Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 641867, 14 pages
doi:10.1155/2011/641867

Research Article

Quality of Service Regulation in Secure Body Area Networks: System Modeling and Adaptation Methods

Francis Minhthang Bui and Dimitrios Hatzinakos

The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, 10 King's College Road, Toronto, ON, Canada M5S 3G4

Correspondence should be addressed to Francis Minhthang Bui, bui@comm.utoronto.ca

Received 3 November 2010; Accepted 2 January 2011

Academic Editor: Arie Reichman

Body area network (BAN) has recently emerged as a promising platform for future research and development. The applications are myriad and encompass a wide range of scenarios, including those in not only medicine but also in everyday activities. However, while the applicability and necessity of BAN have been firmly assured, the underlying technological platforms to practically realize these networks are still in the developmental stages, with many outstanding key problems to be addressed. Due to their envisioned domains of applicability, an important problem in BANs is security and user privacy. Providing security in a practical BAN configuration is challenging due to various conflicting resource constraints. In this paper, the focus is to study signal processing methods for delivering secure communications in BANs, particularly when using biometrics. An optimization framework is presented to aggregate various methods, enabling overall quality of service (QoS) regulation in an integrated and flexible manner. In particular, this resource allocation approach is shown to be effective in managing security solutions for BANs.

1. Introduction

Although originally conceived as a subclass of the *ad hoc* network family, body area network (BAN) systems have grown and developed as a noteworthy and distinctive class of their own [1–5]. This fact is acknowledged by the establishment of the working standard IEEE 802.15.6 [6], which aims to cover the communication aspects of low-power devices to be used on, in, or around the body. As stated in the standard, the applications will span from medical to consumer electronics, with vast technological and social implications. In essence, BAN systems represent the convergence of many existing communication devices and algorithms, in attempting to deliver constant and ubiquitous communications with a highly customized mode of operation. Indeed, one of the key aspects separating BANs apart from other networks is the degree of personalization involved. An approximate categorization based on the operating proximity can be made: a local area network (LAN) is intended to operate within a 100 m radius, a personal area network (PAN) within 10 m, and a BAN within 2–5 m [3]. Moreover, the communications are mostly centered around devices on a single body. As such, each BAN will be linked to an individual with unique requirements, habits, and operating preferences. Evidently, to be effective, the BAN architecture will need to be flexible enough to adapt to all of these scenarios. On the other hand, there is a contradictory requirement: BANs are intended to be low-power and light-weight devices for portability and user convenience. These characteristics imply that the power and bandwidth consumptions in BANs need to be severely limited.

In addition, due to personal nature of BANs, security and privacy become a major issue. For instance, in a consumer electronic scenario, the user may not wish for others to eavesdrop on his or her phone conversation or to profile the music listening habit. Similarly, in a medical setting, the release of personal medical information, whether inadvertent or not, is a serious intrusion into a person's privacy. One possible solution is to utilize conventional cryptographic methods, for example, AES, with the public-key algorithm RSA and X.509 digital certificate for performing key exchanges [7–9], as suggested in the emerging communication standards 802.16 and 802.20 [10]. However, due to the constraints in BANs, it is often an untenable challenge to directly apply

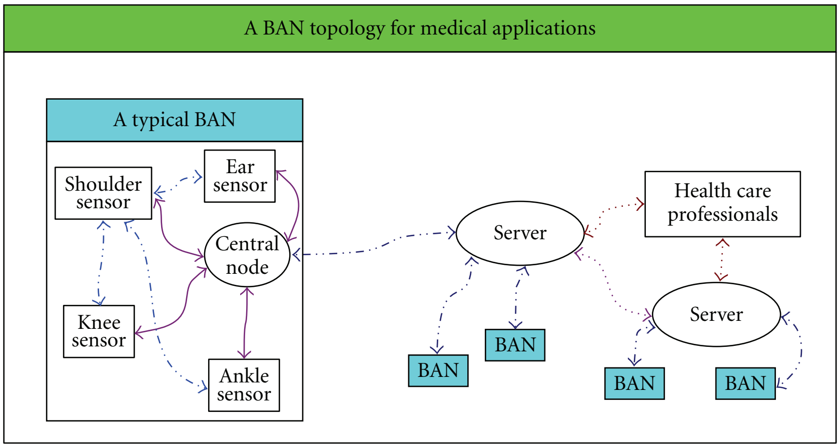

Figure 1: Model of a mobile health topology, consisting of various body area networks.

traditional methods to guarantee security. Instead, methods based on the ECG biometric have been demonstrated to deliver promising results with respect to security and privacy [1, 2, 11].

On the other hand, since biometric signal processing techniques operate mainly at the physical layer, the biometric-based secure BANs are affected directly by issues such as channel variations and signal modulation. As such, in regulating the quality of service (QoS) of the overall system, methods for addressing these issues need to be examined. To this end, the goal of this paper involves studying adaptation strategies for suppressing signal variations due to operating environment changes. In particular, channel tracking, processing block-size adaptation, and adaptive modulation are illustrated as example candidates, depending on the application scenario. Moreover, in order to synergistically combine the benefits of each strategy, an optimization framework is utilized.

The remainder of the paper is organized as follows. In Section 2, a high-level overview of BANs, particularly in relation to biometric security, is presented. Then, the system model to be used is described in Section 3, followed by the optimization framework for integrating various QoS criteria in Section 4. To support this framework, adaptation methods for enhancing QoS from various perspectives are explored in Section 5. Subsequently, the performance of the proposed methods is assessed in Section 6, which is followed by the conclusion in Section 7.

2. Overview of Secure BANs

While most of the original BAN research has focused mainly on medical settings, a wide range of other applications in military and multimedia domains can also be found [1, 2]. An example mobile health topology, consisting of individual BANs organized under several servers, is shown in Figure 1. Since a BAN is essentially a derivative of a sensor network, or more generally of an *ad hoc* network [3], it also suffers from the same nondefinitive system problem: the specific requirements in terms of system resources are typically not defined, until the particular *ad hoc* applications are known. Depending on the envisioned applications, the number of servers, sensors, and associated resources may vary significantly [4, 5].

In order to enable potentially demanding signal processing tasks, each BAN in Figure 1 has a central node, equipped with more advanced computational capabilities. Only the central node is destined to communicate directly with external devices. The remaining peripheral nodes may or may not communicate with one another. However, they all communicate with the central node. The peripheral nodes, which are usually limited in computational resources, convey the sensing data from different parts of the body, whereas the central node collects and organizes the data for further transmission. This hierarchical arrangement allows for an optimization framework to be subsequently implemented.

As mentioned in Section 1, biometrics based on the cardiovascular features, such as electrocardiogram (ECG), phonocardiogram (PCG), and photoplethysmogram (PPG), have been shown to be an attractive solution for secure key distribution in BAN. Indeed, the relevant biometric feature is the so-called interpulse interval (IPI) sequence, which is a sequence of time durations between R-R peaks [1, 2]. Then, by incorporating the body itself and the various physiological signal pathways as secure channels, a key distribution scheme based on fuzzy commitment is appropriate [12, 13]. A biometric signal is utilized for committing, or securely binding, a cryptographic key for secure transmission over an insecure channel.

Essentially, for this construction, the biometric merely serves as a witness. The actual cryptographic key, for symmetric encryption [7], is externally generated, (i.e., independent from the physiological signals). This strategy for key binding, known as biometric encryption, can also be achieved using other techniques such as quantization index modulation [14, 15]. The common property of these biometric schemes is the fact that many required operations are performed in the physical layer of the communication network. As such, in the context of secure biometric-based BAN, the physical layer issues are of direct relevance.

3. System Modeling

The research literature related to secure BAN applications has often refrained from directly including channel propagation effects, or utilized only simple models such as AWGN, in the system analysis. However, there are also existing works that, although agnostic of the security question in BAN, have otherwise addressed the antenna design and propagation issues for the BAN framework in a more comprehensive manner [16, 17]. Essentially, the main conclusion from this perspective is that no single-channel model can describe all the paths in a BAN. Instead, the types of channels applicable depend on the device types and the locations of device placement on the body.

3.1. Channel Models for BANs. A key determining factor is whether the signals will travel within the body (implanted devices, or inherent physiological pathways, e.g., cardiovascular signals from the heart to a measuring site), or outside the body (between wearable sensors).

3.1.1. BAN Device Types and Channel Effects. In this categorization, the devices are classified as either implanted or nonimplanted (wearable). Devices that are implanted are significantly affected by the various material composition and structure of the human body, which have the tendency to absorb and attenuate signal propagations. The overall effects create a channel propagation path that is best characterized by path loss models [16, 18, 19]. There also appear to be significant variations depending on how deeply, and at what organs, the devices are implanted within the body.

On the other hand, for devices that are not implanted, but worn externally, the applicable channels are described by multipath fading models, with the average number of significant multipath components ranging from 1.8 to 3.0 [16, 17, 20]. However, the exact nature of these channels depends on the relative location and geometry of placement on the body, as discussed in the next section.

3.1.2. BAN Device Locations and Channel Effects. It should be noted that the emphasis of this paper will be on nonimplanted devices, that is, which are worn externally on the body to perform various communication tasks. Therefore, while implanted devices are certainly affected by the location of implantation [16], such characteristics will not be considered here.

Wearable devices, being essentially specialized wireless sensor devices, inherit many characteristics from this device class. In the BAN context, the following criteria have been noted to affect the channel variations [19]: local scattering, changes in the geometry of the body, standing or sitting, and other physical activities. For example, more vigorous activities, such as sports, often result in rapid and sudden channel changes. This is equivalent to a short coherence time.

Furthermore, the body can be geometrically partitioned into several angular zones or regions, around the torso, with common general characteristics: front (0° to 60°, left and right), side (60° to 160°, left and right), and back (160° to 180°, left and right) regions. For instance, devices on the far side of the body tend to be affected by deep nulls caused by the absorption of power by the body, which make reliable communications in BANs problematic [19–21].

Table 1: Position-dependent power delay profiles for BAN channels [20].

Position	Average decay rate (dB/ns)	Bin 1 & 2 power ratio (dB)
Front	−12.4	7.4
Side	−10.4	7.3
Back	−10.6	1.5

Similarly, the relative placements of the transmitting and receiving devices are also significant. For example, the trunk-to-limb path is characterized by extreme variations due to movement of the limb. In particular, devices placed on the hand or wrist are notorious for having rapid changes, with short associated coherence times. By contrast the trunk-to-trunk link is more stable, with longer coherence times [16, 17, 19].

Various power delay profiles related to BAN devices have also been experimentally recorded. Table 1 summarizes the three profiles based on the body zones [16, 20]. The authors in [20] select a bin width of 0.5 ns for these measurements. According to these authors, there is generally a longer impulse response on the back and sides of the body compared with the front of the body, which is likely due to echoes off of the body itself, and because there are more signal paths when devices are placed on opposite sides of the torso. As such, the channel model used for analysis and simulation need to be selected according to these various geometric criteria. Additional experimental measurements and parameters for other device configurations can be found in [16] and the references therein.

3.2. Wearable Devices and Multistate Characterization. As discussed in Section 3.1, the focus of this paper will be on wearable devices. In addition, for these devices, the relevant model is a multipath fading channel, which has parameters determined by the device location. Then, such a channel can be viewed as an equivalent time-varying FIR filter, with impulse response

$$h(t,\tau) = \sum_{p=0}^{P-1} \alpha_p(t)\delta\left(\tau - \tau_p\right), \tag{1}$$

where P is the number of observable paths and τ_p and $\alpha_p(t)$, respectively, and the delay and gain of the pth path. The time variations, due to the Doppler effect, are described for each of the P paths by the Jakes power spectral density

$$S_p(f) = \begin{cases} \dfrac{\sigma_p^2}{\pi f_m \sqrt{\left(1 - (f/f_m)^2\right)}}, & |f| < f_m, \\ 0, & |f| > f_m, \end{cases} \tag{2}$$

where σ_p^2 is the average power of the pth path and f_m is the maximum Doppler shift. Moreover, the frequency selectivity is described by the power delay profile [22].

Corresponding to the above impulse response, the following discrete-time baseband equivalent received signal can be obtained

$$y(n) = \sum_{l=0}^{L} h(n;l)x(n-l) + v(n), \tag{3}$$

where n is the discrete time index, $x(n)$ the transmitted symbol, $y(n)$ the received symbol, $h(n;l)$ the channel impulse response, L the channel length, and $v(n)$ the additive white Gaussian noise (AWGN).

Suppose that blocks of N data symbols, with symbol duration T_S, are to be transmitted. The channel impulse response can also be expressed using the following basis-expansion model (BEM) representation, [23, 24]:

$$h(n;l) = \sum_{q=0}^{Q} h_{q,l}(n)e^{jw_q n}, \tag{4}$$

where Q indicates the number of basis functions $e^{jw_q n}$, $w_q = 2\pi(q - Q/2)/K$, $h_{q,l}(n)$ the slowly varying basis coefficients, provided that: $LT_S \geq \tau_{\max}$, the delay spread and $Q/(KT_S) \geq 2f_{\max}$, the Doppler spread. Hence for bounded $\tau_{\max}$ and $f_{\max}$, the parameters Q, K, L are finite. Furthermore, it is assumed that $2f_{\max}\tau_{\max} < 1$, that is, the channel is underspread.

The motivation for the above BEM representation is that, for a Jakes spectrum (such as for a multipath channel), the basis coefficients are slowly time-varying [23–25], a property which tremendously facilitates channel estimation for rapidly varying environments.

Due to movements of the sensors attached to the human body, it is evident that the rate of variations of the channel coefficients will not be constant. Specifically, since the Doppler shift f_m is affected by relative speed, variations in the user's activities imply that a single Jakes spectrum is inadequate to characterize the channel dynamics. In other words, while the above model is both time and frequency selective, it essentially describes one single-channel *state* or environment, where a state is characterized by a particular f_m. Therefore, to characterize the effects of user's activities on the BAN, a multistate characterization is useful. In fact, the multistate extension model from [22] can be adopted for this goal. For instance, a slow state is associated with idle durations, whereas a fast state is due to vigorous sport activities. Then, the probabilities of various associated states account for the user's dynamics as follows. Suppose the user's mobile activities are such that there are κ distinguishable states: $\{k_1, k_2, \ldots, k_\kappa\}$. Denote the probability of the user being in the k_i state as $p(k_i)$, then $\sum_{i=1}^{\kappa} p(k_i) = 1$. Moreover, it should be noted that the BEM formulation is particularly appropriate for tackling fast states, associated with a short channel coherence time, that is, high f_m.

3.3. Channel Equalization. It should be noted that in most current BAN implementations, the system parameters are selected such that only simple processing algorithms in the transceivers are needed. In particular, by selecting the symbol duration to be sufficiently long relative to the delay spread of the multipath channel, intersymbol interference (ISI) is minimal, and no equalization should be required for adequate performance [22]. This makes it possible to utilize low-power devices with reduced computational complexity. However, in this paper, we will consider scenarios where explicit equalization may be needed. The rationale is twofold. First, with the possibilities of the BAN framework being employed for multimedia and gaming applications, the required data rates may potentially exceed the threshold for equalization necessity; therefore, explicit consideration of equalization enables the proposed framework to be ready for various applications. Second, the case without equalization can be simply considered a special case in this framework, that is, either ignored altogether, or only simplified equalization is needed, since matrix computations typically reduce to scalar operations. Of course, for high data-rate applications, the implication is that microcontrollers with sufficient computational resources may be needed.

To evaluate the baseline performance behavior, conventional methods for channel equalization are used, namely minimum mean-squared error (MMSE) equalization. Essentially, two versions are formulated, depending on whether or not a BEM representation is in effect [22, 23].

For the case without BEM, a quasistatic approximation is made, in which the channel coefficients are assumed to be constant over some block duration, which is much less than the coherence time [22]. This means that the dependence of $h[n;l]$ on n is suppressed. Then, collecting N consecutive received symbols in a block, the following matrix formulation can be obtained

$$\mathbf{y}(n) = \mathbf{H}\mathbf{x}(n) + \mathbf{v}(n), \tag{5}$$

with $\mathbf{y}[n] = [y[n], \ldots, y[n-N+1]]^T$, $\mathbf{v}[n] = [v[n], \ldots, v[n-N+1]]^T$, $\mathbf{x}[n] = [x[n], \ldots, x[n-N-L+2]]^T$, and $\mathbf{H}$ is an appropriately defined convolution matrix [22]. With the MMSE criterion, the linear equalizer $\mathbf{f}$ is found by minimizing the cost function [26]

$$J_{\mathrm{MSE}}(\mathbf{f}) = E\left(\left|\mathbf{f}^H\, \mathbf{y}(n) - x[n-\delta]\right|^2\right), \tag{6}$$

where $E(\cdot)$ denotes the expectation operator, $(\cdot)^H$ the Hermitian transpose, δ is a delay. The solution to (6) is [26]:

$$\mathbf{f} = \mathbf{R}^{-1}\mathbf{p}, \tag{7}$$

where, $\mathbf{R} = E(\mathbf{y}(n)\,\mathbf{y}^H(n))$, $\mathbf{p} = E(x^*[n-\delta]\,\mathbf{y}(n))$ are, respectively, the autocorrelation and cross-correlation.

Similarly for the case with BEM, the same MMSE criterion may be applied. However, the matrix signal model is constructed as follows, for the kth block [23]

$$\mathbf{y}(k) = \mathbf{H}(k)\mathbf{x}(k) + \mathbf{v}(k), \tag{8}$$

where $\mathbf{H}(k)$ is a lower triangular $N \times N$ matrix with elements $[\mathbf{H}(k)]_{m,n} = h(kN + m - 1; m - n)$. Note that zero padding is assumed in this case, so that the last L (channel length) elements of $\mathbf{x}(k)$ are zeros, to prevent interblock interference (IBI) [27]. The channel matrix is expressed in terms of the basis functions as

$$\mathbf{H}(k) = \sum_{q=0}^{Q} \mathbf{D}_q \mathbf{H}_q(k), \tag{9}$$

where $\mathbf{D}_q = \operatorname{diag}[1, e^{jw_q}, \dots, e^{jw_q(N-1)}]$, and $\mathbf{H}_q(k)$ an equivalent channel matrix with elements constructed from the basis coefficients $h_{q,l}(n)$ in (4). Next, make the assumption that, due to slow variations, the coefficients $h_{q,l}(n)$ are block-invariant, that is,

$$h_{q,l}(n) = \widetilde{h}_{q,l}(k), \quad n = kN, \dots, (k+1)N - 1 \tag{10}$$

are constants for the kth block (recall that n is the discrete-time index, while k is the block index). Then, the equivalent $N \times N$ channel matrix $\mathbf{H}_q(k)$ is Toeplitz, with the first column constructed from $[\widetilde{h}_{q,0}(k), \widetilde{h}_{q,1}(k), \dots, \widetilde{h}_{q,L}(k)]^T$.

Hence, the equivalent block matrix $\mathbf{H}_q(k)$ is composed entirely of time-invariant (with respect to the same block) quantities, with a Toeplitz structure typical of regular time-invariant channels [27]. In other words, the time-variance exhibited by the channel matrix $\mathbf{H}(k)$ is now captured by the basis functions in $\mathbf{D}_q$, facilitating the estimation of the block-invariant coefficients $[\widetilde{h}_{q,0}(k), \widetilde{h}_{q,1}(k), \dots, \widetilde{h}_{q,L}(k)]$, which can then be used to reconstruct $\mathbf{H}(k)$ in (9).

The above equalization strategies assume knowledge of the channel, which is not always known *a priori*. Therefore, estimates will be obtained in the next section.

3.4. Channel Estimation.

3.4. Channel Estimation. While channel equalization is typically not required by most current BAN implementations, as described in the previous section, channel estimation is by contrast a necessity if any practical form of system adaptation is envisioned. In the general case, a vector or FIR filter is estimated for a frequency-selective channel. And in the frequency-flat case, the use of training symbols for estimation can be interpreted as an evaluation of the environment equality, for example, signal-to-noise ratio, which has an impact on the system performance. This quality evaluation allows for appropriate adaptation in the communication system parameters.

As in the previous section, we are interested in baseline performance with channel estimation. Therefore, a conventional maximum likelihood (ML) estimation strategy is used. Training symbols located in preamble, that is, at the beginning of the block, are used for estimation. Two cases are again distinguished based on the absence or presence of BEM representation.

3.4.1. Estimate without BEM Representation. For the quasistatic case, without BEM, we consider an estimate using training symbols for (possibly) multiple consecutive blocks, or an aggregate block. The motivation is that, if the consecutive blocks are quasistatic with the same channel coefficients, utilizing the aggregate training symbols from these blocks produces a better estimate, compared to that obtained from only a single block. Consider the first block, at instant k, in the aggregate, with M training symbols, that is, $x[k], \dots, x[k+M-1]$ are known symbols. Denote the corresponding index set $I_1 = \{k, \dots, k+M-1\}$. Then, we can form the received signal portion corresponding to the training symbols as [22],

$$\mathbf{y}_{I_1} = \mathbf{x}_{I_1}\mathbf{h} + \mathbf{v}_{I_1}. \tag{11}$$

Suppose there are μ consecutive blocks in the aggregate block, with subsequent index sets $I_2, \dots, I_\mu$, these quantities can be stacked to form

$$\begin{bmatrix} \mathbf{y}_{I_1} \\ \ddots \\ \mathbf{y}_{I_\mu} \end{bmatrix} = \begin{bmatrix} \mathbf{x}_{I_1} \\ \ddots \\ \mathbf{x}_{I_\mu} \end{bmatrix} \mathbf{h} + \begin{bmatrix} \mathbf{v}_{I_1} \\ \ddots \\ \mathbf{v}_{I_\mu} \end{bmatrix}, \tag{12}$$

or

$$\mathbf{y}_\Sigma = \mathbf{x}_\Sigma \mathbf{h} + \mathbf{v}_\Sigma. \tag{13}$$

The ML channel estimate is

$$\mathbf{h}_{\mathrm{ML}} = \mathbf{x}_\Sigma^\dagger \mathbf{y}_\Sigma, \tag{14}$$

where $(\cdot)^\dagger$ denotes the Moore-Penrose pseudoinverse [26].

3.4.2. Estimate with BEM Representation. Similarly, for the BEM case, the channel estimate is obtained first for a single block, then extended to multiple consecutive blocks [23].

For the single-block estimate, note that to determine an output symbol $y(n)$, the input symbols $x(n-L), \dots, x(n)$ are needed. However, if T training symbols in the kth block, $\mathbf{x}_T(k) = \{x(n), n = kN, \dots, kN + T - 1\}$, are located in the *preamble position* (at the beginning of the block), then, due to zero padding in the input blocks, the corresponding first T output symbols $\mathbf{y}_T(k) = \{y(n), n = kN, \dots, kN + T - 1\}$ can be determined (this is also implied by (8)). Hence,

$$\mathbf{y}_T(k) = \sum_{q=0}^{Q} \mathbf{D}_{q,T} \mathbf{H}_{q,T}(k) \mathbf{x}_T(k) + \mathbf{v}_T(k), \tag{15}$$

where $\mathbf{D}_{q,T}$, $\mathbf{H}_{q,T}(k)$, $\mathbf{v}_T(k)$, are submatrices of the matrices in (8), (9), partitioned from the upper-left corner in obvious manners, for example, $\mathbf{D}_{q,T} = \operatorname{diag}[1, e^{jw_q}, \dots, e^{jw_q(T-1)}]$ is a $T \times T$ diagonal (sub)matrix of $\mathbf{D}_q$. For extensions to the more general cases where the T training symbols are *not* located in preamble, for example, dispersed throughout the block, see [28].

For $T > L$, the Toeplitz structure of $\mathbf{H}_{q,T}(k)$ implies that

$$\mathbf{H}_{q,T}(k)\ \mathbf{x}_T(k) = \mathbf{X}_T(k) \mathbf{h}_q(k), \tag{16}$$

where $\mathbf{X}_T(k)$ is a $T \times (L+1)$ Toeplitz matrix, with the first column consisting of the training symbols $[x(0), \dots, x(T-1)]^T$ and $\mathbf{h}_q(k) = [\widetilde{h}_{q,0}(k), \widetilde{h}_{q,1}(k), \dots, \widetilde{h}_{q,L}(k)]^T$, that is, the block-invariant coefficients from (10). Then, from (15), (16),

$$\mathbf{y}_T(k) = \mathbf{\Phi}(k)\mathbf{h}(k) + \mathbf{v}_T(k), \qquad (17)$$

where $\mathbf{h}(k) = [\mathbf{h}_0(k)^T, \mathbf{h}_1(k)^T, \dots, \mathbf{h}_Q(k)^T]^T$ is the (block-invariant) vector of all the basis coefficients, and $\mathbf{\Phi}(k)$ the matrix of (modulated) training symbols defined as: $\mathbf{\Phi}(k) = [\mathbf{D}_{0,T}\ \mathbf{X}_T(k), \mathbf{D}_{1,T}\ \mathbf{X}_T(k), \dots, \mathbf{D}_{Q,T}\ \mathbf{X}_T(k)]$, with $\mathbf{D}_{q,T}$ the diagonal matrices of basis functions from (15). Then a maximum-likelihood estimate of $\mathbf{h}(k)$ can be obtained as

$$\mathbf{h}_{\mathrm{ML}}(k) = \mathbf{\Phi}(k)^{\dagger}\mathbf{y}(k), \qquad (18)$$

where $(\cdot)^{\dagger}$ denotes the Moore-Penrose pseudoinverse.

Next, the aggregate block estimate is considered, when the basis coefficients $\mathbf{h}(k)$ remain valid over M multiple consecutive blocks (each of N data symbols), the training symbols from these multiple consecutive blocks can be combined for improved channel identification as follows.

Consider the next consecutive block $k+1$. Similar to(17)

$$\mathbf{y}_T(k+1) = \mathbf{\Phi}_{\mathrm{MB}}(k+1)\mathbf{h}(k) + \mathbf{v}_T(k+1), \qquad (19)$$

where the fact $\mathbf{h}(k+1) = \mathbf{h}(k)$ is used. Furthermore, the multiple-block matrix, $\mathbf{\Phi}_{\mathrm{MB}}(k+1)$, of modulated training symbols for the first consecutive block is related to the single-block version by $\mathbf{\Phi}_{\mathrm{MB}}(k+1) = e^{jNw_q}\mathbf{\Phi}(k+1)$, and more generally, $\mathbf{\Phi}_{\mathrm{MB}}(k+\kappa) = e^{j\kappa N w_q}\mathbf{\Phi}(k+\kappa)$. This can be seen by computing (4) for the κth consecutive block: $h(n+\kappa N; l) = \sum_{q=0}^{Q} h_{q,l}(n+\kappa N)e^{jw_q(n+\kappa N)} = \sum_{q=0}^{Q} e^{j\kappa N w_q}(h_{q,l}(n)e^{jw_q n})$, which accordingly changes $\mathbf{D}_q$ in (9) to the diagonal matrix $e^{j\kappa N w_q}\mathbf{D}_q$.

As a result, the M consecutive blocks combine to yield

$$\begin{bmatrix} \mathbf{y}_T(k) \\ \mathbf{y}_T(k+1) \\ \vdots \\ \mathbf{y}_T(k+M-1) \end{bmatrix} = \begin{bmatrix} \mathbf{\Phi}_{\mathrm{MB}}(k) \\ \mathbf{\Phi}_{\mathrm{MB}}(k+1) \\ \vdots \\ \mathbf{\Phi}_{\mathrm{MB}}(k+M-1) \end{bmatrix} \mathbf{h}(k) + \mathbf{v}_{\Sigma}(M), \qquad (20)$$

or

$$\mathbf{y}_{\Sigma}(M) = \mathbf{\Phi}_{\Sigma}(M)\mathbf{h}(k) + \mathbf{v}_{\Sigma}(M). \qquad (21)$$

Then a maximum-likelihood estimate of $\mathbf{h}(k)$ can be obtained as

$$\mathbf{h}_{\mathrm{ML}}(k) = \mathbf{\Phi}_{\Sigma}(M)^{\dagger}\ \mathbf{y}_{\Sigma}(M). \qquad (22)$$

Evidently, a larger M provides a more accurate estimate of the overall basis coefficients $\mathbf{h}(k)$, since more training symbols are available.

4. Optimization Framework

The previous section provides the means to monitor or track the operating environment, as characterized by the encountered channel conditions. Thus, at this point, it should be possible to quantify of the channel quality, for example, producing a QoS metric, in order to motivate adaptation methods for enhancing the QoS. However, we will defer these developments until the following section. Instead, a framework for constructing and combining these methods is considered. In fact, since the ability to enhance QoS in wireless networks is important for resource sensitive scenarios, myriad methods have been proposed [29–32]. Unfortunately, these methods are not always compatible from a resource utilization perspective. Furthermore, it is often not obvious how the various schemes may be used together in the same system for optimal QoS gains [33, 34]. In this section, a unified approach towards uniting various signal processing methods for QoS regulation is examined, mainly based on mathematical optimization [35, 36].

4.1. QoS Metrics. QoS is itself a polysemous term, in that depending on the context considered, many criteria may be construed as conveying system quality [10, 29, 37]. Generally, in using QoS to attain a unified method for assessing system performance, the following properties are essential: relevance, consistency, repeatability and numerical quantifiability. From a signal processing perspective, the last point is perhaps most practical, because without a numerical value, decision algorithms may not be feasibly proposed. At the same time, if the numerical values do not reflect in a relevant manner the intended performance, the signal processing method applied cannot be expected to fulfill the intended objective. In a communication network, the following criteria may be considered as indicators of the QoS [10, 34, 38].

(i) Data rate: the rate of information that is transferred over a network. Depending on the nature of the data, the rate required can vary significantly. For example, a text message needs only low data rate, while a video stream may consume a significant amount of information over time.

(ii) Bit-error rate (BER), mean-squared error (MSE) [26, 39]: metrics to quantify the errors between the transmitted and received signals. These quantities are arguably among the most commonly used metrics to compare system performances.

(iii) Latency: the delay imposed by the communication system. Some applications may be more delay-sensitive or delay-tolerant than others, for example, a real-time conversation is often delay-sensitive.

(iv) Security: even though it certainly represents an important system feature, treating security as a QoS parameter to be assigned has not been a very popular practice until more recently [10, 32]. The reason is that many definitions of security exist, and metrics for security are also difficult to be constructed. However, when a reliable encryption scheme is used, the system security can be characterized almost exclusively based on the cryptographic key length involved [7, 8].

(v) Economic costs or profits: the viability of a proposed system often depends on its potential to generate economic incentives. In some cases, this may be reflected by the number of network subscribers. However, other short-term and long-term scenarios may distort the obtained results in an unpredictable manner. For example, while the initial number of subscribers may indicate economic prosperity, if the social and political changes somehow discourage users from adopting a certain communication application, then significant measures beyond the signal processing may be needed to ensure a timely and adequate response.

While the above criteria can be used to propose QoS methods, practical signal processing algorithms often do not directly account for or make decisions based on these criteria. This is due either to mathematical intractability in the problem formulation, or more practically to difficulty in obtaining these quantities in an accurate or timely manner. For example, estimating the BER accurately, and on a regular basis, may require modified communication protocol or unnecessarily high resource consumption [29, 40, 41].

Instead, a variety of QoS metrics are typically used to enable system adaptation. These metrics are more readily available quantities, that are nonetheless related to the QoS in a meaningful manner. Specifically, the relationship between a QoS criterion and an associated QoS metric should ideally be bijective (one-to-one and onto) and monotonic. Then, a proposed signal processing method may be based entirely on the QoS metric, and still deliver adequate QoS performance. However, since ideal QoS metrics may not always be found, the following cases and practical issues need to be considered.

(i) A QoS metric may be ideal in an existential sense only. For instance, in general, it is known that BER is a monotonic and bijective function of the channel SNR. However, for certain types of channel settings, the relationship may be highly nonlinear or may not even admit a closed form expression. In other words, while the ideal relationship certain exists, it may not be known or expressible in a practical form. Then, the adaptation method needs to rely on empirical or simulated performance to parametrically set the thresholds for system performance.

(ii) A QoS metric may be bijective but nonmonotonic. It is still possible to propose adaptation methods based on this metric. However, the system performance is prone to metric errors: minor errors may translate to high performance errors. Moreover, the system adaptation may not be possible based on a threshold-scheme, but may have to be based on a table of values, which should moreover be sufficiently exhaustive.

(iii) A QoS metric may be injective (one-to-one) but not surjective (onto). This implies that certain QoS performance values may not be monitored or assessed by the metric. However, in this case, such a scenario likely indicates that the requested QoS performance is infeasible with the given hardware resources or infrastructure.

(iv) A QoS metric may be surjective but not injective. Since ambiguous cases exist, with potential large differences in input values, the system performance may also be prone to metric errors. Moreover, a threshold-based scheme may not be possible.

It should be noted that the last case is perhaps the least desirable. This is because without an injective mapping, the relationship needs to be known exhaustively to ensure that all cases are accounted for. Otherwise, the system performance may vary unpredictably whenever the metric deviates from a known or nominal range of values.

Various quantities have been used as QoS metrics to adapt the system structure and improve the QoS performance, including training or pilot data symbols, equalizer outputs, or estimated errors from decision-directed algorithms [32, 42]. Generally, for methods that target the BER performance, the metric is usually related to the signal-to-noise or signal-to-interference ratios. And for methods that seek to improve the data rate, the transmission protocol or data block structure usually provide the suitable metric for adaptation.

4.2. Standard Forms for Optimization. Constrained optimization facilitates unifying various QoS enhancing methods towards a common objective [35, 43, 44]. Mathematically, this involves first defining the problem, which in turn consists of [34–36, 45] as the following:

(i) formulating an objective function, to be minimized or maximized,

(ii) specifying equality and inequality constraints,

(iii) accounting for unknown quantities or variables which may affect the QoS.

In practice, these seemingly innocuous steps leading to a good problem formulation may be quite challenging. Among the obstacles encountered.

(i) Closed form or analytical expressions for typical constraints such as delay, bandwidth and power consumption may be intractably cumbersome, being complicated functions of many nondeterministic variables [36]. In that case, these quantities have to be estimated, often with only average or worst case values. Clearly, an algorithm that is based on false inputs is bound to deliver unreliable results.

(ii) Due to the dynamic nature of the wireless channels, the operating variables may change constantly, requiring frequent system updates. To this end, the estimation and tracking methods proposed in this paper are based on practical channel models which take into account important aspects from the physical scenarios.

(iii) The optimality bestowed by the mathematical solution may not be directly reflected into the real-world performance. This is often because the outcome of an optimization problem may overlook practical requirements such as buffering, and the inability of the human subjects involved to exactly implement the required steps necessary to furnish the optimal solution.

Nonetheless, formulating an appropriate optimization problem to model the behavior of a system represents an important first step to further advancement. This is because, once formulated accurately, the mathematical tools available to solve problems of well-defined forms or structures are relatively comprehensive and mature. Therefore, in an QoS framework context, it is often the problem formulation itself that is problematic and time-consuming. Generally, the problem of interest is reformulated into a standard form. Perhaps the most popular standard form is as follows [43, 44]:

(i) Find vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ in order to

$$\begin{aligned} \text{minimize} \quad & f(\mathbf{x}), \\ \text{subject to} \quad & g_i(\mathbf{x}) \leq 0, \quad i = 1, 2, \ldots, m, \\ & h_i(\mathbf{x}) = 0, \quad i = 1, 2, \ldots, p, \end{aligned} \tag{23}$$

where $\mathbf{x} \in \mathcal{R}^n$ is the optimization variable, $f : \mathcal{R}^n \to \mathcal{R}$ is the objective or cost function, the inequalities and equalities constraints are, respectively, accounted for by $g_i : \mathcal{R}^n \to \mathcal{R}$ and $h_i : \mathcal{R}^n \to \mathcal{R}$.

In addition, for various QoS problems, the optimization variables are integers or of discrete values. The presence of discrete variables can dramatically alter the complexity of the problem, especially when the cardinality of the set is sufficient large. Whenever both discrete and continuous variables appear in the optimization problem, it is referred to as mixed-integer (MI). Corresponding to the standard form of continuous constrained optimization in (23), mixed-integer nonlinear programming (MINLP) problems of the following form will be considered [46, 47]:

$$\begin{aligned} \min_{\mathbf{x},\mathbf{y}} \quad & f(\mathbf{x}, \mathbf{y}), \\ \text{subject to} \quad & g_i(\mathbf{x}, \mathbf{y}) \leq 0, \quad i = 1, 2, \ldots, m, \\ & h_i(\mathbf{x}, \mathbf{y}) = 0, \quad i = 1, 2, \ldots, p, \\ & \mathbf{x} \in \mathbf{X} \subseteq \mathbf{R}^n, \\ & \mathbf{y} \in \mathbf{Y} \subseteq \mathbf{Z}^n. \end{aligned} \tag{24}$$

It should be noted that MI problems are NP-hard [35, 48]. For many continuous problems of the form (23), the optimality of a solution can be checked using the Karush-Kuhn-Tucker (KKT) conditions, which describe a set of necessary first-order requirements for a point $\overline{\mathbf{x}}$ to be a (local) minimum point. However, in the mixed-integer domain, optimal conditions only exist for a few limited special cases [46, 47].

The KKT conditions are particularly useful for cases where closed-form analysis is desired. In principle, it is possible to solve the simultaneous equations to obtain the KKT candidates. In practice, the equations are nonlinear, which may cause difficulties in computer implementations. In fact, when the various gradients for the optimization procedure are not analytically available, some numerical form of gradient estimation or interpolation would be needed. Alternatively, methods that numerically search for the solutions directly can be used [43, 49]. For the MINLP formulation, a solver known as the branch-and-bound algorithm can be applied, based on the concepts of separation, relaxation and fathoming [46, 47].

Furthermore, there are resource allocation scenarios in which multiple objectives exist. Then scalarization is an approach that simply combines the objectives with a linear combination operation [50, 51]. Thus, given objectives $f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_M(\mathbf{x})$. Then a scalarized or weighted sum objective can be defined as

$$f_0(\mathbf{x}) = \sum_{m=1}^{M} \lambda_m f_m(\mathbf{x}), \tag{25}$$

where λ_m provides a means to subjectively give preference to certain objectives. In other words, the various weighting coefficients are used to reflect the relative importance of the corresponding objective: a larger weight indicates that more emphasis is placed on the corresponding optimization aspect.

4.3. Block-by-Block Resource Allocation.

As described in Section 3.1, user activities and movements in BAN applications lead to inherently dynamic operating environments. Therefore, the associated time-varying channels cannot be effectively handled by static optimization. Instead, a block-by-block scheme, coinciding with the block used for estimation and equalization, is adopted. Essentially, given that the operating environment is estimated per block, the associated QoS metric can be also updated per block in response. Taking into account the issues described in [35, 36, 52], the block-by-block framework can be conceptually represented as in Figure 2.

For each block iteration, the optimization problem is renewed according to the operating environments. The updated solution is then utilized to direct the adaptation methods towards feasible solutions, with improved QoS while still satisfying the constraints. In particular, the QoS metrics, as described in Section 4.1, are computed for each block, so that the adaptation methods can tune its system parameters for performance requirements.

At this point, it behooves us to examine the implementation requirements of the described framework in the BAN context. As described in Section 2, by design, the peripheral nodes typically do not possess advanced computational capabilities. Therefore, the operations required for optimization algorithms would most practically be executed by the central node only. In this respect, the strategy is analogous to the asymmetric master-slave architecture described in [53], where the peripheral slaves are directed by the master

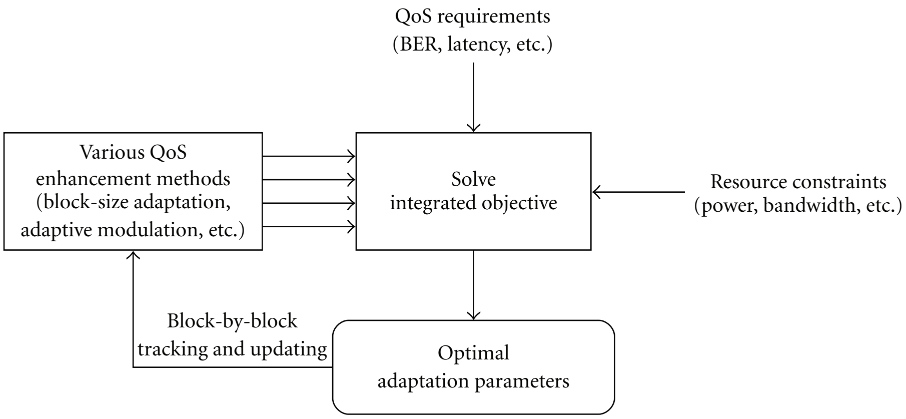

Figure 2: The conceptual framework of block-by-block optimization.

central node. Moreover, in practice, possibilities for reducing the optimization operations should be exploited, depending on the adaptation methods involved. For instance, in the subsequent sections, it is shown that the combination of block-size adaptation and adaptive modulation can be made in an iterative manner, which is suitable for practical implementation.

5. Adaptation Methods

With the objective of improving QoS, many existing methods can be found in the literature, for example, from [29–32] and the references therein. Therefore, it would be beyond the scope of this paper to merely survey all these existing techniques even in a superficial manner. There is of course also the danger of overcomplicating the design with too many adaptation schemes, leading to impractical implementation requirements. As such, the goal here is to examine specific schemes that are particularly suitable for subsequent integration in a unified framework. Among other properties, the methods should exhibit flexibility and adaptivity, which should be parametrically adjustable, so that they can accommodate a wide range of operating conditions. As such, this section should not be regarded as an exhaustive repository of currently available techniques, but rather as an initial foundation for supplementary methods. In other words, for applications that require or can provide additional adaptation capabilities, they can be considered in an analogous fashion, with similar design factors and constraints.

5.1. Channel Tracking and Block-Size Adaptation. In Section 3.4, the estimation scheme utilizes training symbols, assumed to be present in preamble for a fundamental processing block, of fixed size. More training leads to improved estimation, which can be achieved by aggregating consecutive processing blocks, to form a larger processing block. However, the estimation improvement is only valid when the channel coefficients remain the same over the entire aggregate processing block. In other words, there is an associated channel tracking problem involved with the adaptation of the block-size for processing.

The problem can be stated as follows. Let the objective $F(\mu) = M\mu$ be the total number of training symbols as a function of M, the number of training symbols in a fundamental block, and μ, the number of fundamental blocks in the aggregate. Note that M is typically a fixed constant, defined by the training density. Also, let $\mathbf{h}_i$ be the channel associated with the ith fundamental block in the accumulated. Then, the block-size adaptation problem is equivalent to

$$\begin{aligned} &\text{maximize} \quad F(\mu) = M\mu, \\ &\text{subject to} \quad \mu \in \mathbf{Z} \text{ (an integer)}; \quad \mu \leq \text{bsize}_{\max}, \\ &\qquad\qquad \mathbf{h}_1 = \mathbf{h}_2 = \cdots = \mathbf{h}_\mu \text{ (channel invariance).} \end{aligned} \tag{26}$$

Hence, the block-size adaptation is a mixed-integer optimization problem (which can be converted to a standard form [46]). It turns out that an iterative procedure known as variable-size block construction can be used to find the appropriate block size for both the quasistatic case [22] and the BEM case [23]. Essentially, the idea is to track the estimation error of the channel coefficient estimates, and compare against a threshold for decision. In other words, the QoS metric for block-size adaptation is the amount of change in the channels between consecutive blocks.

However, there are several limitations with these schemes. First, for the quasistatic approach, the coefficients are of course unequal across the blocks with probability one (especially in the presence of estimation errors and noises). This means that the corresponding MMSE equalizer and other QoS metrics based on the ML channel estimate will inevitably suffer from errors. Second, while the BEM approach produces improvement, it is based on a deterministic model which is targeted specifically for multipath fading channels, for example, with Jakes spectrum. In addition, certain parameters are assumed known for proper operations, such as the number of bases and frequencies present. While methods exist for addressing such issues [24], the fundamental limitation is for channels not conforming to a multipath model, in which case the deterministic BEM assumed may not represent a suitable match. In the BAN context, such scenarios may occur for the implanted devices, where the material composition and structure of the human body contribute to the channel itself.

Alternatively, a more statistical approach may be pursued, using the Kalman filter for tracking the channel [54]. However, the conventional Kalman filter itself requires a state space model, which are not always known. In addition, the multistate dynamics in BAN, due to user movements, also lead to different state space models to be formulated. As such, an approximate model based on random walk can be employed. Consider the output and process equations, where in this case the state represents the channel $\mathbf{h}_i$

$$\begin{aligned}\mathbf{y}_i &= \mathbf{X}_i\mathbf{h}_i + \mathbf{v}_i,\\ \mathbf{h}_{i+1} &= \mathbf{F}_i\mathbf{h}_i + \mathbf{G}_i\mathbf{w}_i.\end{aligned} \tag{27}$$

with the covariance matrix $\text{Cov}[w_i] = \mathbf{W}$. Then, the random walk Kalman filter (RWKF) makes the following parameter selections [24]

$$\mathbf{F}_i = \mathbf{I}, \qquad \mathbf{G}_i = \mathbf{I}, \qquad \mathbf{W} = \sigma_w^2\mathbf{I}, \tag{28}$$

which essentially describes a Gauss-Markov process with unity correlation. In this case, the Kalman filter solution depends on one user-dependent quantity, namely the variance quotient $\kappa^2 = \sigma_w^2/\sigma_v^2$, that is, between the process and measurement noise. In the context of BAN channels, the variance σ_w^2 describes the mean square rate of parameter change, which is related to the channel coherence time: a larger value of σ_w^2 implies more rapid variations (smaller coherence time). Therefore, each channel state, as characterized by an associated coherence time (or equivalently, Doppler shift f_m), is associated with a particular variance value. As such, by tracking the corresponding σ_w^2 for each data block, the channel change can be detected for block-size adaptation. Compared to the BEM scheme, the difference is that minimal knowledge of the channel model is assumed. As noted in [24], this seemingly naive reduction in parameters does produce surprisingly acceptable results in practical applications. Therefore, in cases where no prior knowledge is available for the channel structure, the use of RWKF represents a potential solution for channel tracking.

5.2. Adaptive Modulation. For the block-by-block optimization framework, an estimate of the channel quality is basically provided for each block iteration. In other words, the channel quality over each such constructed block can be considered constant, while from block to block, the channel quality changes. This knowledge can also be used to perform adaptive modulation, changing the modulation mode for the data symbols on a block-by-block basis. When the channel is benign or of good quality, a higher-order modulation constellation, for example, 16-QAM, can be used for efficiency while still maintaining a good QoS, defined by a target BER. However, when the channel is hostile or of poor quality, a lower-order modulation mode, for example, BPSK, is selected to maintain an acceptable QoS. This methodology permits an overall improvement in spectral efficiency [22, 32, 42, 55]. In conjunction with block-size adaptation, the corresponding optimization problem can be stated as follows.

Let the objective $G(q) = \log_2 q$ be the throughput (number of transmitted bits per symbol) as a function of the modulation mode q. For simplicity, let us assume that there are 4 modulation modes, that is, $q = 0$ (no transmission), 2 (BPSK), 4 (4-QAM), 16 (16-QAM). Then adaptive modulation with block adaptation is equivalent to

$$\begin{aligned}\text{maximize}\quad & G(q) = \log_2 q,\\ \text{subject to}\quad & \mu \in \mathbf{Z} \text{ (an integer)};\quad \mu \leq \text{bsize}_{\max},\\ & \mathbf{h}_1 = \mathbf{h}_2 = \cdots = \mathbf{h}_\mu \text{ (channel invariance)},\\ & \text{BER}(\mu, q) \leq \text{BER}_{\max};\quad q \in \{0, 2, 4, 16\},\\ & \sigma_x^2 = \text{constant},\end{aligned} \tag{29}$$

where $\text{BER}_{\max}$ specifies the maximum acceptable bit-error rate for a desired QoS, and $\sigma_x^2 = E(|x[n]|^2)$ is the symbol energy. A two-layer strategy can be shown to approximate the above problem, by iteratively searching for the optimal (μ, q) [22]. As such, a practical implementation can be made to combine block-size adaptation and adaptive modulation. Several possible QoS metrics can be used for adaptive modulation, including pseudoSNR and MSE-based metric. The precise expressions, as well as other issues related to adaptive modulation, including the effects of metric errors, can be found in [22, 55].

5.3. Other Candidates. While block-size adaptation and adaptive modulation can be combined without significant computational and protocol requirements in an iterative procedure [22], the introduction of other adaptation methods into the optimization framework may not lead to elegant solutions. Then, numerical methods and the branch-and-bound algorithm need to be applied to solve the associated optimization problem [43, 46, 49].

In the context of secure BAN, at least another aspect of adaptation should be considered. Specifically, for biometric key binding schemes such as fuzzy commitment, an error control code (ECC) is inherently needed. At the same time, ECC can also play a role in mitigating channel noises, that is, improving QoS. Based on knowledge of identified channel, a channel metric can be used to select the operating ECC mode. This method of adapting the QoS according to channel conditions is known as adaptive coding, and can be effective in enhancing both the biometric key binding module as well as the overall system performance [55].

Last but not least, for the central node device, which can be worn on the chest similar to the Hidalgo Equivital belt for physiological monitoring, the possibility of multiple antenna reception can be considered. In this case, the associated adaptation problem involves allocating the number of antennas depending on the estimated channel quality per block. At the expense of increased computational complexity at the central

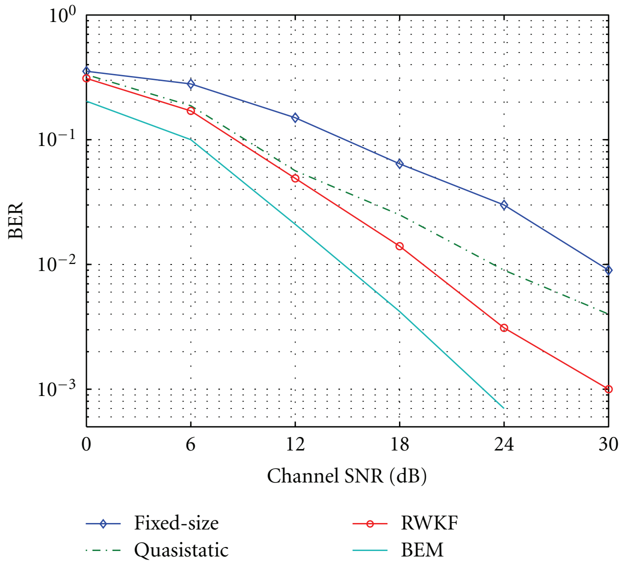

Figure 3: BER comparisons for various channel tracking schemes.

node, this approach can play an important role in regulating the QoS, as quantified by data rate and bandwidth efficiency [32, 42, 56].

6. Simulation Examples

In this section, a number of example scenarios are considered to illustrate the potential benefits of utilizing the described QoS framework.

6.1. Tracking Performance for Block-Size Adaptation. First, the tracking performance is studied for the following schemes: fixed size, quasistatic approximation, BEM, and RWKF. It should be noted that the last three schemes create variable-size processing blocks. The following settings are utilized: data symbols with 4-QAM alphabet, block size $N = 63$, number of training symbols $T = 20$, channel length $L = 3$, with BEM parameters $Q = 2$, $K = 5N$.

Figure 3 shows the associated BER performances. It can be seen that the block-size adaptation allows for improved performance, compared to the fixed size case. Moreover, the RWKF is closest to the BEM case, despite being based on a simple approximate modeling assumption. This shows promise for the RWKF applicability where little is known about the channel structure. It should also be noted that, from a computational perspective, the RWKF is preferred to the BEM construction, which requires more complicated operations.

6.2. Data Scrambling and the Effects of Fading Channels. Next, the effects of multipath fading for security applictions in BAN are examined. To this end, a data scrambling scheme based on interpolation and sampling (INTRAS), previously described in [2], is utilized. Since this scheme operates at a signal-level, it is directly affected by the physical layer channel distortions. A high-level summary of the INTRAS scheme is as follows. First, the scrambling step is

$$x_d[n] = \text{INTRAS}(x[n], d[n]) \tag{30}$$

with input $x[n]$ and key sequence $d[n]$. The corresponding descrambling step for ideal recovery of the original signal is

$$x[n] = \text{INTRAS}^{-1}(x_d[n], d[n]) \tag{31}$$

To account for the channel distortion, the signal seen at the input to the descrambler or receiver side is

$$\widehat{x_d[n]} = x_d[n] + v[n] = \text{INTRAS}(x[n], d[n]) + v[n], \tag{32}$$

where $v[n]$ is the AWGN. This represents the AWGN case. More realistic models for the channel propagation paths involve the consideration of multipath fading models. Therefore, two additional types of channels are investigated, characterizing the trunk-to-limb link (fast fading) and the trunk-to-trunk link (slow fading) as described in Section 3.1.

Depending on the key used for descrambling, there are two main recovery strategies shown in the results. Let $d[n]$, $d_{\text{BAN}}[n]$, $d_{\text{non-BAN}}[n]$, be, respectively, the original key sequence used for scrambling (i.e., ideal key), a key sequence from a device in the same BAN (i.e., correct key), and a key sequence from an intruder outside of the intended BAN (i.e., incorrect key). Then the corresponding MSE performances, between the original signal and the signal recovered using one of these key sequences, can be computed. For example, when the correct key is known

$$\text{MSE}_{\text{correct}} = \text{MSE}\left(x[n], \text{INTRAS}^{-1}\left(\widehat{x_d[n]}, d_{\text{BAN}}[n]\right)\right). \tag{33}$$

The performances with these channel fading effects are shown in Figure 4 when using Lagrange interpolation [2]. Compared to the AWGN lower bound, the performance of the correct key for fast fading case, characterizing the trunk-to-limb link, is more severely degraded. Physically, the degradation is caused by the more extreme movements of the limb relatively to the body trunk. On the other hand, the results for the incorrect keys do not exhibit significant distinctiveness for the different channel scenarios. This effect is due to the fact that the incorrect keys all already produce poor MSE performance, even without the fading channels.

6.3. Performance of Data Scrambling Using Block-Size Adaptation. Having observed the degradations caused by multipath fading in the previous simulation, the block-size adaptation approach is now utilized to improve the performance by allocating the block-size according to the encountered channel. For this simulation, the trunk-to-limb path, which is fast fading as surveyed in Section 3.1, is the channel scenario for the three block processing schemes: fixed, variable and ideal.

The resulting performance with channel fading effects is shown in Figure 5.

It can be seen that with a variable-size block, the MSE for the correct key is further reduced, approaching that

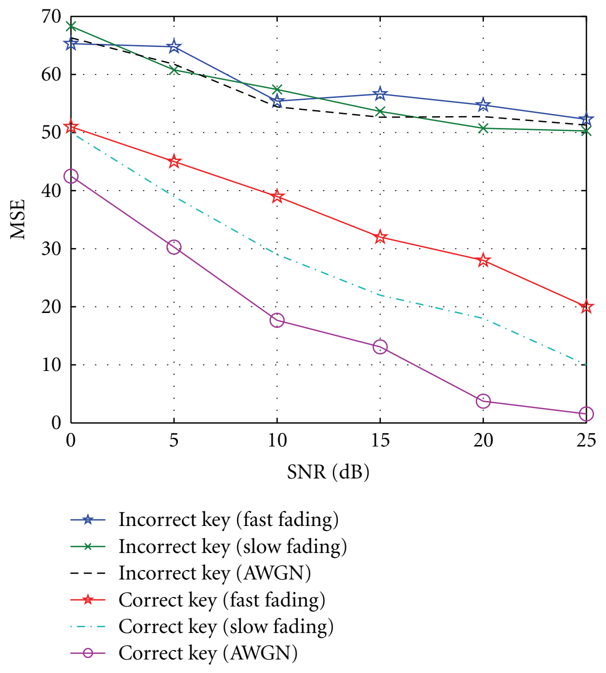

Figure 4: Data scrambling under fading channels.

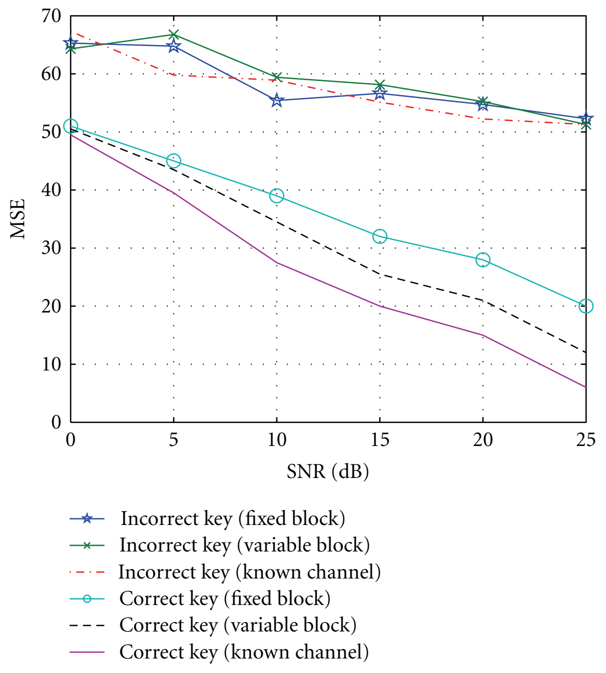

Figure 5: Data scrambling using variable block-size adaptation.

of the ideal scenario with no channel estimation required (assuming prior channel knowledge). On the other hand, the use of variable-size block has no major effect on the incorrect key performance. Since no major effect implies that the MSE is not decreased, this is still a desirable effect. Indeed it means that an authorized intruder does not have any benefit in attempting to compromise a variable-size block system for data scrambling.

7. Concluding Remarks

The BAN methodology presents promising potentials for interesting applications in a wide range of domains, including medical monitoring and mobile multimedia personalization. However, there remain many key problems to be addressed in delivering practical BAN systems, with good QoS at acceptable costs. In this paper, a framework for QoS regulation in secure BANs has been presented based on optimization principles for synergistically uniting various adaptation strategies, each with the ability to enhance one aspect of QoS in the overall system. Central to the framework is a block-by-block processing methodology, which is supported by a tracking algorithm in order to quantify the encountered channel quality. This enables adaptation of various physical layer aspects of the system, including processing block-size and adaptive modulation. The flexibility bestowed by this QoS regulation framework makes it appropriate for adapting secure BANs to a wide range of scenarios, in which the resource constraints and QoS service requirements may vary. Furthermore, other algorithms for enhancing the QoS can also be integrated into the same overall system for additional performance gains. At the same time, there is a tradeoff to be considered in terms of QoS and computational complexity. In particular, the BAN architecture is envisioned to be composed of low-power devices, and may not be suitable to realize algorithms with significant computational requirements.

Acknowledgment

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] C. C. Y. Poon, Y. T. Zhang, and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[2] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 529879, 16 pages, 2008.

[3] M. Ilyas, *The Handbook of Ad Hoc Wireless Networks*, CRC Press, New York, NY, USA, 2003.

[4] G.-Z. Yang, *Body Sensor Networks*, Springer, New York, NY, USA, 2006.

[5] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: a survey," *Mobile Networks and Applications*, pp. 1–23, 2010.

[6] IEEE, The IEEE 802.15 task group 6: Body area networks (BAN), *IEEE Wireless PAN*, 2008, http://www.ieee802.org/15/pub/TG6.html.

[7] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, New York, NY, USA, 4th edition, 2006.

[8] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, New York, NY, USA, 1996.

[9] J. Lopez and J. Zhou, *Wireless Sensor Network Security*, IOS Press, 2008.

[10] A. Mishra, *Security and Quality of Service in Ad Hoc Wireless Networks*, Cambridge University Press, Cambridge, UK, 2008.

[11] F. M. Bui, F. Agrafioti, and D. Hatzinakos, "Electrocardiogram (ECG) biometric for robust identification and secure communication," *Biometrics*. In press.

[12] A. Juels and M. Wattenberg, "Fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security (ACM CCS)*, pp. 28–36, November 1999.

[13] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proceedings of the International Conference on Parallel Processing Workshops*, pp. 432–439, 2003.

[14] F. M. Bui and D. Hatzinakos, "Secure methods for fuzzy key binding in biometric authentication applications," in *Proceedings of the Asilomar Conference on Signals, Systems and Computers*, pp. 1363–1367, Pacific Groove, Calif, USA, 2008.

[15] F. M. Bui, K. Martin, H. Lu, K. N. Plataniotis, and D. Hatzinakos, "Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 118–132, 2010.

[16] P. S. Hall and Y. Hao, *Antennas and Propagation for Body-Centric Wireless Communications*, Artech House, Norwood, Mass, USA, 2006.

[17] Z. H. Hu, Y. I. Nechayev, P. S. Hall, C. C. Constantinou, and Y. Hao, "Measurements and statistical analysis of on-body channel fading at 2.45 GHz," *IEEE Antennas and Wireless Propagation Letters*, vol. 6, pp. 612–615, 2007.

[18] Y. I. Nechayev, P. S. Hall, C. C. Constantinou et al., "On-body path gain variations with changing body posture and antenna position," in *Proceedings of the IEEE Antennas and Propagation Society International Symposium and USNC/URSI Meeting*, pp. 731–734, July 2005.

[19] K. Y. Yazdandoost, H. Sawada, S. T. Choi, J. ichi Takada, and R. Kohno, "Channel characterization for BAN communications," IEEE 802.15-07-0641-00-0ban, 2007.

[20] A. Fort, C. Desset, J. Ryckaert, P. De Doncker, L. Van Biesen, and S. Donnay, "Ultra wide-band body area channel model," in *Proceedings of the IEEE International Conference on Communications (ICC '05)*, pp. 2840–2844, May 2005.

[21] A. Fort, C. Desset, J. Ryckaert, P. De Doncker, L. Van Biesen, and P. Wambacq, "Characterization of the ultra wideband body area propagation channel," in *Proceedings of the IEEE International Conference on Ultra-Wideband (ICU '05)*, pp. 22–27, September 2005.

[22] F. M. Bui and D. Hatzinakos, "Spectrally efficient communication over time-varying frequency-selective mobile channels: variable-size burst construction and adaptive modulation," *EURASIP Journal on Applied Signal Processing*, vol. 2006, Article ID 35352, 16 pages, 2006.

[23] F. M. Bui and D. Hatzinakos, "Identification and tracking of rapidly time-varying mobile channels for improved equalization: a basis-expansion model approach," in *Proceedings of the 5th International Symposium on Communication Systems*, Patras, Greece, July 2006.

[24] M. Niedzwiecki, *Identification of Time-Varying Processes*, John Wiley & Sons, New York, NY, USA, 2000.

[25] G. B. Giannakis and C. Tepedelenlioğlu, "Basis expansion models and diversity techniques for blind identification and equalization of time-varying channels," *Proceedings of the IEEE*, vol. 86, no. 10, pp. 1969–1986, 1998.

[26] S. Haykin, *Adaptive Filter Theory*, Prentice Hall, New York, NY, USA, 1996.

[27] Z. Wang and G. B. Giannakis, "Wireless multicarrier communications: where Fourier meets Shannon," *IEEE Signal Processing Magazine*, vol. 17, no. 3, pp. 29–48, 2000.

[28] X. Ma, G. B. Giannakis, and S. Ohno, "Optimal training for block transmissions over doubly selective wireless fading channels," *IEEE Transactions on Signal Processing*, vol. 51, no. 5, pp. 1351–1366, 2003.

[29] H. Arslan, "Adaptation techniques and enabling parameter estimation algorithms for wireless communications systems," in *Signal Processing for Mobile Communications*, M. Ibnkahla, Ed., CRC Press, 2004.

[30] R. A. Berry and E. M. Yeh, "Cross-layer wireless resource allocation," *IEEE Signal Processing Magazine*, vol. 21, no. 5, pp. 59–68, 2004.

[31] V. Huang and W. Zhuang, "QoS-oriented access control for 4G mobile multimedia CDMA communications," *IEEE Communications Magazine*, vol. 40, no. 3, pp. 118–125, 2002.

[32] S. G. Glisic, *Advanced Wireless Networks: 4G Technologies*, John Wiley & Sons, New York, NY, USA, 2004.

[33] V. Kawadia and P. R. Kumar, "A cautionary perspective on cross-layer design," *IEEE Wireless Communications*, vol. 12, no. 1, pp. 3–11, 2005.

[34] I. Wong and B. Evans, *Resource Allocation in Multiuser Multicarrier Wireless Systems*, Springer, New York, NY, USA, 2007.

[35] A. Eisenblätter and H. F. Geerdes, "Wireless network design: solution-oriented modeling and mathematical optimization," *IEEE Wireless Communications*, vol. 13, no. 6, pp. 8–14, 2006.

[36] M. Van Der Schaar and S. Shankar N, "Cross-layer wireless multimedia transmission: challenges, principles, and new paradigms," *IEEE Wireless Communications*, vol. 12, no. 4, pp. 50–58, 2005.

[37] S. A. Ahson and M. Ilyas, *WiMAX: Technologies, Performance Analysis, and QoS*, CRC Press, New York, NY, USA, 2007.

[38] D. Soldani, M. Li, and R. Cuny, *QoS and QoE Management in UMTS Cellular Systems*, John Wiley & Sons, New York, NY, USA, 2006.

[39] S. Haykin and M. Moher, *Modern Wireless Communication*, Prentice Hall, New York, NY, USA, 2004.

[40] Z. Wang and G. B. Giannakis, "A simple and general approach to the average and outage performance analysis in fading," *IEEE Transactions on Communications*, vol. 51, pp. 1389–1398, 2003.

[41] V. Mitlin, *Performance Optimization of Digital Communications Systems*, Auerbach, 2006.

[42] V. K. Lau and Y. K. R. Kwok, *Channel-Adaptive Technologies and Cross-Layer Designs for Wireless Systems with Multiple Antennas: Theory and Applications*, Wiley-Interscience, New York, NY, USA, 2006.

[43] M. A. Bhatti, *Practical Optimization Methods: With Mathematica Applications*, Springer, New York, NY, USA, 2000.

[44] D. G. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, Springer, New York, NY, USA, 3rd edition, 2008.

[45] H. Boche, M. Wiczanowski, and S. Stanczak, "Characterization of optimal resource allocation in cellular networks," in *Proceedings of the IEEE 5th Workshop on Signal Processing Advances in Wireless Communications (SPAWC '04)*, pp. 454–458, July 2004.

[46] C. A. Floudas, *Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications*, Oxford University Press, Oxford, UK, 1995.

[47] D. Li and X. Sun, *Nonlinear Integer Programming*, Springer, New York, NY, USA, 2006.

[48] R. G. Parker and R. L. Rardin, *Discrete Optimization*, Academic Press, New York, NY, USA, 1988.

[49] J. Nocedal and S. Wright, *Numerical Optimization: Theoretical and Practical Aspects*, Springer, New York, NY, USA, 2006.

[50] G. Eichfeld, *Adaptive Scalarization Methods in Multiobjective Optimization*, Springer, New York, NY, USA, 2008.

[51] S. P. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, Cambridge, UK, 2004.

[52] K. B. Letaief and Y. J. Zhang, “Dynamic multiuser resource allocation and adaptation for wireless systems,” *IEEE Wireless Communications*, vol. 13, no. 4, pp. 38–47, 2006.

[53] G. Zhou, J. Lu, C. Y. Wan, M. D. Yarvis, and J. A. Stankovic, “BodyQoS: adaptive and radio-agnostic QoS for body sensor networks,” in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM ’08)*, pp. 1238–1246, April 2008.

[54] C. K. Chui and G. Chen, *Kalman Filtering: With Real-Time Applications*, Springer, New York, NY, USA, 4th edition, 2009.

[55] L. Hanzo, C. Wong, and M. Yee, *Adaptive Wireless Transceivers: Turbo-Coded, Turbo-Equalized and Space-Time Coded TDMA, CDMA, and OFDM Systems*, John Wiley & Sons, New York, NY, USA, 2002.

[56] A. Hottinen, O. Tirkkonen, and R. Wichman, *Multi-Antenna Transceiver Techniques for 3G and Beyond*, John Wiley & Sons, New York, NY, USA, 2003.