Hindawi Publishing Corporation
Advances in Multimedia
Volume 2007, Article ID 25187, 9 pages
doi:10.1155/2007/25187

Research Article

Energy-Constrained Quality Optimization for Secure Image Transmission in Wireless Sensor Networks

Wei Wang,[1] Dongming Peng,[1] Honggang Wang,[1] Hamid Sharif,[1] and Hsiao-Hwa Chen[2]

[1] *Faculty of Computer and Electronics Engineering, University of Nebraska-Lincoln, Omaha, NE 68182, USA*
[2] *Institute of Communication Engineering, National Sun Yat-Sen University, 70 Lien-hai Rd., Kaohsiung 804, Taiwan*

Received 1 May 2007; Accepted 22 August 2007

Recommended by Tasos Dagiuklas

Resource allocation for multimedia selective encryption and energy efficient transmission has not been fully investigated in literature for wireless sensor networks (WSNs). In this article, we propose a new cross-layer approach to optimize selectively encrypted image transmission quality in WSNs with strict energy constraint. A new selective image encryption approach favorable for unequal error protection (UEP) is proposed, which reduces encryption overhead considerably by controlling the structure of image bitstreams. Also, a novel cross-layer UEP scheme based on cipher-plain-text diversity is studied. In this UEP scheme, resources are unequally and optimally allocated in the encrypted bitstream structure, including data position information and magnitude value information. Simulation studies demonstrate that the proposed approach can simultaneously achieve improved image quality and assured energy efficiency with secure transmissions over WSNs.

1. INTRODUCTION

The constraints in computation, memory, and energy resources are well-known challenges to sensor network designs especially for multimedia transmission. Although recently there has been a rapid increase of interest on wireless multimedia sensor networks (WMSN), many realistic difficulties are in the way of such advancement, including but not limited to data authentication, secret data protection, image transmission quality, and energy efficiency.

Image encryption and decryption are particularly time-consuming [1], hence justifying a compromise solution where image data are only selectively encrypted to reduce the total computational complexity. This concept proves to be effective and efficient considering that the complex interdependence structure among image compression bit streams [1] can be completely hidden by partial encryption. However, there have been very few papers in literature addressing the correlations among such partial encryption methods and the associated wireless transmission approaches, not to mention the corresponding efforts to meet the resource constraints for sensor networks.

Selective encryption can be effectively performed on the positions of image pixels other than the various values of these pixels conveyed in the natural digital image. Besides layered unequal importance [2], wavelet image compressions such as zerotree-based EZW [3], SPIHT [4], or EBCOT [5] based JPEG2000 produce position information of the objects and the magnitude information of objects. Packet losses of position information destroy the bitstream structure which is crucial for decoding; the bitstream structure is not changed if packet losses of magnitude value information occur. This is called position-value (P-V) diversity inborn with wavelet-based image compression, which provides remarkable potentials for designing multimedia selective encryption algorithms.

This paper proposes a cross-layer approach to deliver selectively encrypted images for minimal distortion with strict energy budget constraints. We first develop a simple but effective position-based selective encryption scheme to reduce encryption overhead by tightly controlling the bitstream structure. Cross-layer optimized UEP strategies are then exploited to allocate the resources among selective encrypted structure information, position information, and magnitude information. Overall, minimized distortion in image transmissions is achieved and the goal of energy efficiency is met.

In recent literature on image selective encryption, most of the popular approaches focus on selecting the important DCT or wavelet coefficients. Research in [6] proposes an effective frequency domain significant coefficients

scrambling scheme. To achieve authorized user access control for digital video streaming, a compressed domain scrambling is proposed in [7]. Unfortunately, frequency scrambling techniques usually randomize energy distribution in coefficient matrixes, which sacrifice multimedia compression efficiency according to research in [8]. Similar researches working in frequency domain are found in [9, 10]. Other researches explore selective encryption at entropy coding stage, where the compression performance is not negatively affected. Multiple entropy coding table scheme is proposed in [8] to achieve high-level security. In this approach, entropy coding table is pseudorandomly selected according to the given key. Tree-based selective encryption is proposed in [11], in which the tree structure information is ciphered; without the tree structure information, leaf and children nodes will be put to wrong position, and thus it is impossible to decode the whole image. However, all of these aforementioned works focus on application layer and have not considered the delivery of encrypted images in time-varying wireless channels.

In recent literature on UEP studies for multimedia delivery over wireless networks, most of them focus on rate-distortion or delay-distortion oriented optimization, where different protection levels are applied to different media stream layers. The security factor is largely overlooked. Because selective encryption controls the skeleton of the streaming media and redistributes more importance on cipher-text, traditional optimized UEP schemes are no longer optimal when selective encryption is taken into account. How to transmit image efficiently over WSNs through exploring interdependency and unequal importance nature among selectively encrypted blocks, position information, and value information, has not been extensively discussed in literature.

Wu et al. in [12] proposes an optimized joint source channel coding (JSCC) scheme to achieve minimized total distortion for multiple images over lossy channels simultaneously. The layer-based dependency as well as distortion reduction expectation is well modeled, and combined total distortion is minimized subject to total rate constraint. Hamzaoui et al. survey recent advances in forward error correction (FEC) based scalable image coder in [13], and proposes a local-search-based rate-distortion optimization solution. Li et al. in research [14] develop a real-time link layer retry limit adaptation algorithm for robust video streaming over 802.11-based wireless networks. Multiple video layers are unequally protected by different link layer retry limits. van der Schaar and Turaga in [15] propose cross-layer optimized packtization and retransmission strategies for delay sensitive video delivery over WLANs. The cross-layer optimization problem is formulated as distortion minimization given delay constraints, and significant multimedia quality gain is reported by packtization and retransmission optimization. The aforementioned works are mainly delay-distortion or rate-distortion optimization algorithms suitable for general wireless networks; it is hard to be directly used in WSNs due to the limited energy rather than bandwidth resource in WSNs. One of our preliminary works proposed in [16] shows the energy-distortion gain by considering multimedia selective encryption in resource allocation.

Selective encryption scrambles the intersegment correlation in the final bitstream, leading to significant potential for encryption-oriented cross-layer optimization. In this paper we systematically formulate energy efficient secure image transmission problem, which is significant different from previous layer-based UEP schemes in literature. The paper is organized as follows. In Section 2, position-based selective encryption is proposed. In Section 3, security aware distortion reduction optimization is proposed with energy constraint. In Section 4, frame-level energy consumption and frame-loss ratio are modeled in details for multirate WSNs. Section 5 shows simulation results. The conclusion is drawn in Section 6. Major symbols in equations and notations are defined in Table 1.

2. SELECTIVE ENCRYPTION OF IMAGE DATA

Positions of significant wavelet coefficients are much more important than the magnitudes of those coefficients. Furthermore, the positions of significant coefficients are determined by the clustering model of insignificant coefficients, which is translated into bitstream structure after compression. To effectively cipher the bitstream structure in the proposed approach, position information is packed into p-segments and magnitude information is packed into v-segments bit-plane by bit-plane. This p-segment and v-segment packing processes in each bit-plane are described as follows. In each embedded bit-plane coding iteration, two coding passes are applied to the coefficient matrix with a given reference threshold to determine the significance of wavelet coefficients. In the dominant pass, a coefficient can be coded as one of the four symbols: positive significance, negative significance, tree root, or isolated zero. All the coded symbols in dominant pass are put to p-segment. If the current coding coefficient is in the highest two resolution levels, the coded symbol is marked as Paramount skeleton (PS). PS symbols contain the root information of wavelet decomposition trees, and Morton scanning assures the continuity of PS residing in each p-segment. The very beginning PS symbols to be encrypted are marked as encrypted processions (EP), where the length of EP in each PS can be flexibly configured by users. Because run-length coding and arithmetic coding propagate any single bit error to the rest of the code stream, EP tightly controls PS and PS controls p-segment. Subordinate pass performs magnitude refinement after dominant pass, where the coded magnitude bits of each significant coefficient are put to v-segment. The reference threshold is decreased by half in each iteration, and EP, PS, p-segment, and v-segment are form bit-plane by bit-plane in an embedded manner. Selective encryption is not applied to v-segments because tree structures are only stored in p-segments. The data flow of proposed selective encryption is shown in Figure 1.

The length of each EP can be scalable from zero to the length of the containing PS, and encryption starts from the most significant bit-plane to the least significant bit-plane. The multiple EP indices in entropy coding table are

Table 1: Major symbol summarization for equations.

Equation Sym	Notations
Δd	Distortion reduction of one image packet
$\varepsilon[\Delta D]$	Image distortion reduction expectation
Bk	Association set of the kth EP block
g	Average segment loss ratio of each p-segment or v-segment
E_{MAX}	Energy budget constraint for transmitting one image
M_{MAX}	Link layer ARQ retry limit
$\overline{M}$	Average number of PDU transmissions
L_{RTS}	RTS frame length
L_{CTS}	CTS frame length
L_{DATA}	DATA frame length
L_{ACK}	ACK frame length
T_o	Link layer time-out value for receiving frames
$\mathrm{BER}_{\mathrm{CTRL}}$	BER of the control frames
BER	Desirable BER of the data frame
R_{CTRL}	Fixed PHY transmission rate for control frames
R_{DATA}	Scalable PHY transmission rate for data frames
P^{RX}	Power required for receiving circuits
$P^{\mathrm{TX}}_{\mathrm{CTRL}}$	Power required for transmitting RTS, CTS, ACK control frames
$P^{\mathrm{TX}}_{\mathrm{DATA}}$	Power required for transmitting DATA frames
Fitness	The fitness evaluation of a chromosome in genetic evolution

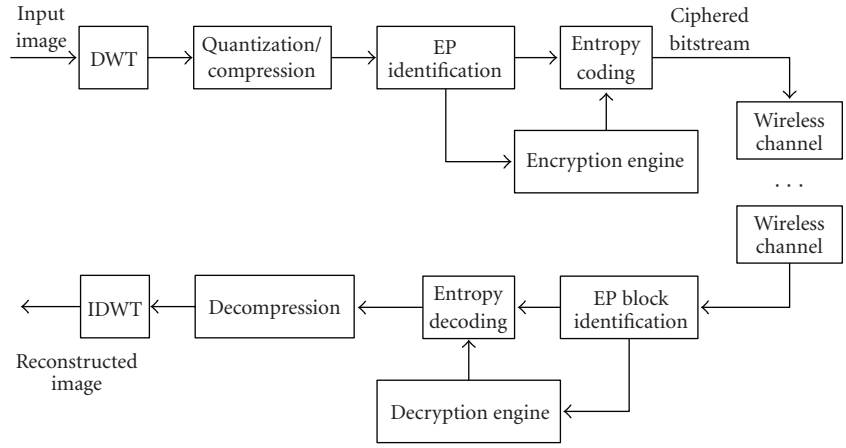

Figure 1: Selective encryption data flow for embedded bitstream.

encrypted and the ciphered code words form the EP blocks which are securely protected. Given the EP length in each p-segment and the encryption block length, one can determine the associated EP blocks of each EP. By this kind of selective encryption, the structure of compressed bitstream is effectively protected. Missing the descriptive information of the structure in p-segments, the magnitude information in v-segments will be placed on totally wrong positions of the wavelet coefficient matrix, which results in chaotic distributions of reconstructed image pixels. The small amount of PS information determines the structure of each p-segment. Modification of PS information scrambles the positions of wavelet coefficients associated with those PS. Strong-block-based robust encryption method, for example, 128-bit advanced encryption standard (AES) [17] applied on EP would make the entire decoding process hardly achievable. Thus, encrypting the tiny amount EP information in each bit-plane can efficiently make the image undecodable without cipher-key. The proposed selective encryption scheme is encryption algorithm independent, and simple low-complexity algorithm such as TEA [18] is applicable. The challenge of key exchange in unsecure networks is effectively solved because the significantly reduced encryption overhead makes the time consuming public-key encryption algorithms such as RSA [19] or ECC [20] algorithms feasible. Finally, image compression codec and entropy coding process in source coding domain can be blind of the existence of selective encryption module, making it format compliant, because p-segments, PS, and EP information are identified directly from the compressed bitstream, and the indices of EP

symbols are encrypted after code book lookup. During decryption processes, original indices of EPs are reconstructed after EP block decryption. Then symbols and their runlengths of EP are determined from entropy code book using those decrypted EP indices. PS are reconstructed with the decrypted EPs. Then p-segments are recreated according to decoded PS information, and v-segments are recreated according to the decoded p-segments bit-plane by bit-plane in a progressive way.

3. CROSS-LAYER OPTIMIZATION PROBLEM FORMULATION

Here we formulate the cross-layer optimization as a distortion reduction maximization (distortion minimization) problem with strict energy budget constraint. The distortion of the reconstructed image and the energy consumption of transmitting this image are both related to the network resource parameters including desirable target BER, link layer ARQ retry limit, and physical layer transmission rate (translated to modulation schemes in this paper). These resources are fine tuned among EP blocks, p-segments, and v-segments.

The final bitstream is composed of a ciphertext stream and a plaintext stream. An example of the final bitstream is shown in Figure 2. Each EP block in the ciphertext stream controls several p-segments in the plaintext stream, and each p-segment in the plaintext stream controls all the p-segments and v-segments further down. Here we define $B_k = \{0, 1, 2, \dots\}$ as the kth EP block set containing the layer number of those encrypted p-segments associated with it. Without the kth EP block, all the p-segments associated with it will be useless for decoding. Referring to the example in Figure 2, $B_0 = \{0, 1\}$ and $B_1 = \{2, 3\}$. This can be formulated as p-segment0, psegment1 are associated with EP block0, while p-segment2 and p-segment3 are associated with EP block1; if EP block0 packet is dropped during transmission, both p-segment0 and p-segment1 cannot make distortion reduction contribution for decoding. Ciphertext stream is transmitted first, because plaintext stream cannot be reconstructed correctly without ciphertext stream. Then zigzag transmission is applied to the plaintext stream starting from p-segment0. Here two choices can be selected as the next transmitted packet after p-segment0: p-segment1 and v-segment0. Because p-segment1 controls all the p-segments as well as v-segments further down the plaintext stream while v-segment0 controls only all the v-segments further down, p-segment1 is transmitted as the next packet, and then v-segment0. The remaining p-segments and v-segments are transmitted in the same way. The bitstream is truncated if a specific p-segment is erased by wireless channel.

The total expected distortion reduction can be expressed in terms of transmissions error rates for each EP block, important p-segment, and unimportant v-segment respectively. Let N be the number of bitstream layers, $\Delta d_p(j)$ and $\Delta d_v(j)$ be the distortion reduction of the p-segment and v-segment in layer j, and g be the corresponding segment loss probability or segment loss ratio (SLR) of one segment packet during transmission. The total expected distortion reduction $\varepsilon[\Delta D]$

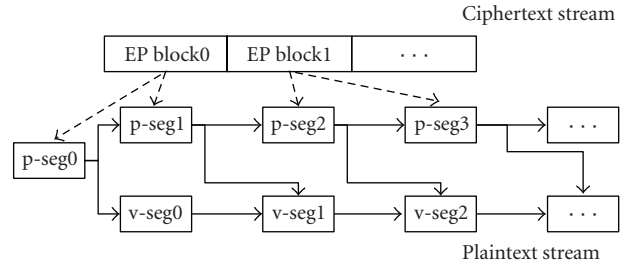

Figure 2: Image codestream format after selective encryption.

of the reconstructed image can be expressed as

$$\begin{aligned}\varepsilon[\Delta D] = \sum_{i=0}^{N-1} \Bigg(\Bigg(\sum_{j=0}^{i} \Delta d_p(j) \Bigg) \cdot g_p(i+1) \\ \cdot \prod_{j=0}^{i} \Bigg((1 - g_p(j)) \cdot \prod_{k \mid j \in B_k} (1 - g_B(k)) \Bigg) \Bigg) \\ + \sum_{j=0}^{N-2} \Bigg(\Bigg(\sum_{j=0}^{i} \Delta d_v(j) \Bigg) \cdot \prod_{j=0}^{i} (1 - g_v(j)) \cdot g_p(i+1) \\ \cdot \prod_{j=0}^{i+1} \Bigg((1 - g_p(j)) \cdot \prod_{k \mid j \in B_k} (1 - g_B(k)) \Bigg) \Bigg).\end{aligned} \tag{1}$$

In (1), each SLR g can be expressed in terms of link layer average packet loss ratio $\overline{\text{PER}}$ and the number of fragmentations $Q : g = 1 - (1 - \overline{\text{PER}})^Q$. Given the average packet loss ratio and distortion reduction measurement of each segment, the total expected distortion reduction can be expressed in close form in terms of desirable BER, ARQ retry limit. Let H denote the length of one segment, let L denote the link layer fragmentation threshold, the number of link layer fragmentations can be straightforwardly expressed as $Q = \lceil H/L \rceil$. Let N_B denote EP block count, let $\overline{E_B}$, $\overline{E_p}$ and $\overline{E_v}$ denote the energy consumption of transmitting one link layer fragment of EP block, p-segment, and v-segment, respectively. Let E_{MAX} denote the energy budget constraint, the overall optimization problem can be formulated as follows: finding the desirable BER, ARQ retry limit, and transmission rate for each EP block, p-segment, and v-segment, respectively, to achieve maximized overall distortion reduction:

$$\left\{ \underset{i \in \{\text{EP}\} \cup \{p\text{-segment}\} \cup \{v\text{-segment}\}}{\text{BER}(i), M_{\text{MAX}}(i), R_{\text{DATA}}(i)} \right\} = \arg\max \{\varepsilon[\Delta D]\}. \tag{2}$$

Subject to the total energy budget constraint E_{MAX},

$$\sum_{i=0}^{N_B-1} Q_B(i) \cdot \overline{E_B}(i) + \sum_{i=0}^{N-1} Q_p(i) \cdot \overline{E_p}(i) + \sum_{i=0}^{N-2} Q_v(i) \cdot \overline{E_v}(i) \le E_{\text{MAX}}. \tag{3}$$

In order to solve the overall optimization problem, we propose a simplified evolution approximation methodology based on genetic algorithm. We assume the channel state changes slowly. Because we use adaptive power control

according to desirable BER value, the transmission rate, and hence, the modulation scheme in physical layer is uncorrelated to the distortion reduction expectation. Thus transmission rate can be optimized independently for minimal energy consumption. Letting all the p-segments use one desirable BER and letting ARQ retry limit pair automatically produces a layer based UEP, because the lengths of bitstream segments are almost nondecreasing through all layers. The desirable BER and ARQ retry limit assignments for v-segments work the same way. Furthermore, the lengths of EP blocks are determined by encryption algorithms, which are usually much shorter than p-segments packets. Thus desirable BER and ARQ retry limit assignments for EP blocks can be performed together with those of p-segments, while reducing solution space for optimization. The solutions of overall optimization are jointly simplified as $\{\mathrm{BER}_p, M_{\mathrm{MAX\_}p}, \mathrm{BER}_v, M_{\mathrm{MAX\_}v}\}$. The complexity of the cross-layer optimization problem is significantly reduced by this approximation. The proposed algorithm is formulated as follows. Note that it can be solved offline and various precalculated result patterns can be stored to lookup tables in sensor nodes.

(a) Initialization for gene binary coding and decoding: each element in the solution matrix $\{\mathrm{BER}_p, M_{\mathrm{MAX\_}p}, \mathrm{BER}_v, M_{\mathrm{MAX\_}v}\}$ is coded as a gene, thus each possible solution is coded as a chromosome.

(b) Set the population space size POP_SIZE and maximal generations G_MAX, and randomly generate the first generation with the specified population size.

(c) Calculate the fitness and perform fitness evaluation of each of each chromosome. Fitness is defined as the expected distortion reduction calculated using the chromosome Fitness $= \varepsilon[\Delta D]$ if the total energy consumption is less than or equals to the energy budget; otherwise the fitness is zero. Sort the chromosomes in descending order according to their fitness values.

(d) Select the elitism of parents in current generation according to the fitness of each chromosome. Denote the fitness of the ith chromosome as Fitness(i) where $0 \le i \le \mathrm{POP\_SIZE} - 1$, then the crossover probability of a chromosome with others is expressed as $p(i) = \mathrm{Fitness}(i) / \sum_{i=0}^{\mathrm{POP\_SIZE}-1} \mathrm{Fitness}(i)$. Start chromosome crossover from the chromosome with the highest probability until a new generation with the same population size is created.

(e) Calculate the number of performed generations. If the number of generations > G_MAX, then go to (f), else go to (c) to refine the next generation population.

(f) Output the best chromosome in the current population with the best fitness. This assures the maximum distortion reduction, while the energy consumption is within the budget constraint.

4. ENERGY MODELING WITH OPTIMAL TRANSMISSION POWER AND RATE

To model the link layer energy consumption and transmission quality, to optimize the transmission rate for minimized energy consumption, link layer transmission overhead should be considered. Both payload data transfer errors and overhead frame such as in RTS, CTS, and ACK loss cause the upper PDU delivery failure. A binary event tree illustrated in Figure 3 can be a good model for link layer frame delivery. Each edge in the tree denotes the probability of a specific frame loss event, and the corresponding leaf node denotes the energy consumption penalty of that event. More details have been presented in [21].

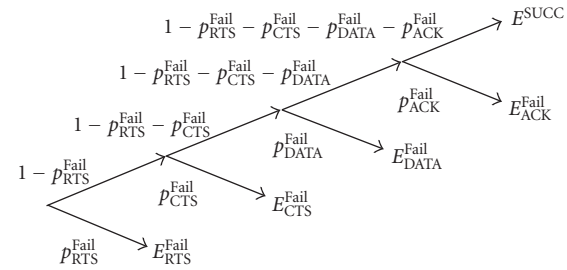

Figure 3: Binary event tree of frame failure and energy cost.

For a single round handshake (without ARQ applied) transmission of an upper layer PDU, the frame error rate (FER) can be expressed as follows, given specific control frame bit error rate $\mathrm{BER}_{\mathrm{CTRL}}$ and desirable bit error rate BER for data frames:

$$\begin{aligned}\mathrm{FER} &= 1 - (1 - \mathrm{BER}_{\mathrm{CTRL}})^{L_{\mathrm{RTS}}} \\ &\quad + (1 - \mathrm{BER}_{\mathrm{CTRL}})^{L_{\mathrm{RTS}}} \cdot (1 - (1 - \mathrm{BER}_{\mathrm{CTRL}})^{L_{\mathrm{CTS}}}) \\ &\quad + (1 - \mathrm{BER}_{\mathrm{CTRL}})^{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}} \cdot (1 - (1 - \mathrm{BER})^{L_{\mathrm{DATA}}}) \\ &\quad + (1 - \mathrm{BER}_{\mathrm{CTRL}})^{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}+L_{\mathrm{ACk}}} \\ &\quad \cdot (1 - (1 - \mathrm{BER}_{\mathrm{CTRL}})^{L_{\mathrm{ACK}}}) \\ &= 1 - (1 - \mathrm{BER})^{L_{\mathrm{DATA}}} \cdot (1 - \mathrm{BER}_{\mathrm{CTRL}})^{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}+L_{\mathrm{ACk}}}.\end{aligned} \tag{4}$$

In this equation $\mathrm{BER}_{\mathrm{CTRL}}$ can be determined according to [22, 23] using the fixed control frame transmission power $P_{\mathrm{CTRL}}^{\mathrm{TX}}$, channel state factor A, noise power density N_0, and control frame transmission rate R_{CTRL}, assuming control frames are transmitted using BPSK modulation with constellation size $b = 1$,

$$P_{\mathrm{CTRL}}^{\mathrm{TX}} = R_{\mathrm{CTRL}} \cdot \frac{N_0}{A} \cdot \left[\mathrm{erfc}^{-1}(2 \cdot \mathrm{BER}_{\mathrm{CTRL}})\right]^2. \tag{5}$$

Also assume data frames are transmitted using scalable QAM-based modulation scheme (constellation size $b > 1$) and power control, the optimized transmission power for data frames is expressed as follows according to [24]:

$$P_{\mathrm{DATA}}^{\mathrm{TX}} = R_{\mathrm{DATA}} \frac{2(2^b - 1)}{3b} \frac{N_0}{A} \left[\mathrm{erfc}^{-1}\left(\frac{(b/2)\mathrm{BER}}{1 - (1/2^{b/2})}\right)\right]^2. \tag{6}$$

The frame error rate is reduced while the number of retransmission is increased if automatic retransmission request (ARQ) is applied. According to [14] the average number of transmissions $\overline{M}$ can be expressed as a nondecreasing

function of link layer ARQ retry limit M_{MAX}:

$$\begin{aligned}\overline{M} &= 1\cdot(1-\mathrm{FER})+2\cdot\mathrm{FER}\cdot(1-\mathrm{FER})\\ &\quad+\cdots+M_{\mathrm{MAX}}\cdot\mathrm{FER}^{M_{\mathrm{MAX}}-1}\cdot(1-\mathrm{FER})\\ &\quad+(M_{\mathrm{MAX}}+1)\cdot\mathrm{FER}^{M_{\mathrm{MAX}}}\\ &=\frac{1-\mathrm{FER}^{M_{\mathrm{MAX}}+1}}{1-\mathrm{FER}}.\end{aligned}\tag{7}$$

Thus the average packet error rate $\overline{\mathrm{PER}}$ provided to upper layer can be approximated as

$$\overline{\mathrm{PER}}=\mathrm{FER}^{(1-\mathrm{FER}^{M_{\mathrm{MAX}}+1})/(1-\mathrm{FER})}.\tag{8}$$

It is clear that the average packet error rate is independent of transmission rate R_{DATA}, thus transmission rate (modulation) optimization can be performed separately from distortion reduction optimization. Let $\overline{E}$ denote the average energy consumption of delivering a PDU with length L_{DATA}, then $\overline{E}$ can be expressed as a function of R_{DATA}. The optimal transmission rate (modulation scheme) can be simply determined by treating $\overline{E}$ as a consecutive function of R_{DATA} and getting the first order derivative $\partial(\overline{E})/\partial(R_{\mathrm{DATA}})$. The discrete transmission rate closest to the zero value first order derivative is selected if there is one R_{DATA} leading to $\partial(\overline{E})/\partial(R_{\mathrm{DATA}})=0$. Otherwise the optimal transmission rate leading to minimal energy consumption must be the highest or the lowest rate depending on the slope of the function $\overline{E}(R_{\mathrm{DATA}})$. According to the binary event tree, the average energy consumption $\overline{E}$ can be expressed as (9) in close form of desirable BER , transmission rate, and ARQ retry limit given channel state information,

$$\begin{aligned}\overline{E}&=\frac{1-\mathrm{FER}^{M_{\mathrm{MAX}}+1}}{1-\mathrm{FER}}\\ &\Bigg(\left(1-\left(1-\mathrm{BER}_{\mathrm{CTRL}}\right)^{L_{\mathrm{RTS}}}\right)\\ &\times\left(P_{\mathrm{CTRL}}^{\mathrm{TX}}\frac{L_{\mathrm{RTS}}}{R_{\mathrm{CTRL}}}+P^{\mathrm{RX}}\left(\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}}{R_{\mathrm{CTRL}}}+2T_o\right)\right)\\ &+\left(1-\mathrm{BER}_{\mathrm{CTRL}}\right)^{L_{\mathrm{RTS}}}\left(1-\left(1-\mathrm{BER}_{\mathrm{CTRL}}\right)^{L_{\mathrm{CTS}}}\right)\\ &\times\left(P_{\mathrm{CTRL}}^{\mathrm{TX}}\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}}{R_{\mathrm{CTRL}}}+P^{\mathrm{RX}}\left(\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}}{R_{\mathrm{CTRL}}}+\frac{L_{\mathrm{DATA}}}{R_{\mathrm{DATA}}}+2T_o\right)\right)\\ &+\left(1-\mathrm{BER}_{\mathrm{CTRL}}\right)^{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}}\left(1-\left(1-\mathrm{BER}\right)^{L_{\mathrm{DATA}}}\right)\\ &\times\left(P_{\mathrm{CTRL}}^{\mathrm{TX}}\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}}{R_{\mathrm{CTRL}}}+P_{\mathrm{DATA}}^{\mathrm{TX}}\frac{L_{\mathrm{DATA}}}{R_{\mathrm{DATA}}}\right.\\ &\left.+P^{\mathrm{RX}}\left(\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}+L_{\mathrm{ACK}}}{R_{\mathrm{CTRL}}}+\frac{L_{\mathrm{DATA}}}{R_{\mathrm{DATA}}}+2T_o\right)\right)\\ &+\left(1-\mathrm{BER}_{\mathrm{CTRL}}\right)^{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}}\left(1-\mathrm{BER}\right)^{L_{\mathrm{DATA}}}\\ &\left(1-\left(1-\mathrm{BER}_{\mathrm{CTRL}}\right)^{L_{\mathrm{ACK}}}\right)\left(P_{\mathrm{CTRL}}^{\mathrm{TX}}\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}+L_{\mathrm{ACK}}}{R_{\mathrm{CTRL}}}+P_{\mathrm{DATA}}^{\mathrm{TX}}\frac{L_{\mathrm{DATA}}}{R_{\mathrm{DATA}}}\right.\\ &\left.+P^{\mathrm{RX}}\left(\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}+L_{\mathrm{ACK}}}{R_{\mathrm{CTRL}}}+\frac{L_{\mathrm{DATA}}}{R_{\mathrm{DATA}}}+T_o\right)\right)+(1-\mathrm{FER})\\ &\times\left(P_{\mathrm{CTRL}}^{\mathrm{TX}}\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}+L_{\mathrm{ACK}}}{R_{\mathrm{CTRL}}}+P_{\mathrm{CTRL}}^{\mathrm{TX}}\frac{L_{\mathrm{DATA}}}{R_{\mathrm{DATA}}}\right.\\ &\left.+P^{\mathrm{RX}}\left(\frac{L_{\mathrm{RTS}}+L_{\mathrm{CTS}}+L_{\mathrm{ACK}}}{R_{\mathrm{CTRL}}}+\frac{L_{\mathrm{DATA}}}{R_{\mathrm{DATA}}}\right)\right)\Bigg).\end{aligned}\tag{9}$$

Up to now the link layer transmission quality in (8) as well as energy consumption in (9) is modeled as close form functions of network resources including desirable BER, transmission rate, and ARQ retry limit. In the cross-layer optimization algorithm proposed in the previous section, the energy consumption and transmission quality of each packet are jointly fine tuned by adjusting the resource allocation. The optimal transmission rate is also determined independently from the cross-layer optimization algorithm.

5. SIMULATION

In this section, the performance of the proposed UEP scheme as well as the proposed position-based selective encryption is evaluated via simulation studies. The performance of transmission rate optimization is also evaluated, showing its significant energy efficiency gain. T-MAC [25] is selected for WSNs medium access, and multirate plug-in presented in [22] is selected for transmission rate optimization. The simulation parameters are stated as follows. Link layer fragmentation threshold is 36 bytes and MAC header is 11 bytes [26]. Control frame length is 13 bytes. Short preamble is applied with the length of 2 bytes [26], and the receive power is 0.01 mW. The noise power density N_0 is 4×10^{-21} J/Hz and the default value of channel state factor A is -100 dB. Frequency bandwidth is 1 MHz and the modulation is scaled by adjusting constellation size b = 1, 2, 4, 6, 8, respectively. Timeout value is set as one-fifth of the RTS transmission time with BPSK modulation. The test image is shown in Figure 4(a) with 64∗64 pixels and 8 bpp. AES standard encryption algorithm is utilized with 128 bits block cipher. The number of EP blocks can be scaled with two p-segments associated to one EP block, starting encryption from the most significant bit-plane (bit-plane 0) to the least significant bit-planes.

Figure 4 shows the original image as well as the decoded images with or without key. The proposed position-based selective encryption scheme is compared with the popular subband selection encryption approach. From these subfigures it is clear that without the correct key for decryption, the qualities of blindly decoded images are very low for both selective encryption schemes. The subband selective encryption renders very coarse images as shown in Figure 4(c) by hiding low-frequency wavelet coefficients, but image information energy concentration may not be directly related to intelligibility. The unprotected wavelet coefficients especially those in middle frequency subbands can still provide significant information for image reconstruction, because the structure of bitstream is unprotected. Unlike subband selection, the position-based selective encryption protects the bitstream structure as well as the positions of wavelet coefficients in all frequency bands. Thus middle- and high-frequency band wavelet coefficients cannot render a blurred image because the positions of those coefficients controlled by bitstream structure are effectively protected.

Figure 5 shows that the position-based selective encryption significantly reduces encryption overhead by reducing the number of encrypted blocks. Subband selection scheme achieves reduced image quality when the number

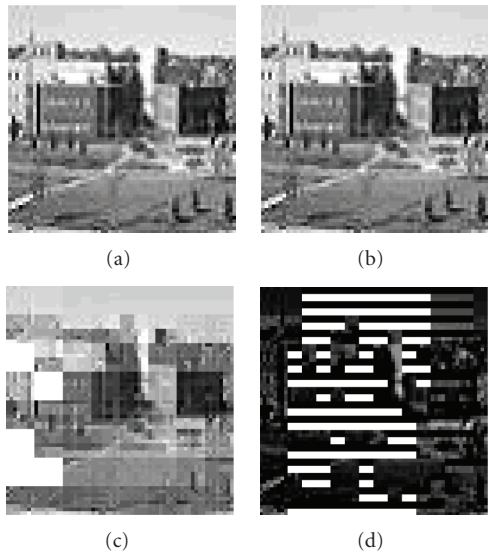

Figure 4: Test image and decoded images. (a) Original "building" image. (b) Correctly decoded image. (c) Blindly decoded image without AES key, for subband selection scheme with 2 blocks of 128-bit AES encryption. (d) Blindly decoded image without AES key, for position-based scheme with 2 blocks of 128-bit AES encryption.

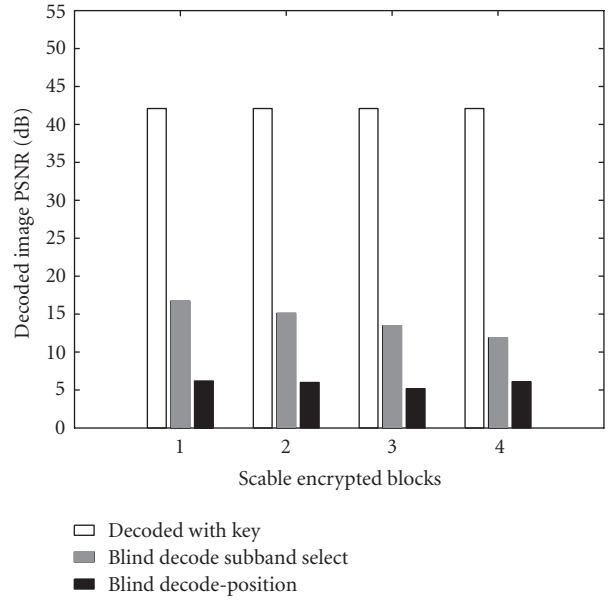

Figure 5: Selective encryption performances. Decoded image quality with different number of encryption blocks for "building" image.

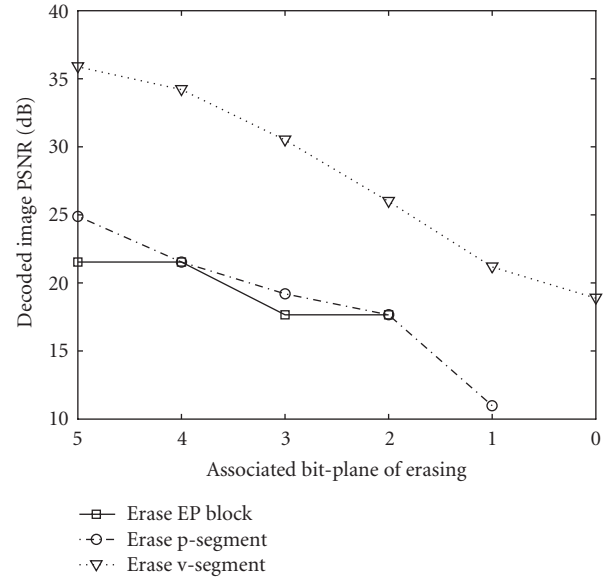

Figure 6: Image quality for "building" with erasing different p-segments, v-segments, or EP blocks in different bit-planes.

of encrypted blocks increases. To achieve acceptable image protection, more blocks need to be encrypted compared with position-based scheme. Again, the reason is due to the distortion reduction contribution of middle and high frequency coefficients. For the position-based selective encryption scheme, the original image is successfully protected even only encrypting one or two blocks of coarser bit-plane EP information. Without the correct EP information in coarser bit-planes, EP information in finer bit-planes can hardly make any contribution for distortion reduction due to wrong positions of significant wavelet coefficients.

The visual effect importance of EP blocks, p-segments, and v-segments for image reconstruction is illustrated in Figure 6, where image qualities with erased EP blocks, p-segments, or v-segments in different bit-planes are shown. The EP blocks contain p-segment structure information, and p-segments contain position information of wavelet coefficients. The magnitude information resides in v-segments. As shown in this figure, EP blocks are more important than p-segments and p-segments are much more important than v-segments. Thus, more robust protection should be applied to EP blocks and p-segments to improve image transmission quality, and less protection can be applied to v-segments to reduce energy consumption.

The energy efficiency gain of transmission rate optimization itself is shown in Figure 7, with different channel state information. Here normalized energy consumption is defined as the energy consumed by transmitting and receiving one bit of pure payload data. The normalized energy cost using optimal transmission rate and modulation scheme is much less than those using nonoptimized ones. For instance, draw a vertical line in Figure 7 at the point where channel state factor is −80 dB, 1.1626e-7 mJ energy is consumed per bit using the worst matched modulation scheme and transmission rate; 0.3265e-7 mJ energy is consumed by transmission using suboptimal matched modulation and transmission rate. However, the optimized transmission rate and modulation scheme achieves only 0.2899e-7 mJ energy consumption for each information bit. In this case, transmission rate and modulation optimization reduces 75% and 11% energy saving than the worst case and suboptimal transmission ones, respectively.

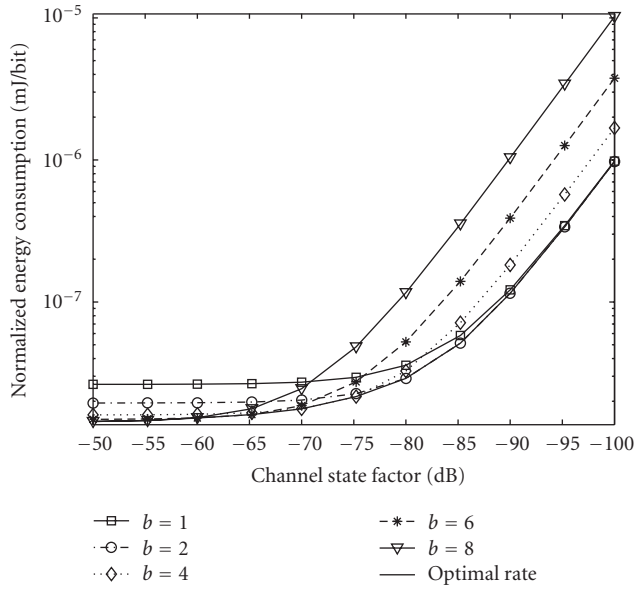

Figure 7: Normalized energy consumption in different channel conditions for different modulation schemes. Link layer fragmentation and payload are both 36 bytes, desirable BER is −50 dB, and retry limit is 3.

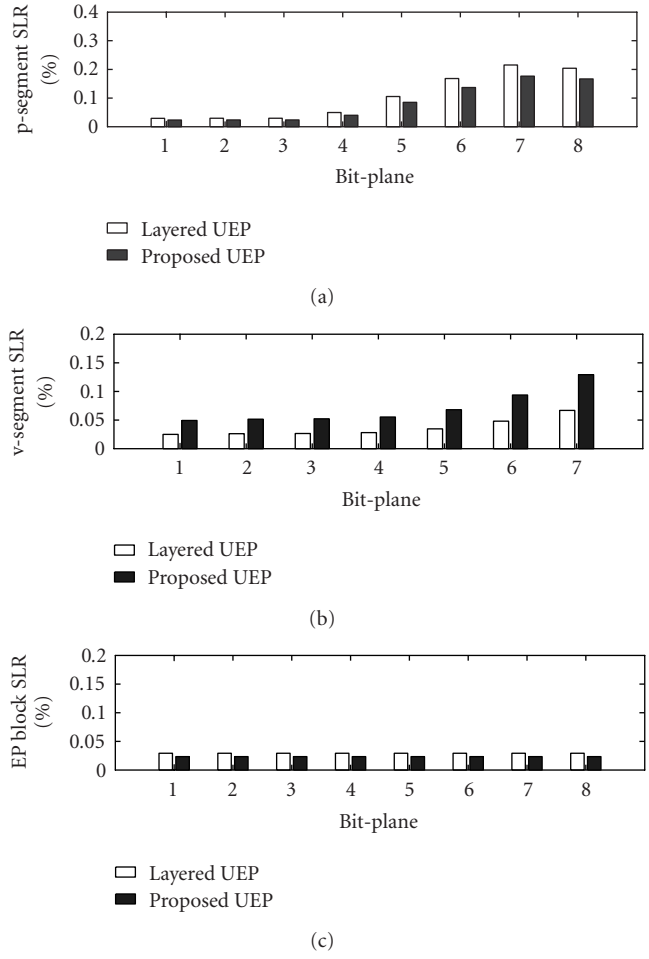

Figure 8: Segment loss ratio (SLR) of EP blocks, p-segments, and v-segments, for the scenario of 0.008 mJ energy budget.

To show the quality-energy improvement of the proposed UEP optimization scheme, the performance is compared with traditional layer based optimal UEP approach. Six scenarios are simulated with energy budget from 0.006 mJ to 0.0085 mJ with 0.0005 mJ granularity. The simulation results show that given the same energy budget, the proposed cross-layer optimal UEP approach enhances the image transmission quality while meeting energy budget requirement. The proposed cross-layer optimization approach fine tunes UEP between EP blocks, p-segments, and v-segments as well as the UEP between different bit-plane layers. The segment loss ratio (SLR) of all EP blocks, p-segments, and v-segments for transmitting the encrypted image with 0.008 mJ energy budget constraint is shown in Figure 8. SLR is directly related to the PER of each packet of that segment, which is in turn related to desirable BER and ARQ retry limit allocation of each packet. Compared with layered UEP, the SLRs of encrypted EP blocks and important p-segments are reduced while the SLRs of unimportant v-segments are increased. This is because the proposed UEP allocates more resources to EP blocks and p-segments and less resources to v-segments. The distortion reduction is increased due to more efficient resource allocation.

In the proposed novel UEP method, we have optimized the image quality and confined the energy consumption given the resource budget requirement. The image quality and energy consumption performance is shown in Figure 9. The vertical axis represents the distortion reduction expectation value while the horizontal axis is the corresponding communication energy cost. This figure demonstrates that the proposed cross-layer optimization scheme achieves enhanced image quality in comparison with the traditional layered UEP. At the same time, the proposed UEP can fine turn the network resource allocation, leading to higher energy efficiency under strict resource budget constraints.

6. CONCLUSION

This paper proposed a novel cross-layer UEP optimization approach for wireless image data delivery in sensor networks. Not only does it achieve high-energy efficiency but also image security is protected through creative image data encryption method. The proposed image encryption scenario fits well in the UEP approach resulting in enhancements for both image transmission quality and communication energy efficiency. In our approach, the communication energy efficiency is assured while image quality is optimized by specifically protecting encrypted blocks. A new position-based selective encryption scheme is developed that has very low-computation overhead and is appropriate for this original UEP optimization framework. The security aware cross-layer optimization approach has achieved maximal image transmission quality in wireless channels even though the energy budget constraints are met. Simulation results have demonstrated up to 5 dB image transmission quality improvement

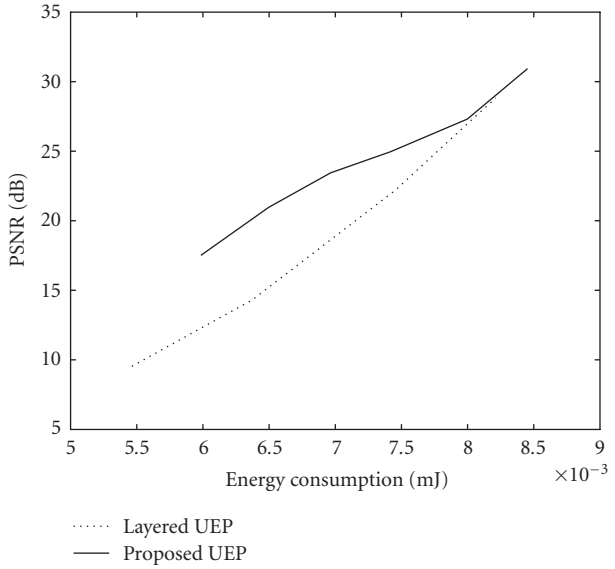

Figure 9: Image quality with different energy consumption.

for energy efficiently transmitting these robustly encrypted image data.

ACKNOWLEDGMENT

This research project was partially supported by the Nebraska Research Initiative grant.

REFERENCES

[1] T. Lookabaugh and D. C. Sicker, "Selective encryption for consumer applications," *IEEE Communications Magazine*, vol. 42, no. 5, pp. 124–129, 2004.

[2] W. Yu, Z. Sahinoglu, and A. Vetro, "Energy efficient JPEG 2000 image transmission over wireless sensor networks," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '04)*, vol. 5, pp. 2738–2743, Dallas, Tex, USA, November-December 2004.

[3] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3445–3462, 1993.

[4] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 6, no. 3, pp. 243–250, 1996.

[5] D. Taubman, "High performance scalable image compression with EBCOT," *IEEE Transactions on Image Processing*, vol. 9, no. 7, pp. 1158–1170, 2000.

[6] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 118–129, 2003.

[7] M. S. Kankanhalli and T. T. Guan, "Compressed-domain scrambler/descrambler for digital video," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 2, pp. 356–365, 2002.

[8] C.-P. Wu and C.-C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia*, vol. 7, no. 5, pp. 828–839, 2005.

[9] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," in *Proceedings of the 4th ACM International Conference on Multimedia (MULTIMEDIA '96)*, pp. 219–229, Boston, Mass, USA, November 1996.

[10] M. Grangetto, E. Magli, and G. Olmo, "Multimedia selective encryption by means of randomized arithmetic coding," *IEEE Transactions on Multimedia*, vol. 8, no. 5, pp. 905–917, 2006.

[11] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[12] Z. Wu, A. Bilgin, and M. W. Marcellin, "Joint source/channel coding for multiple images," *IEEE Transactions on Communications*, vol. 53, no. 10, pp. 1648–1654, 2005.

[13] R. Hamzaoui, V. Stanković, and Z. Xiong, "Optimized error protection of scalable image bit streams," *IEEE Signal Processing Magazine*, vol. 22, no. 6, pp. 91–107, 2005.

[14] Q. Li and M. van der Schaar, "Providing adaptive QoS to layered video over wireless local area networks through real-time retry limit adaptation," *IEEE Transactions on Multimedia*, vol. 6, no. 2, pp. 278–290, 2004.

[15] M. van der Schaar and D. S. Turaga, "Cross-layer packetization and retransmission strategies for delay-sensitive wireless multimedia transmission," *IEEE Transactions on Multimedia*, vol. 9, no. 1, pp. 185–197, 2007.

[16] W. Wang, D. Peng, H. Wang, and H. Sharif, "A cross layer resource allocation scheme for secure image delivery in wireless sensor networks," in *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC '07)*, pp. 152–157, Honolulu, Hawaii, USA, August 2007.

[17] National Institute for Standard Technology (NIST), "Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES)," Washington, DC, USA, 2001.

[18] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Proceedings of the 2nd International Workshop on Fast Software Encryption (FSE '94)*, vol. 1008 of *Lecture Notes in Computer Science*, pp. 363–366, Springer, Leuven, Belgium, December 1994.

[19] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, "Section 31.7: the RSA public-key cryptosystem," in *Introduction to Algorithms*, pp. 881–887, MIT Press and McGraw-Hill, Boston, Mass, USA, 2nd edition, 2001.

[20] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 62–67, 2004.

[21] W. Wang, D. Peng, H. Wang, H. Sharif, and H. H. Chen, "Optimal image component transmissions in multirate wireless sensor networks," in *Proceedings of the 50th Annual IEEE Global Communications Conference (GLOBECOM '07)*, Washington, DC, USA, November 2007.

[22] C. Schurgers, O. Aberthorne, and M. B. Srivastava, "Modulation scaling for energy aware communication systems," in *Proceedings of the International Symposium on Low Power Electronics and Design (ISLPED '01)*, pp. 96–99, Huntington Beach, Calif, USA, August 2001.

[23] S. Haykin, *Communication System*, John Wiley & Sons, New York, NY, USA, 3rd edition, 1994.

[24] W. Stallings, *Data and Computer Communications*, Prentice Hall, Upper Saddle River, NJ, USA, 7th edition, 2000.

[25] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 171–180, Los Angeles, Calif, USA, November 2003.

[26] http://tinyos.cvs.sourceforge.net/*checkout*/tinyos/tinyos-1.x/contrib/t-mac/tos/system/TMACMsg.h?revision=1.2.