation is (23)

$$p_e = \frac{1}{2} exp\left(-\frac{E_s}{N_0}\right). \tag{16}$$

The symbol error probability for M-ary PSK (MPSK) modulation is

$$p_e \approx 2Q\left(\sqrt{\frac{2E_s}{N_o}} sin\left(\frac{\pi}{M}\right)\right), \tag{17}$$

and the symbol error probability for M-ary DPSK (DMPSK) modulation is (15)

$$p_e \approx 2Q\left(\sqrt{\frac{2E_s}{N_o}} sin\left(\frac{\pi}{\sqrt{2}M}\right)\right), \tag{18}$$

where M is is the size of symbol set.

2.3.2 Transmission errors of WLAN(802.11b) integrated systems

To simplify our analysis we use IEEE 802.11b WLAN as a typical communication environment (802.11a, 802.11g or 802.11n will have similar results). There are four transmission rates, 1Mbps, 2Mbps, 5.5Mbps and 11Mbps, in IEEE 802.11b WLAN. Different transmission rates use different modulation methods (38). When the transmission rate equals 1Mbps, DBPSK modulation and DSSS (direct-sequence spread spectrum) are used. When the transmission rate equals 2Mbps, DQPSK (differential quandary PSK) modulation and DSSS are used. When the transmission rate equals 5.5Mbps and 11Mbps, combined PSK and CCK (complementary code keying) are used. Precise evaluation of symbol errors of each transmission rate is a complex problem. Here we analyze the transmission errors of DBPSK and DQPSK modulations as examples.

1. **System Analysis under DBPSK Modulation**

   The probability transition matrix Φ_0 in (5) under DBPSK modulation is similar to that under BPSK modulation, and p_e is given in (16), then

$$\Phi_0 = \begin{bmatrix} 1-p_e & p_e \\ p_e & 1-p_e \end{bmatrix}.$$

   If inputs have only two possible values, i.e. the quantization level m is 2, then matrices Φ and Φ_0 are equal, and by (9)

$$\sigma_t^2 = \sup_{\substack{p_1,p_2 \geq 0 \\ p_1+p_2=1}} \sum_{j=1}^{2} \sum_{i=1}^{2} (q_j - q_i)^2 p_{ij} p_j = (q_2 - q_1)^2 p_e (p_1 + p_2) = (q_2 - q_1)^2 p_e.$$

   Since $p_{12} = p_{21} = p_e$ and $p_1 + p_2 = 1$, by (3), $\sigma_t^2 = (q_2 - q_1)^2 p_e = \delta^2 p_e$. In general, the corresponding elements of the probability transition matrix Φ in (4) under DBPSK modulation is $p_{ij} = (p_e)^\alpha (1-p_e)^{(l-\alpha)}, i, j = 1, 2, .., m$, where l is the number of bits per code, and α is the number of error bits. As a result, the mean squares errors of transmission

(9) is

$$\begin{aligned}
\sigma_t^2 &= \sup_{\substack{p_1,\ldots,p_m \geq 0 \\ p_1+\ldots+p_m=1}} \sum_{j=1}^{m}\sum_{i=1}^{m}(q_j - q_i)^2 p_{ij} p_j \\
&= \sup_{\substack{p_1,\ldots,p_m \geq 0 \\ p_1+\ldots+p_m=1}} \sum_{j=1}^{m}\sum_{i=1}^{m}(q_j - q_i)^2 (p_e)^{\alpha}(1-p_e)^{(l-\alpha)} p_j \\
&= \max_{j=1,..,m} \sum_{i=1}^{m}(q_j - q_i)^2 (p_e)^{\alpha}(1-p_e)^{(l-\alpha)}.
\end{aligned}$$

2. **System Analysis under DQPSK Modulation**
   The probability transition matrix Φ_0 in (5) under DQPSK modulation now becomes a 4 × 4 matrix. We have

$$\Phi_0 = \begin{bmatrix} 1-2p_e-p_e' & p_e & p_e' & p_e \\ p_e & 1-2p_e-p_e' & p_e & p_e' \\ p_e' & p_e & 1-2p_e-p_e' & p_e \\ p_e & p_e' & p_e & 1-2p_e-p_e' \end{bmatrix}.$$

   By equation (18)

$$p_e \approx 2Q\left(\sqrt{\frac{2E_s}{N_o}} sin\left(\frac{\pi}{4\sqrt{2}}\right)\right).$$

   For DQPSK modulation $p_e' \approx p_e^2$, and the transmission error σ_t^2 in equation (9) is

$$\begin{aligned}
\sigma_t^2 &= \sup_{\substack{p_1,\ldots,p_4 \geq 0 \\ p_1+\ldots+p_4=1}} \sum_{j=1}^{4}\sum_{i=1}^{4}(q_j - q_i)^2 p_{ij} p_j \\
&= \max_{j=1,..,4} \sum_{i=1}^{4}(q_j - q_i)^2 p_{ij} \\
&= (q_2 - q_1)^2 p_e + (q_3 - q_1)^2 p_e' + (q_4 - q_1)^2 p_e \\
&= 10\delta^2 p_e + 4\delta^2 p_e'.
\end{aligned}$$

3. **An Illustrative Example: Uniformly Distributed Signals through 1Mbps Rate WLAN Channel (DBPSK Modulation)**
   Suppose a signal is transmitted through a WLAN channel using 1Mbps transmission rate (DBPSK modulation). Assume the input signal v_k is uniformly distributed from 1 to m, where m is quantization level. Then we have $p_j = \frac{1}{m}$, for $j = 1, ..., m$. A quantized value needs $l = log_2 m$ bits to represent, and transmission probability matrix Φ of the WLAN channel is same as matrix (4) with $p_{ij} = P\{y_k = q_i | v_k = q_j\} = (p_e)^{\alpha}(1-p_e)^{(l-\alpha)}$ where α is the number of error bits. If no error occurs after passing through a wireless channel, then $y_k = v_k$, $p_{ij} = (1-p_e)^l$, and $\sum_{i=1}^{m} p_{ij} = 1$. Normally when a quantized value is transmitted through the WLAN channel, the possibility of error transmission is much less than the possibility of error-free transmission, namely, $p_e << 1 - p_e$. Hence, for simplicity we assume that all error possibility for a particular input is $p_{ij} = \frac{1-(1-p_e)^l}{m-1}$ for any $i \neq j$.

When quantization level is m or bits per value are l in our case, p_{ij} is

$$p_{ij} = \begin{cases} (1-p_e)^l & \text{if } q_i = q_j; \\ \frac{1-(1-p_e)^l}{m-1} & \text{if } q_i \neq q_j. \end{cases}$$

The probability matrix (4) becomes

$$\Phi = \begin{bmatrix} (1-p_e)^l & \frac{1-(1-p_e)^l}{m-1} & \cdots & \frac{1-(1-p_e)^l}{m-1} & \frac{1-(1-p_e)^l}{m-1} \\ \frac{1-(1-p_e)^l}{m-1} & (1-p_e)^l & \cdots & \frac{1-(1-p_e)^l}{m-1} & \frac{1-(1-p_e)^l}{m-1} \\ \vdots & & \cdots & & \vdots \\ \frac{1-(1-p_e)^l}{m-1} & \frac{1-(1-p_e)^l}{m-1} & \cdots & \frac{1-(1-p_e)^l}{m-1} & (1-p_e)^l \end{bmatrix}.$$

The transmission error σ_t^2 of (9) is

$$\begin{aligned} \sigma_t^2 &= \sup_{\substack{p_1,\dots,p_m \geq 0 \\ p_1+\dots+p_m=1}} \sum_{j=1}^{m}\sum_{i=1}^{m}(q_j-q_i)^2 p_{ij} p_j \\ &= \frac{1-(1-p_e)^l}{(m-1)m} \sum_{j=1}^{m}\sum_{i=1}^{m}(q_j-q_i)^2 \\ &= \left[\frac{1-(1-p_e)^l}{(m-1)m}\right] \delta^2 \sum_{j=1}^{m}\sum_{i=1}^{m}(j-i)^2 \\ &= \left[\frac{1-(1-p_e)^l}{(m-1)m}\delta^2\right] \left[2L\sum_{i=1}^{m} i^2 - 2\left(\sum_{i=1}^{m} i\right)^2\right] \\ &= \left[\frac{1-(1-p_e)^l}{(m-1)}\delta^2\right] \left[\frac{m(m+1)(2m+1)}{3} - \frac{m(m+1)^2}{2}\right] \\ &= \delta^2 \left[1-(1-p_e)^l\right] \left[\frac{2^l(2^l+1)}{6}\right], \end{aligned}$$

where p_e equals $\frac{1}{2}exp\left(-\frac{E_s}{N_0}\right)$ by equation (16).

To get a general equation of overall error in the studied system, we do not compress the signal here, since as shown in Figure 2, compression ratio μ and compression error σ_c^2 are highly specific to the input signals. The compression ratio will vary greatly for different signals with a given threshold ε. Consequently, the overall error in equation (11) for signal y_k is:

$$\sigma^2 = E[e_k - E(e_k)]^2 = \sigma_q^2 + \sigma_t^2 = \frac{y_{max}^2}{2^{2l}}\left[\frac{1}{3} + 4\left(1-(1-p_e)^l\right)\left(\frac{2^l(2^l+1)}{6}\right)\right].$$

Figure 3 shows the mathematic results for a signal with $y_{max} = 1$. For a given uniformly distributed signal y_k there is an optimized value l to minimize the overall error when

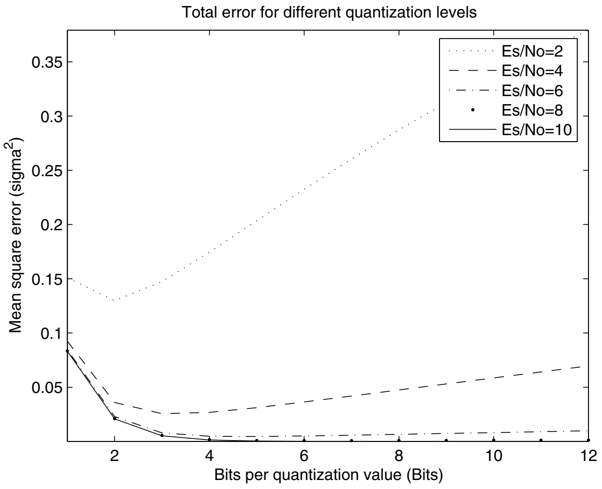


Fig. 3. Optimized quantization levels for Es/No=2, 4, 6, 8, 10

the signals are transmitted through a wireless channel. The optimized values vary with different signal-to-noise ratios.

3. Wireless-based medical information processing: Information accuracy and diagnosis reliability

3.1 WLAN-based medical information system simulation model

An integrated medical information processing and WLAN system is simulated in a MATLAB environment. Similar to the mathematical model in Figure 1, it includes six blocks: DCT block, data compression block, transmitter block (quantizer is included inside) (18), WLAN channel block, receiver block (18), and IDCT block.

The compressed DCT coefficients is embedded into IEEE 802.11b WLAN physical layer frames by adding PLCP (physical layer convergence protocol) preamble and header, modulation and spreading, upsampling and pulse shaping, etc. Packet sizes (1 to 8191 bytes) and preambles can be selected manually. The thermal noise characteristics (additive,white,and Gaussian) are used to model the noise in most wireless systems (13; 23). We simulated the WLAN channel using a memoryless symmetric binary AWGN (add white Gaussian noise) channel. Different channel (1 to 11), different signal-to-noise ratio (-10db to 20 db) and different transmission rates (1Mbps, 2Mbps, 5.5Mbps, and 11Mbps) can be selected. At receiver side, the 802.11b physical layer frames are processed by demodulation and despreading, deframing, removing PLCP preamble and header, etc., to recover the input DCT coefficients from the transmitter, and further through the IDCT block to retrieve the original time-domain medical signals.

1. **Simulation Scenario 1**

   Compression ratios and compression errors are highly specific to the input medical signals. As a result, it is difficult to get a general mathematics equation of compression errors. However, we can study compression effects using our simulation models. For simulation parameters, we select the signal-to-noise ratios to be sufficiently large to avoid errors involved with the WLAN channel. Figure 4 shows simulation results with compression ratio $\mu = 0.2$ (threshold $\varepsilon = 0.0141$). It compares the original time-domain signal and DCT coefficients with the received DCT coefficients and recovered signals, and shows the absolute errors in the fifth sub-figure. The errors in this scenario are mainly introduced through compression (note: in this scenario we set the quantization level to 2^{16}, and the resulting quantization errors are much smaller than the compression errors). We use the percentage RMS difference (PRD), which is calculated as in (19), to evaluate signal distortion. The PRD for the simulated lung sound signal is 2.59% when the compression ratio equals 0.2.

$$PRD(\%) = \sqrt{\frac{\sum_{i=1}^{n}[x_{org}(i) - x_{rec}(i)]^2}{\sum_{i=1}^{n}[x_{org}(i)]^2}} \times 100. \tag{19}$$

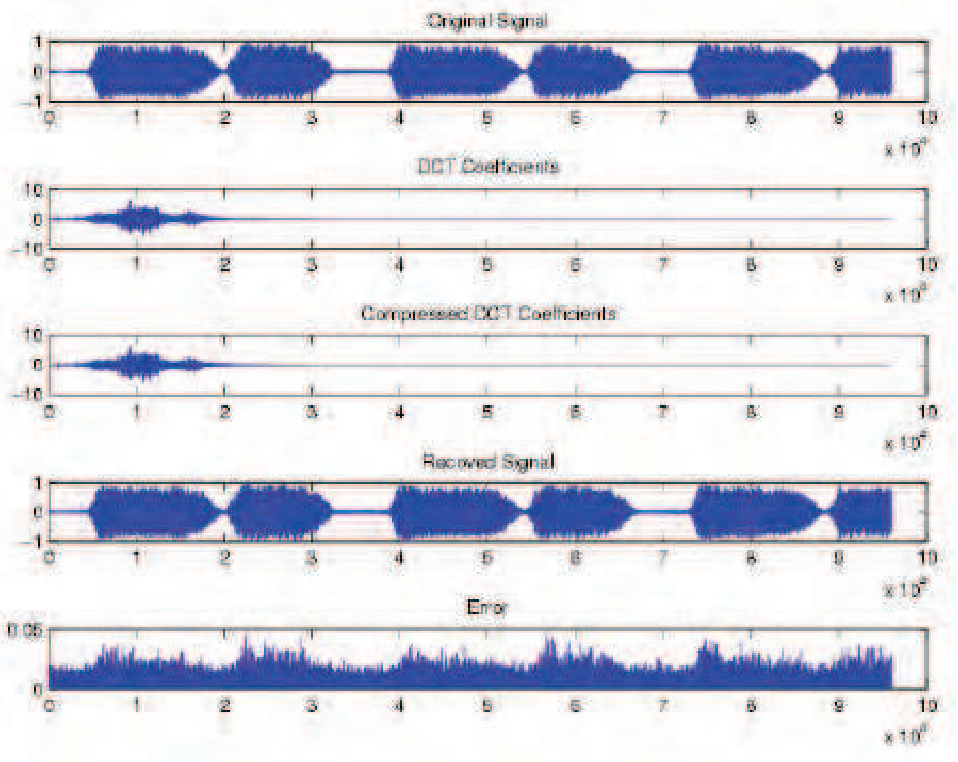


Fig. 4. Lung sound signal compression

For the lung sounds of Figure 4, the simulation results of PRD relationship to the compression ratio are plotted in Figure 5. The signal distortion is a monotone, non-increasing function of the compression ratio.

2. **Simulation Scenario 2**

   Equation (12) shows that the overall complexity is a function of the signal-to-noise ratio. To find the relationship of PRD to E_s/N_o, we transmit the lung sound signal through four WLAN channels (1Mbps, 2Mbps, 5.5Mbps, 11Mbps) with different signal-to-noise ratios. Figure 6 shows the results. In general, the larger the signal-to-noise ratio is, the less the transmission error is. If E_s/N_0 is larger than 12 dB, there is no transmission error on any WLAN channel. If Es/N_0 is smaller than 2 dB, 1Mbps becomes the only reasonable transmission rate. When the environment is noisy, to keep the same PRD value, we must increase the signal strength or transmit the signal at a low transmission rate. This involves an optimization problem between transmission power and transmission rate.

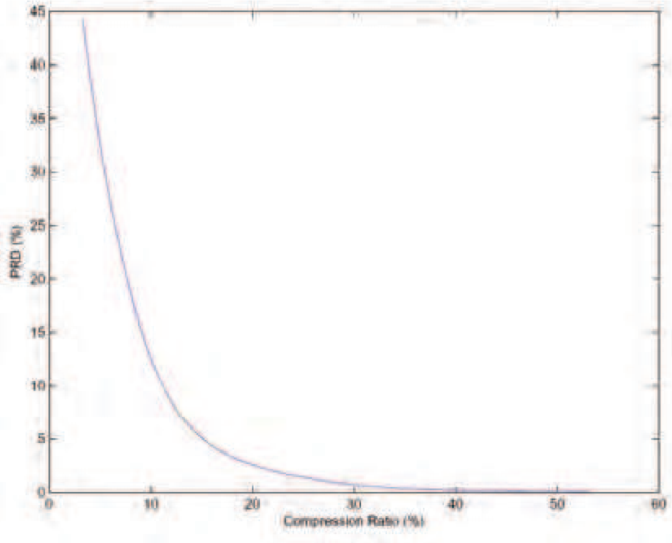


Fig. 5. PRD to compression ratio

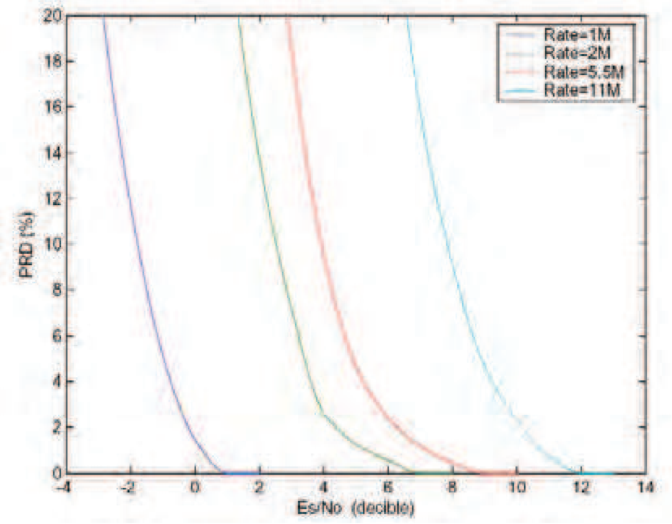


Fig. 6. PRD to Es/No using different WLAN transmission rate

3. **Simulation Scenario 3**

In this scenario, we study the trade-off between compression ratios (and/or quantization levels) and transmission rates in WLAN under different signal-to-noise ratios.

The more the compression ratio is (and/or the less the quantization levels are), the less the data size becomes. So the medical signal can be transmitted at a slower transmission rate with a higher compression error (and/or higher quantization error) and lower transmission error. There is an optimal point to minimize the overall error. Figure 7 shows the simulation results in different signal-to-noise ratios with a fixed quantization level (2^{16}). There is an optimized compression rate for a given signal-to-noise ratio with a fixed quantization level. For example, when E_s/N_o is 10db, the optimal compression ratio is about 40% with very small PRD. When E_s/N_o is 2db, the optimal compression ratio is about 10% with PRD around 16%. Optimizing medical data and wireless resources is important for an integrated medical information processing and

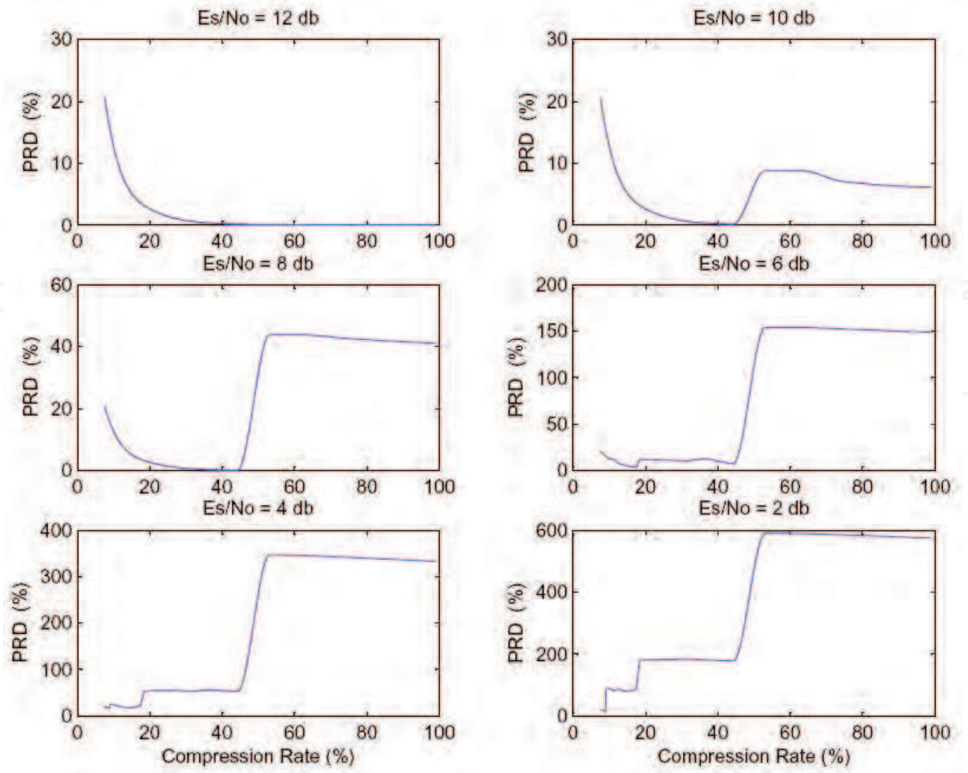


Fig. 7. PRD to compression ratio in different Es/No environment

communication system. From the figures, we notice that a small difference in compression ratio for a fix quantization level can result in a large difference in overall errors.

3.2 Medical pattern recognition and diagnosis reliability

3.2.1 Impact of information processing and transmission errors on lung sound diagnosis

Shown in the previous section, wireless transferred lung sound may be contaminated by data processing errors and/or transmission errors. If the overall errors are so severe as to alter the lung sound waveforms and patterns significantly, the lung sounds may no longer be suitable for diagnosis. Here we use an example of wheeze detection to illustrate the impact of overall errors on lung sound pattern recognition and diagnosis. Lung sounds were collected from a sophisticated human patient simulator under normal and wheeze conditions. Low, medium and high random noises were added to lung sounds to generate three sets of simulated overall errors. Several essential lung sound parameters were derived from lung sound data, such as FC_e (exhale peaking frequency), PS_e (exhale frequency bandwidth, i.e., exhale 90% frequency bandwidth that contains 90% of total power,), P_e (exhale total power), T_i (inhale length), S_i (inhale strength: RMS values), T_e (exhale length), S_e (exhale strength: RMS values), T (breath cycle length), etc., and diagnosis regions were designated from one or several parameters. Figure 8 illustrates the lung sound frequency domain parameter points (X-axle: exhale peaking frequency; Y-axle: exhale frequency bandwidth) under low, medium and high levels of overall error conditions respectively. Under the low error level, parameter points are clustered for both normal breath and wheeze, indicating a potential in achieving a high level of confidence in distinguishing wheeze from normal patterns. When the lung sound is corrupted by medium level errors, the parameter patterns are intervened, leading to a difficult pattern recognition problem. When errors are further increased to a high level,

the problem becomes even worse, and the parameter points of wheeze start to drift out of the wheeze region towards the normal region. This pattern shifting by noise artifacts significantly reduces diagnosis accuracy.
From the figure we can see that when lung sound is interfered by errors to some levels, the lung sound patterns have larger deviations and have a pattern shifting as well. Reduction of noise artifacts and signal processing errors is of essential relevance in medical diagnosis and highlights the issues of optimal utility of communication resources in medical diagnosis problems.

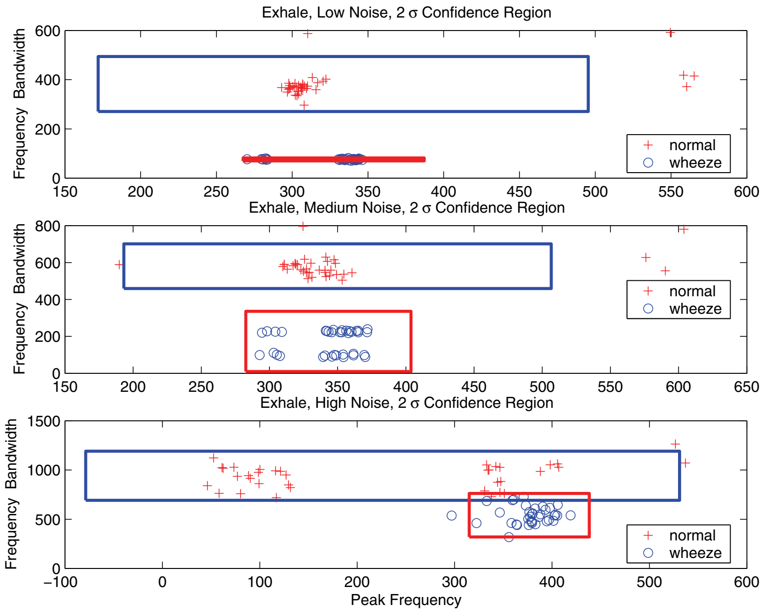
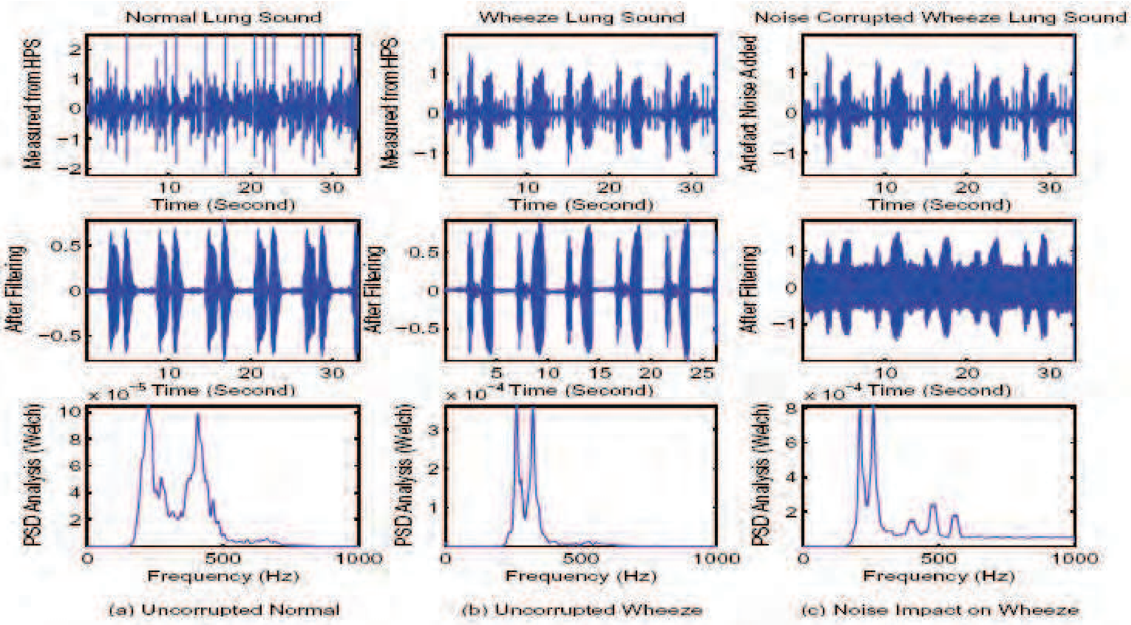


Fig. 8. Noise impact on normal lung sound and wheeze

3.2.2 Impact of noise on sound characteristics

To find the lung sound diagnosis pattern after passing the wireless telemedicine system we transmitted both normal and wheeze lung sound through the system. As we illustrated before noise will impact on lung sound patterns. Figure 9(a) shows a typical normal breathing sound and figure 9(b) shows an expirational wheeze (these are from the Human Patient Simulator, i.e. HPS, which was set as a 50 year old truck driver with normal condition and with wheeze disease respectively) (33–35). When collecting the data, we used a ventilation machine to control the breath and the environment noise was set as low as possible. The top figures are the raw data measured directly from the HPS. Since the existence of some low-frequency noise such as skin-scraping noises, chest movement noises, etc., the breathing patterns are not obvious. We used a high-pass filter to eliminate the noise under 200 Hz. After filtering, the difference between normal and wheeze lung sound can be clearly seen from their time domain waveforms. In the frequency domain analysis, the wheeze can be further characterized by a substantial narrowing of spectrum, shifting of center frequency (towards low pitch in this example), etc.. For this example, sounds are obviously very clean with minimum noise corruption. Lung Sound patterns are significantly altered when noise artifacts are present. Figure 9(c) shows the corrupted wheeze signal, both in its time-domain waveform and frequency-domain spectrum. It is clear that in a noisy environment, the characteristics of a wheeze are distorted to the point that it is no longer possible to recognize sound patterns.



(a) Uncorrupted Normal

(b) Uncorrupted Wheeze

(c) Noise Impact on Wheeze

Fig. 9. A normal sound, a wheeze, and noise impact on sound patterns

3.2.3 Lung sound diagnosis after passing the wireless telemedicine systems

We shall reduce the noise by adaptive noise cancelation (ANC) method, see (33–35) for the details of ANC method, and use frequency domain characteristics of exhale signal to show the pattern of lung sound signals. Previous section told us that there is an optimized compression ratio or quantization level (in bits) for a particular signal-to-noise ratio of communication channel. Here we select same simulation module in section 5, and to simplified the analysis we do not compress the signal. Simulation result shows the optimal quantization level is 2^8.

After we received the lung sound signal, we plotted the lung sound frequency domain parameter points in a x(peak frequency)-y(frequency bandwidth) plane. Figure 10 illustrates the lung sound diagnosis pattern. The top figure shows the points of original lung sound signal, the meddle figure show the points of lung sound signal passing the WLAN-based telemedicine system when the quantization level is 2^8 and the signal to noise ratio is 10dB, and bottom one shows points of received lung sound signal after ANC process. To make clear we drew a 2σ confidence region both for normal and wheeze lung sound extracted parameters. From the figures we can see that after signals are transmitted through the system, the wheeze pattern data points are no longer in the wheeze region due to the quantization errors and transmission errors, and they mix with normal region, which makes the diagnosis incorrect. Fortunately, after ANC process the wheeze pattern data points are separated from normal region again, which correct the diagnosis.

ANC method separates the wheeze pattern region from normal pattern region. And the bottom one of figure 10 shows that there is distance between the normal 2σ confidence region and the wheeze 2σ confidence region. This comes out a problem: is it possible to reduce original lung sound signal data further while still make correct diagnosis ? The answer is: Yes. Figure 11 shows the result. Here quantization level is not 2^8 but 2^4 (The length of original lung sound data becomes half), and the other parameters of the system are kept same. We can see from bottom one of figure 11 that after noise cancellation the wheeze pattern region can still be separate from normal pattern region, however the distance of the two lung sound pattern region becomes shorter. So we can transmit less lung sound data than optimal one

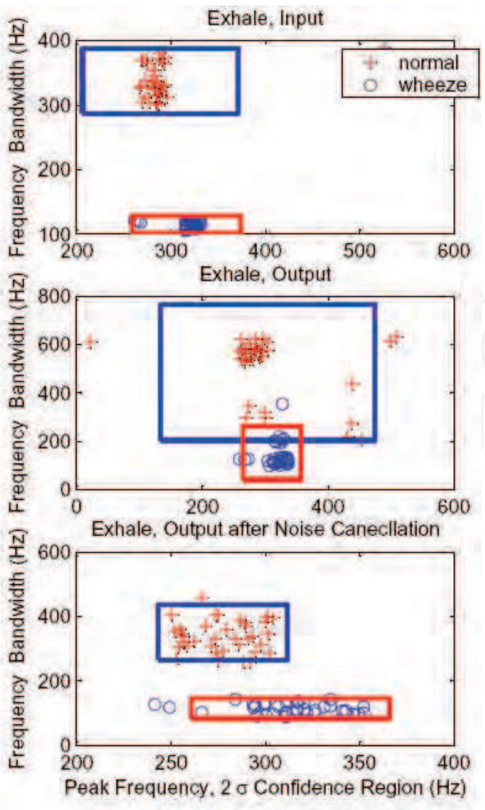


Fig. 10. Lung sound pattern when quantization level is 2^8

while can still distinguish wheeze lung sound to normal lung sound at receiver side, but the probability of error diagnosis will increase. There is a trade-off between them.

4. Security impacts of wireless channels

4.1 Weakness in wireless-based telemedicine systems

As wireless systems use an open medium, all the data transmitted or received over a wireless system like WLAN is susceptible to attacks from both passive eavesdropping and active interfering. There are several main common security threats in WLAN networks such as eavesdropping, deny of service, theft of service, etc. For example, an attacker can use some utilities like NetStumbler (47) to monitor all active access points in the area, and start Ethereal (48) to look for additional information. The attacker can then capture the packets with Airsnort (49), and crack the WEP key. With WEP key, an attacker can further sniff layer 3-7 packets. Portable medical equipment and sensors based on SCADA technology, increasingly utilize WiFi networks and thus are vulnerable to a combined wireless / SCADA attack. Such SCADA attacks would include Unauthorized Command Execution, SCADA Denial of Service, SCADA Man-in-the-Middle, Replay, and Malicious Service Commands. A focus on protection of the WiFi network is an essential step in reducing these vulnerabilities (14). As such security becomes one of the most pressing and challenging problems faced by WLAN networks (28). When a telemedicine system uses WLAN to transmit or receive medical signal, security becomes extremely important. Security features such as authentication and encryption are always considered, and the goal is to make WLAN traffic as secure as wired traffic (37).

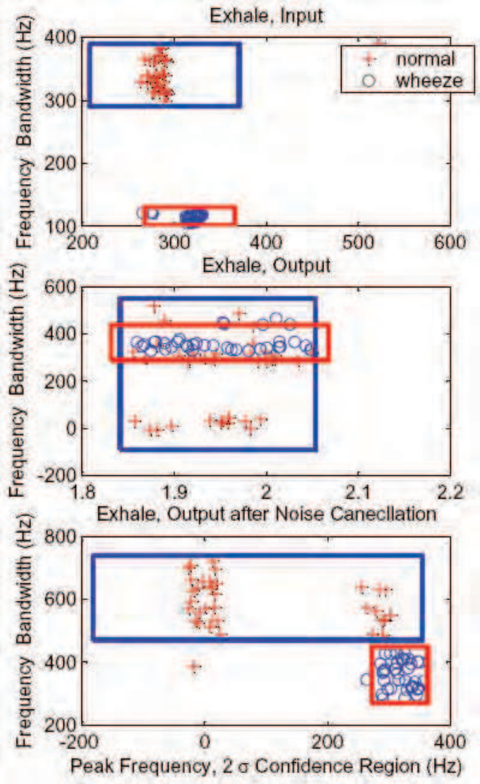


Fig. 11. Lung sound pattern when quantization level is 2^4

Bluetooth is another widely used wireless network standard. Though the security of Bluetooth is enhanced, malicious nodes can still use Denial of Service (DoS) attacks to prevent victims going through Bluetooth LAN access points.

4.2 Enhancement of WiFi security using 802.11i standard

WiFi alliance (52) defined two authentication standards i.e., WPA (Wi-Fi Protected Access) and WPA2. WPA was based on IEEE 802.11i standard (40), and used to replace WEP (Wired Equivalent Privacy). One major improvement in WPA is the TKIP (Temporal Key Integrity Protocol) which dynamically changes encryption keys when the WiFi is used. TKIP is combined with the much larger initialization vector to provide greatly improved protection from attacks against WEP. Moreover, WPA also provides MIC (Message Integrity Code) to greatly improve payload integrity. WPA2 is the advanced version of WPA which implemented the full mandatory parts of 802.11i. In addition to the TKIP and MIC, it also implements a new AES (Advanced Encryption Standard) based algorithm and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) to enhance the security.

There are two modes for both WPA and WPA2: enterprise and personal. Enterprise WPA and WPA2 use IEEE 802.1X protocol (41), which is based on EAP (Extensible Authentication Protocol), and distributes different keys to each user through RADIUS authentication server. Figure 12 shows the authentication procedures (50). When an 802.11 mobile node (supplicant) tries to connect to the WLAN network, the access point will sent out EAP-Request identity packet, and the mobile node will response with the EAP-response packet that will be forwarded to the RADIUS server. The authentication server then begins the authentication procedures including sending out challenge and verifying challenge response. If mobile node passes the authentication, RADIUS will accept the request, and allow normal traffic. Otherwise, RADIUS will reject the request and block all non-EAP traffic.

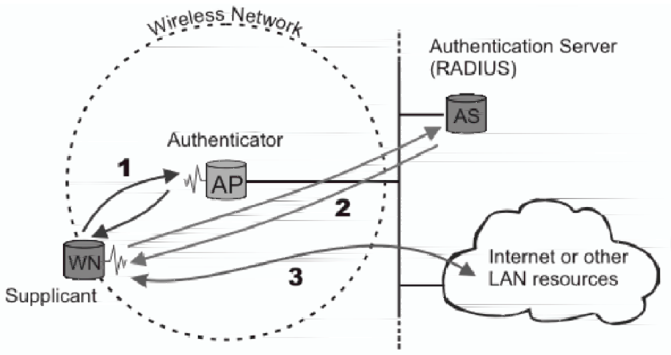


Fig. 12. EAP authentication

Personal WPA and WPA2 do not use RADIUS server to authenticate but utilize less scalable Pre-shared Key (PSK). In PSK mode, each mobile node is given the same passphrase.

4.3 Enhancement of security at home or residential areas

In most personal and residential areas where RADIUS is not available, the WLAN medical sensor nodes will use the PSK mode for both WPA and WPA2. Instead of using a complex and expensive authentication server, each user must enter a passphrase (up to 63 ASCII characters or 64 hexadecimal digits) to access the network. When using the ASCII characters, a hash function reduces it from 504 bits (63 characters × 8 bits/character) to 256 bits. For the PSK mode, the security level depends on the strength and secrecy of the passphrase, and is vulnerable to some attacks such as password cracking attacks, brute force attack, etc. Aircrack is one tool used to retrieve WPA and WPA2 PSK keys (44).
There are several ways to strengthen the PSK mode:

- Generate passphrases at their discretion, and pre-store on the medical sensor node to avoid re-entry;
- Employ a PBKDF2 (Password-Based Key Derivation Function) key derivation function;
- Bypass weak passphrase, and only allow passphrase using 40 characters or more.

Alternatively, mobile sensor nodes and access points can choose some privately defined security protocols to enhance the security level in residential areas. There are several such protocols, such as WAPI (WLAN Authentication and Privacy Infrastructure) (51). People may also implement high complexity authentication protocols based on their research and preference. However, as those methods are not standardized, people need to have the access to change the firmware of access points. Moreover, while private protocols are a good step, they do not ensure security. A prime example is the Lightweight Extensible Authentication Protocol (LEAP) developed by Cisco Systems which blocks all access until the client provides authentication credentials before a session key and access to the network is granted. ASLEAP is a tool to exploit LEAP. "Within months, some helpful person invested their time into generating a cracker tool. Publicizing the threat was a service to everyone, but I leave it as an exercise for readers to determine what satisfaction is obtained by the authors of tools that turn threat into reality and lay waste to millions of dollars of investments (45)."

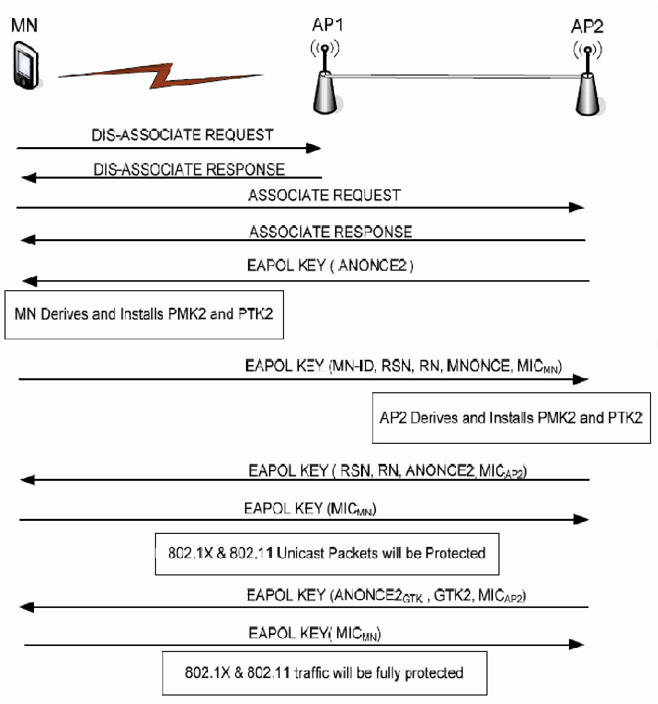

MN
AP1
AP2
DIS-ASSOCIATE REQUEST
DIS-ASSOCIATE RESPONSE
ASSOCIATE REQUEST
ASSOCIATE RESPONSE
EAPOL KEY (ANONCE2)
MN Derives and Installs PMK2 and PTK2
EAPOL KEY (MN-ID, RSN, RN, MNONCE, MIC_{MN})
AP2 Derives and Installs PMK2 and PTK2
EAPOL KEY (RSN, RN, ANONCE2, MIC_{AP2})
EAPOL KEY (MIC_{MN})
802.1X & 802.11 Unicast Packets will be Protected
EAPOL KEY ($ANONCE2_{GTK}$, GTK2, MIC_{AP2})
EAPOL KEY(MIC_{MN})
802.1X & 802.11 traffic will be fully protected

Fig. 13. Secure Fast Roaming Packet Streams

4.4 Secure session based fast roaming

WiFi-based telemedicine networks will normally comprise multiple access points in healthcare centers or at home to have full coverage. WiFi medical sensor nodes can roam freely between access points once they have been authenticated and associated to the telemedicine network, which means a sensor node can move in and out of coverage of different access points, and always associates with the strongest RF signal as it moves across the WiFi network. When a sensor node starts a roaming procedure, it will disassociate from the current access point and subsequently associate with the desired access point without losing connection and current communication session. And no new authentication is needed when a sensor node swap the access points. To do this, the WiFi sensor node will still keep catching neighbor access points' information from their beacon packets and/or probe response packets when it associates an access point. A roaming process will be triggered when one or more of following conditions meets (30):

1. RSSI (receive signal strength indication) from current access point is too low;
2. RSSI difference between neighbor access point and current access point is larger then threshold;
3. Excessive interface or noise for current access point;
4. Excessive retries when re-associates to access point;
5. Current access point has insufficient capacity;
6. Other transmission error exceed threshold; etc.

Medical sensor nodes must complete roaming and be able to pass data within 100-200 milliseconds when it decides to roam to a new access point (36). Figure 13 shows detailed roaming procedures when a WiFi mobile node moves from the coverage of one access point to another.

4.5 Problems with standard wireless security tactics

While it is essential to implement standard security methods, one needs to realize that individually each method is not enough. For example, disabling SSID broadcasting has no impact on network traffic. This is one layer of defense for a wireless network. A determined hacker tools like Kismet will probe wireless networks and by default the WAP responds with a message that contains its SSID. MAC filtering attempts to restrict access to known devices; but tools like Macshift (windows) and Macchanger (Linux) allow spoofing of MAC addresses to work around this defense.

Multiple layers of defense and complex defenses are the best methods of promoting security.

4.6 Wireless SCADA system concerns

In addition to the computers, laptops, and handheld devices, medical environments are increasingly integrating medical equipment and sensors into their wireless networks. Wireless smart beds automate patient charting, wireless robots bring pills to patients, wireless smart intravenous (I.V.) pumps deliver medication into patients (16), wireless heart monitoring tracks patients' heart health and adjusts medication accordingly (1), and various other wireless medical technologies are becoming common place (2; 8; 25; 39). Such medical equipment and sensors are supervisory control and data acquisition (SCADA) systems.

In July 2010, vulnerabilities of SCADA systems hit the mainstream news with the discovery of the Stuxnet trojan. The Stuxnet trojan attacked Siemens PLCs, using a default password hard-coded in the Siemens Simatric WinCC software to access the SCADA MS SQL database. Stuxnet readily infiltrated systems that were NOT directly connected to the internet. Even before Stuxnet the President's Critical Infrastructure Protection Board and the Department of Energy realized the serious nature of SCADA vulnerabilities and developed 21 steps to improve the security of SCADA systems (42). DoD initiated a series of SCADA Security Workshops, which include a plugfest for live vulnerability testing of SCADA systems (43). There have been a number of examples of "war driving" to attack SCADA systems. The Maroochy Shire Sewage Spill in 2000, where a disgruntled employee accessed wireless sewage pumping stations, released millions of liters of raw sewage into nearby rivers and parks. SCADA attacks can take the form of unauthorized command execution, SCADA denial of service, SCADA man-in-the-middle, replay attacks, and malicious service commands.

With these examples in mind, one can easily envision wireless attacks aimed at wireless medical equipment and sensors. Patient charting could be manipulated. Medication dosage could be changed. Medical "war driving" would be localized, but trojans aimed at specific wireless medical equipment could impact large numbers of patients across the nation or even across the globe. The idea of deploying these wireless tools is to reduce errors by enabling doctors and nurses to input critical data on the spot and offer immediate and "reliable" access to patient information and records. Yet pursuit of this worthy goal via wireless and SCADA technologies introduces new and frightening vulnerabilities. There are some basic steps that can be applied to wireless medical equipment and sensors:

- Identify all wireless connections.
- Perform risk assessments and audits.
- Establish red teams.
- Limit access by MAC address.
- Disable SSID broadcasting.

- Lock down backdoors and change default passwords
- Disconnect unnecessary wireless connections
- Appropriately configure firewall
- Implement manufactures security features.

Some more in-depth security tactics would be:

- Install a wireless IDS (46)
- Encrypt bluetooth channels (a method which could be revised for any WiFi traffic)
- Utilize anomaly-based behavior analysis of wireless network traffic (4)

4.7 Advanced wireless security protection methods

This section will discuss a scheme to successfully trace attacking paths from malicious nodes as well as segregate and protect systems from these malicious nodes (3). It can be implemented in both WLAN (WiFi) and WPAN (Bluetooth, Zigbee). Another method mentioned in this section are Wireless Self Protection Systems. In combination with standard security methods, these methods build a multilayer defense for wireless security.

4.7.1 Wireless covert channel signaling

Denial of service (DoS) attacks is one of active interfering attacks using which an attacker can cause congestion in WLAN or WPAN network either by generating an excessive amount of traffic itself, or by making other nodes generate excessive amounts of traffic. Besides common DoS attacks incurred in wired networks which transmit falsified route updates or reduces the TTL (time-to-live) field in the IP header, etc., WLAN or WPAN networks have their own unique DoS attacks. For example, an attacker can cause a particular node to continuously relay dump data to use up the battery of that node. DoS attack is a serious problem for WLAN or WPAN networks for medical applications, especially when the they networks are connected to a scatternet or a local area network. In this case, because malicious nodes from anywhere in the scatternet or anywhere in the LAN can launch the DoS attacks, they can block time-essential or even life-threatening information from being sent through the networks or disable the WLAN or WPAN networks. Covert channel signalling can be used to trace DoS attack paths back to the malicious nodes:

Establish Cover Channels

An end-to-end authentication may prevent DoS attacks from being launched, however if two nodes collude, DoS attacks are still quite feasible (10). To detect malicious nodes in a WLAN or WPAN network, schemes of covert channels have been designed (3; 21), which are implemented in baseband layer, logical link control layer, and service discovery layer. Those covert channels may inject probabilistically device information through the access points, and based on the injected information the DoS victims may reconstruct the complete path from the packets.

Trace Back with Covert Channels

When tracking back function is enabled, the WLAN or WPAN access points write their MAC addresses (each has 48 bits) or IP addresses (each has 32 bits for IPv4 or 48 bits for IPv6) into the designed covert channel of packet headers probabilistically (3; 20). When the victim receives the packets, necessary information can be extracted from the covert channels of those packets. To make the tracing back more accurate and robust, access points need to insert the checksum into the packets header fragments. Checksum function should be random and unpredictable to the attacker. A random hash function, for example, can be used (9).

Reconstruct Attack Paths
When the victim node receives a set of packets which were marked by access points with a certain probability, it extracts the embedded bits from the covert channel. After removes the duplicates, it then sorts the blocks that have the same checksum. By combining all the fragments, the victim will recover the original address chain information (3; 9). The attacking path from the malicious node to the victim is reconstructed.

4.7.2 Wireless self protection systems

Wireless Self Protection Systems (WSPS) are an advance security method capable of detecting complex attacks and responding to these attacks. WSPS uses abnormality metrics collected from multi-channel packet monitors and signal analyzers. These metrics form a foundation to recognize potential attacks, which allows appropriate responses. The collected signal, channel and frame metric attributes are unique for each wireless network device (5). Figure 14 shows the flowchart of WSPS.

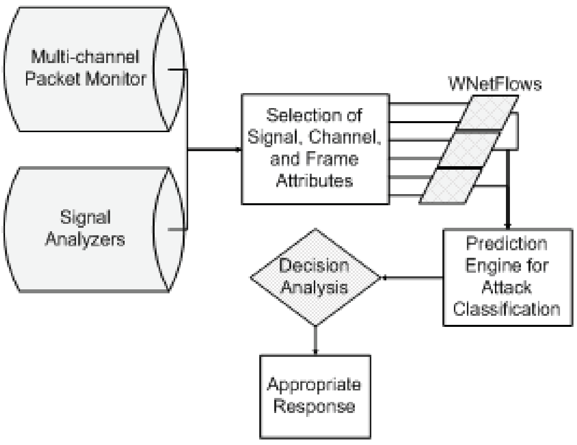

Multi-channel Packet Monitor
Signal Analyzers
Selection of Signal, Channel, and Frame Attributes
WNetFlows
Prediction Engine for Attack Classification
Decision Analysis
Appropriate Response

Fig. 14. WSPS Flowchart

Signal attributes can include device name, encryption type, signal strength, and source type (client station, WAP, etc.). These are good for detecting man-in-the-middle attacks and MAC attacks. Channel attributes can include channel number, frequency used, IEEE standard used, AP and master device names, and channel reuse. Frame attributes can include sequence ID, date and time, source and destination (MAC and IP), packet size, frame type, application name, source rate, and frame sequence number. Good for detecting replay and address spoofing (12).
Wireless network flows (WNetFlows) are developed and explored by anomaly based behavior analysis to identify relevant attributes of normal traffic (6). Metric attributes combine to form a WNetFlow-key for each WNetFlow. Common attributes of the WNetFlow keys are utilized to determine specific traffic types. Based on the WNetFlows, a prediction engine classifies the attack. When an attack is identified, then a decision analysis function dynamically determines an appropriate response in order to minimize vulnerabilities from that attack. Some actions that can be taken include deauthentication of the attacker, utilizing the attack signal power to identify the attacker location and physically stopping the attack, and shutting down WAPs in

order to stop the attacker (5). Experimental results show that the WSPS approach can protect from wireless network attacks with an average detection rate of 99.13% for experimented attacks (4).

5. Conclusions

In this chapter, medical signal accuracy in a WLAN-based telemedicine system was studied. Relationships of medical information processing and wireless communication channels were discussed in an integrated medical information system containing the key function blocks: DCT transform, data compression, quantization, wireless channels, and IDCT transform. Explicit interactions between complexity and errors of each block were derived. Transmission errors are directly proportional to transmission rates and channel noise level, while data compression and quantization errors are inversely proportional to their respective compression ratios and quantization levels. There is a fundamental trade-off between overall information errors in these blocks. For example, the less the compression ratio is, the less the data size becomes. Consequently, the data can be transmitted at a slower transmission speed. For a given resource such as bandwidth and signal-to-noise ratio, there exists an optimal allocation that maximizes overall information accuracy after passing information processing and communication channels. Relationships between information resource allocation and medical lung sound diagnosis pattern were examined in detail. When applied to medical information processing, it becomes clear that in an integrated medical information processing and wireless communication system, a small deviation from the optimization point of resource allocation can result in a significant change in overall errors, leading to less accurate and unreliable diagnosis. Lung sound signals were used to show the trade-off between signal pattern accuracy and resource allocation. Lung sound pattern was correctly recognized after proper resource optimization and noise cancelation.

Security challenges and methods were also examined in a wireless-based telemedicine system. Enhanced security technologies both in enterprise areas and personal areas were reviewed. Secure fast roaming and wireless SCADA systems were introduced. Finally, two advance security methods for wireless telemedicine systems, i.e., wireless covert channel signalling and wireless self protection systems were discussed.

6. References

[1] W. T Abraham, et al., Wireless pulmonary artery haemodynamic monitoring in chronic heart failure: a randomised controlled trial, *The Lancet, Vol. 377, Iss. 9766, Pgs. 658 - 666*, 19 Feb., 2011.

[2] L. Burnes Bolton, DrPH, RN, FAAN, et al., Smart Technology, Enduring Solutions: Technology Solutions Can Make Nursing Care Safer and More Efficient, *JHIM, FALL 2008, vol. 22 / No. 4*

[3] Q. Cheng, H. Qu, Enhancing Bluetooth Security with Covert Channel Signaling, *IEEE and IFIP Int. Conf. on Wireless Communications Networks*, June 2004.

[4] S. Fayssal, S. Y. Al-Nashif, Anomaly-Based Behavior Analysis of Wireless Network Security, *Fourth Annual International Conference on In Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007. pp. 1-8.* doi:10.1109/MOBIQ.2007.4451054

[5] S. Fayssal, Y. Al-Nashif, B. uk Kim, S. Hariri A Proactive Wireless Self-Protection System, *ACM International Conference on Pervasive Services (ACM ICPS 2008)*.

[6] S. Fayssal, Wireless self-protection system, *Dissertation for The University of Arizona*, 2008, 155 pages.

[7] B. Firoozbakhsh, N. Jayant, S. Park, and S. Jayaraman, Wireless communication of vital signs using the Georgia Tech Wearable Motherboard, *2000 IEEE International Conference on Multimedia and Expo, ICME, Volume 3, 2000 Page(s):1253 - 1256 vol.3*, 30 July-2 Aug.

[8] T. Gao, et al., Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results, Technologies for Homeland Security, *2008 IEEE Conference on In Technologies for Homeland Security, 2008 IEEE Conference on (2008)*, pp. 187-192. doi:10.1109/THS.2008.4534447 Key: citeulike:4460555

[9] M. T. Goodrich, Efficient Parket Marking for Large-Scale IP Trace back. *CCS'02, November 18-22, 2002, Washington, DC, USA*

[10] V. Gupta, S. Krishnamurthy, and M. Faloutsos, Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, *Report, Dept of EECS, UC Riverside*.

[11] S. Haykin, *Communication systems*, ISBN 0471178691, New York: Wiley, c2001.

[12] K. Hulin, C. Locke, P. Mealey, and A., Analysis of Wireless Security Vulnerabilities, Attacks, and Methods of Protection, *Information Security Semester Project*, Fall 2010

[13] T. B. Johnson, Thermal Agitation of Electricity in conductors, *Phys. Rev., Vol. 32*, July 1928.

[14] D. Kelley, Why SCADA Security Matters–And What You Should Know About It. /emph http://www.esecurityplanet.com/views/article.php/3901856/Why-SCADA-Security -Matters–And-What-You-Should-Know-About-It.htm

[15] I. Korn, *Digital Communications*, Van Nostrand Reinhold Company Inc., New York, 1985.

[16] L. Siv-Lee, L. Morgan, Implementation of Wireless Intelligent Pump IV Infusion Technology in a Not-for-Profit Academic Hospital Setting, *Hospital Pharmacy, Thomas Land Publishers Inc., Vol. 42, No. 9, Sept. 2007. http://thomasland.metapress.com/content/x280t2318u35l716/*

[17] S. Lehrer (2002). *Understanding Lung Sounds*, 3rd ed., W.B. Sounders, 2002.

[18] S. McGarrity, 802.11b PHY Simulink Model, *802.11b baseband physical layer, wireless communication*, Aug, 26th, 2002.

[19] H. Pasterkamp, S. Kraman and G. Wodicka, Respiratory sounds, *Am. J. Respir Crit Care Med. Vol. 156, pp.974-987*, 1997.

[20] T. Peng, C. Leckie, R. Kotagiri, Adjusted Probabilistic Packet Marking for IP Traceback, Department of Electrical and Electronic Engineering, The University of Melbourne, Victoria 3010, Australia, 2001

[21] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Practical Network Support for IP Traceback. *In Proceedings of the 2000 Acm Sigcomm Conference*, August 2000.

[22] A. M. Sayeed, A signal modeling framework for integrated design of sensor networks, *IEEE Workshop Statistical Signal Processing*, 28 Sept.-1 Oct. 2003 Page(s):7.

[23] B. Sklar, Digital Communications: Fundamntal and Applications. *ISBN 0-13-084788-7, Prentice Hall PTR Publishers, second edition*, 2001.

[24] A. Sovijarvi, P. Helisto et al., A new versatile PC-based lung sound analyzer with automatic crackle analysis (HeLSA); *repeatability of spectral parameters and sound amplitude in healthy subjects, Technology & Health Care*. 6(1), 1998 Jun, pp. 11-22.

[25] R. S. Tolentino, S. Park, Hospital RFID-Based Patient u-Healthcare Design over Wireless Medical Sensor Network, *Database Theory and Application, Bio-Science and Bio-Technology*

Communications in Computer and Information Science, 2010, Vol. 118, 299-308, DOI: 10.1007/978-3-642-17622-7_31

[26] H. Qu, L. Y. Wang, Y. Zhao, Integrated Information Processing and Wireless Communication: Complexity Analysis, *The International Conference on Communication Systems and Applications (CSA'06)*, July 3-5, 2006, Alberta, Canada.

[27] H. Qu, L. Y. Wang, Q. Cheng, E. Yaprak, H. Zheng, Wireless-Based Medical Information Processing: Integrated System Analysis and Simulation, *Proceedings of the International Conference on Telehealth (Telehealth'06)*, July 3-5, 2006, Alberta, Canada.

[28] H. Qu, Q. Cheng, E. Yaprak, Using Covert Channel to Resist DoS attacks in WLAN, *Proceedings of the International Conference on Wireless Networks (ICWN'05)*, Page.38-44, June 27-30, 2005, Las Vegas, USA..

[29] H. Qu, Q. Cheng, and E. Yaprak, Unconfined E-health care system using UMTS-WLAN, *International Journal of Modelling and Simulation, Issue 4*, 2006, ACTA Press.

[30] H. Qu, J. Cheng, Q. Cheng, L. Y. Wang, WiFi-Based Telemedicine System: Signal Accuracy and Security, *2009 International Conference on Computational Science and Engineering*, Vancouver, Canada August 29-August 31.

[31] H. Wang, L. Y. Wang, and H. Qu, Wireless-Based Identification of Patient Dynamics: Analysis and Quantization Design, *Volume 2 of the proceddings of the 11th WSEAS International Conferences on SYSTEMS*, Agios Nikolaos, Crete Island, Greece, July, 2007.

[32] L. Xiao, M. Johansson, H. Hindi, S. Boyd and A. Goldsmith, Joint optimization of communication rates and linear systems, *IEEE trans. on automatic control, vol. 48, no. 1*, Jan. 2003.

[33] H. Zheng, H. Wang, L. Y. Wang, and G. Yin, Time-Shared Channel Identification for Adaptive Noise Cancellation in Breath Sound Extraction, *Journal of Control Theory and Applications, Number 3, Volume 2*, August 2004, ISSN: 1672-6340, pages 209-221.

[34] H. Zheng, H. Wang, L.Y. Wang, and G. Yin, Lung Sound Pattern Analysis for Anesthesia Monitoring, *Proceedings of 24th American Control Conference*, June 8-10, 2005.

[35] H. Zheng, H. Wang, L.Y. Wang, G. Yin, Cyclic System Reconfiguration and Time-Split Signal Separation with Applications to Lung Sound Pattern Analysis, *IEEE Transactions on Signal Processing*, Vol. 55 Issue 6 Part 2, pp. 2897-2913, June 2007

[36] Cisco Compatible Extensions for WLAN Devices (CCXv1-v4).

[37] S. Weatherspoon, Overview of IEEE 802.11b security, *Network Communications Group, Intel Corporation. Intel Technology Journal*, 2000.

[38] LAN MAN Standards Committee of the IEEE Computer Society, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications ANSI/IEEE Std 802.11b, 2000.

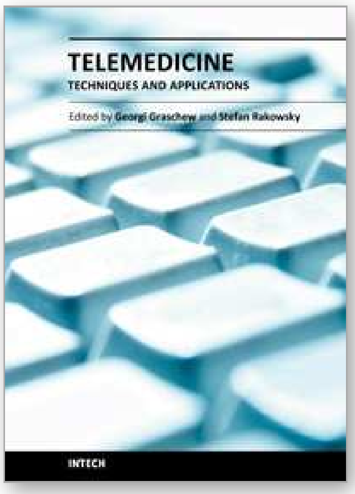
[39] Shoreline Research, Wireless Solutions in Healthcare: Expanding Point of Care Practices and Services in Hospitals, *A Bluesocket BluePaper*.

[40] IEEE Standard for Information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[41] IEEE standard for local and metropolitan area networks Port-based network access control, 2001.

[42] U.S. Department of Energy: 21 Steps to Improve Cyber Security of SCADA Networks. *http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf*

[43] SCADA Security Workshop, *http://www.drighten.com/Events/index.html*
[44] *http//www.aircrack-ng.org*
[45] William Arbaugh and Jon Edney at Real 802.11 Security.
[46] http://www.ijcaonline.org/archives/volume5/number8/934-1312
[47] http://www.netstumbler.com/
[48] http://www.ethereal.com/
[49] http://en.wikipedia.org/wiki/AirSnort
[50] http://en.wikipedia.org/wiki/802.1x
[51] http://www.suntzureport.com/wapi/wapi.pdf
[52] http://www.wi-fi.org/


TELEMEDICINE
TECHNIQUES AND APPLICATIONS
Edited by Georgi Graschew and Stefan Rakowsky
INTECH

Telemedicine Techniques and Applications
Edited by Prof. Georgi Graschew

ISBN 978-953-307-354-5
Hard cover, 514 pages
Publisher InTech
Published online 20, June, 2011
Published in print edition June, 2011

Telemedicine is a rapidly evolving field as new technologies are implemented for example for the development of wireless sensors, quality data transmission. Using the Internet applications such as counseling, clinical consultation support and home care monitoring and management are more and more realized, which improves access to high level medical care in underserved areas. The 23 chapters of this book present manifold examples of telemedicine treating both theoretical and practical foundations and application scenarios.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821