Fall 12-3-2009

QUALITY-DRIVEN CROSS LAYER DESIGN FOR MULTIMEDIA SECURITY OVER RESOURCE CONSTRAINED WIRELESS SENSOR NETWORKS

Wei Wang
University of Nebraska at Lincoln, weiwang@huskers.unl.edu

QUALITY-DRIVEN CROSS LAYER DESIGN FOR MULTIMEDIA SECURITY OVER RESOURCE CONSTRAINED WIRELESS SENSOR NETWORKS

By

Wei Wang

A DISSERTATION

Presented to the Faculty of
The Graduate College at the University of Nebraska
In Partial Fulfillment of the Requirements
For the Degree of Doctor of Philosophy

Major: Engineering

Under the Supervision of Professors Hamid Sharif and Dongming Peng

Lincoln, Nebraska

December 2009

QUALITY-DRIVEN CROSS LAYER DESIGN FOR MULTIMEDIA SECURITY OVER RESOURCE CONSTRAINED WIRELESS SENSOR NETWORKS

Wei Wang, Ph.D.

University of Nebraska, 2009

Advisors: Hamid Sharif, Dongming Peng

The strong need for security guarantee, e.g., integrity and authenticity, as well as privacy and confidentiality in wireless multimedia services has driven the development of an emerging research area in low cost Wireless Multimedia Sensor Networks (WMSNs). Unfortunately, those conventional encryption and authentication techniques cannot be applied directly to WMSNs due to inborn challenges such as extremely limited energy, computing and bandwidth resources. This dissertation provides a quality-driven security design and resource allocation framework for WMSNs. The contribution of this dissertation bridges the inter-disciplinary research gap between high layer multimedia signal processing and low layer computer networking. It formulates the generic problem of quality-driven multimedia resource allocation in WMSNs and proposes a cross layer solution. The fundamental methodologies of multimedia selective encryption and stream authentication, and their application to digital image or video compression standards are presented. New multimedia selective encryption and stream authentication schemes are proposed at application layer, which significantly reduces encryption/authentication complexity. In addition, network resource allocation methodologies at low layers are extensively studied. An unequal error protection-based network resource allocation scheme is proposed to achieve the best effort media quality with integrity and energy

efficiency guarantee. Performance evaluation results show that this cross layer framework achieves considerable energy-quality-security gain by jointly designing multimedia selective encryption/multimedia stream authentication and communication resource allocation.

DEDICATION

I dedicate this dissertation to my parents Qunxiang Wang, Yuhui Wang, and my PhD advisory committee.

ACKNOWLEDGEMENT

First of all, I would like to show my sincerely appreciation to my PhD advisor, Prof. Hamid Sharif, for his guidance and contribution along my academic path toward the PhD degree. My dissertation work would not have been possible without his enlightenment in the research of wireless networks, insight in achieving scholastic success, leadership of pioneering educational activities, advice of academic righteousness and strong and generous support in various situations. Prof. Sharif gave me the key to the treasury of knowledge and showed me the route to overcome the academic challenges. I can still remember the numerous field tests with him in both summer hot sun shine and winter cold winds, where his professional ethic set up an ideal example for my future academic career to follow. I would also like to thank Prof. Sharif for his strong support in my faculty job search. He took his time out of his busy schedule and helped me prepare reference letters as well as responded to time-consuming reference checks. My faculty job search would not have been possible without his strong support. In the meanwhile, I sincerely appreciate the family environment that Prof. Sharif created in our research groups, which made me emotionally comfortable when I am so far from my parents in China. I am so grateful for the feeling that I am part of his big family in U.S., which is the psychologically safe harbor I can always count on. I am extremely proud and I feel ecstatically lucky to be the PhD student under the supervision of Prof. Sharif.

I sincerely thank my PhD study co-advisor, Prof. Dongming Peng, for his insightful enlightenment in bringing me to the signal processing research community. My dissertation research would not have been possible without his creative guidance and advice in the area of wireless multimedia sensor networks. Under the effective supervision of Prof. Peng together with Prof. Sharif, my research has always been on the right track and productive: I had 5 journals articles, 2 book chapters and many conference papers published and got the best paper award in IEEE WCNC 2008. I sincerely appreciate that Prof. Peng taught me how to perform research work by being both creative and down to earth. I can still remember the days, nights and weekends we were working together on discussing the ideas, deriving the equations, and debugging in the WiseCOM labs for demos. Also as a Chinese professor, he gave me so much valuable advice in both academia faculty job search and life guidance as an international PhD student. I sincerely thank Prof. Peng, and I feel so lucky that he is my co-advisor in my PhD study.

I would like to honestly thank Prof. Yaoqing Yang for his guidance and support in my PhD study. He opened the research window of Multiple-Input-Multiple-Output (MIMO) and Space-Time Coding (STC) to me, enlightening me and bringing me into the fantastic areas of MIMO wireless communication. From his class, I learned both advanced communication technologies and rigid research methodologies, and published a research article in IEEE Globecom conference, which laid important foundation for my future research in cooperative wireless communication. I also thank Prof. Yang for his strong support in my faculty job search process, taking care of the reference letter uploading and reference checks. I feel excited and grateful to get all the support from him in my PhD study.

I would like to show me sincere appreciation to Prof. Zhenyuan Wang, for his advice and support in my PhD study. Prof. Wang opened me the window of mathematical optimization and brought me to a higher level understanding of the systematic optimality. Through his class I learned both advanced mathematical theories and rigid thinking and reasoning methodologies, which is much helpful for my research. I would also like to thank Prof. Wang for his kindness and consideration in my life of studying abroad, and I cherish the memory of those Chinese holidays we gathered at his house. I sincerely thank Prof. Wang for his kindness and support in my PhD study.

I would also like to sincerely thank Prof. Jitender Deogun for his kindly support and encouragement in my PhD dissertation process. He took his valuable time from his busy schedule to review my dissertation and discuss the research merit with me. Prof. Deogun’s nice manner and strong encouragement on my research extremely boosted my confidence in my dissertation research as well as my future academic career. I sincerely thank Prof. Deogun’s support and I feel so happy that he is in my PhD study committee.

I would also like to thank Dr. Michael Hempel, for his help and support in my research works. His strong research insight, problem solving skills, project management capabilities, and computer programming expertise all impressed me and set up a good example for me to learn. I enjoy the working experience with him in the WiseCOM lab demo debugging and open house activities, as well as numerous wireless field tests. I sincerely thank Dr. Hempel, and I cherish the memory of working with him these years.

I also want to thank other faculty in our departments and the collaborative organizations. I especially thank Prof. Hsiao-Hwa Chen for his generous academic support and advice in publishing high quality research articles these years. I sincerely thank Prof. Jong-Hoon Youn for his enlightening education in wireless sensor networks, as well as his strong support in my faculty job search. I would also like to thank all the members in our research groups, for the research discussion and friendly environment.

Finally, I dedicate this dissertation to my parents, Qunxiang Wang and Yuhui Wang in China. Although I am so far from them that I cannot take the responsibility of taking care of them as a good son, their unique emotional support and indispensable psychological encouragement are the crucial components leading to every single step of my achievements. I faithful thank my parents for their support in my dissertation research these years.

GRANT INFORMATION

This dissertation research was supported in part by U.S. National Science Foundation grant No. 0707944 for wireless sensor networks research.

TABLE OF CONTENT

LIST OF FIGURES

Chapter 1. Introduction

1.1 Motivation

Content-secure and error robust multimedia applications (e.g., battlefield assistance, disaster relief, telemedicine) have become increasingly popular in energy-constrained Wireless Multimedia Sensor Networks (WMSNs), where content security, multimedia quality and energy efficiency are all critical factors. However, multimedia security (i.e., privacy or confidentiality, achieved by encryption, and integrity or authenticity, achieved by authentication) in wireless sensor networks (WSNs) has formidable research challenges. These challenges include extremely limited power due to battery cell limitations, low computational power and memory due to hardware size and cost, and limited bandwidth resources due to low cost radio transceivers. Because of these challenges, WMSNs can only provide limited Quality of Service (QoS) and security guarantees for multimedia streams transmitted in the wireless channel. The open wireless environment in a WMSN is extremely vulnerable to malicious attacks, including packet interception and injection, traffic eavesdropping, and semantic content modification. In addition, multimedia streaming is usually bulky and content sensitive, while the encryption/decryption and signing/verification operations are extremely slow due to computational complexity. Therefore, providing low cost yet effective security in WMSNs is very challenging. Finally, in error-prone wireless channels, bit errors and packet losses are inevitable due to environmental or thermal noise and ambient interference or collisions that may significantly impact end-to-end multimedia service quality. All of these limitations pose significant challenges in high layer encryption/authentication strategy design and optimization of cross layer network protocol scheduling. In this dissertation, we focus on providing energy-efficient multimedia privacy/integrity while enhancing multimedia quality in WMSNs.

1.2 Contribution

This dissertation addresses inherent problems with providing energy efficient digital multimedia delivery with security guarantees and best-effort quality services. The contribution of the research presented in this dissertation is two-fold.

First, simple but effective selective encryption and stream authentication schemes for digital multimedia are proposed to provide overhead-reduced encryption results and non-ambiguous verification outcomes. The extra authentication overhead is minimized and the encryption workload is significantly reduced in the proposed greedy authentication and position-based selective encryption schemes.

In addition, a new security-aware cross layer resource allocation scheme is proposed to provide best-effort media quality with energy consumption budget constraints. A novel link layer energy-distortion model is also proposed in the network resource allocation strategy design to abstract the synoptic bridge between resource allocation and low layer network protocol control parameters such as multi-rate transmission, power control, and fragmentation and retransmission control. The link layer energy-distortion model also significantly simplifies the network resource allocation design. The joint consideration of digital media security provision and network resource allocation in WMSNs is also highlighted in this dissertation.

1.3 Organization of the Dissertation

The organization of this dissertation is as follows. In Chapter 2, we give an overview of secure multimedia streaming in energy resource-constrained wireless sensor networks, and formulate the quality-driven secure resource allocation in a cross layer fashion. In Chapter 3, we perform a literature review and discuss existing work in multimedia stream authentication, selective encryption and wireless multimedia cross layer resource allocation. In Chapter 4, we present a traffic partitioning strategy to separate important position information from unimportant value information in multimedia. In Chapter 5, we discuss a proposed cross layer resource allocation framework to achieve media quality and energy efficiency simultaneously by means of Unequal Error Protection (UEP). In Chapter 6, we propose a new position-based multimedia selective encryption scheme to reduce encryption overhead, and present a joint encryption-resource allocation framework for privacy protection in WMSNs. In Chapter 7, we discuss the application of stream level authentication to scalable multimedia streaming, and propose heuristic authentication simplification to reduce complexity. In Chapter 8, we analyze the results and discuss the performance of the proposed cross layer secure resource allocation framework. Finally, we give our conclusions in Chapter 9.

Chapter 2. Problem Formulation of Cross layer Design for Secure Multimedia in Wireless Sensor Networks

Recently, advanced multimedia (e.g., digital image, video) coding technologies have been proposed to deal with challenges resulting from bandwidth intensive but loss-tolerant multimedia streaming over packet-erasing wireless networks and energy-limited sensor networks. In wireless sensor networks with low cost wireless sensor nodes, the energy, computational and communication resources are extremely constrained due to the limitations of the hardware size and radio transceivers. These constraints require very efficient communication protocol optimization and effective encryption/authentication algorithm design.

In this research, we primarily study low cost selective encryption, error-robust stream authentication, and unequal network resource allocation algorithms in WMSNs. We propose a quality-driven energy efficient resource allocation framework suitable for transmitting security protected multimedia streams. The research has three independent objectives and two major components, which are discussed in detail below.

2.1 Research Objectives

Multimedia Content Security. Multimedia content security has become a critical issue in trustworthy computing, especially in a wireless environment where malicious packet interception, packet injection and content modification are inevitable. The semantic meaning of multimedia streaming must be hidden with secret ciphers (e.g., [96]-[100]), and secret data must be embedded in the content level (e.g., watermarking [42]-[45]) or attached in the packet level (e.g., stream authentication [1]-[11]) to achieve content secrecy/integrity.

Multimedia Quality. Multimedia data is traffic intensive but loss tolerant. This feature provides a significant foundation from which to design efficient multimedia transmission systems in wireless networks. In a digital image or a Group of Pictures (GOP) in video, some packets are more important than other packets. The decoding of some packets may rely on the successful decoding of some other packets. These features of unequal perceptional importance and codec dependency must be considered to achieve desirable multimedia quality.

Energy and Communication Resource Efficiency. The energy and bandwidth resources are extremely limited in low cost WMSNs due to the limited battery cell size and simple radio transceivers in each sensor node. Transmission parameters such as data rate and power in the physical (PHY) layer, and fragmentation and retransmission limits in the Media Access Control (MAC) layer, can be adaptively controlled to maximize energy efficiency performance [40] [41] [52]. Network resource allocation by means of such parameter adjustment can achieve significant energy and communication resource efficiency by adapting the transmission parameters to the time-varying wireless channel conditions.

2.2 Research Components

Study efficient digital media encryption/authentication algorithms and explore the design spaces for both multimedia compression and security provision. The most advanced image compression standards (such as the DCT based JPEG [46], wavelet-based JPEG2000 [49], zero tree coding [47] [48], and position-value enhancement [50] [51]) will be investigated in detail to uniformly extract “the most important parts,” in conjunction with the most advanced encryption and authentication standards e.g., Advanced Encryption Standard (AES), Eclipse Curve Cryptography (ECC), Digital Signature Algorithm (DSA) [53] [54], and Secure Hash Algorithm (SHA) [55] [56]. This is from a top-down view of the system, where the selective encryption and stream authentication assumes the existence of underlying network resource allocation and may achieve improved service quality and reduced communication complexity.

Propose and evaluate a new security-oriented resource allocation algorithm for secure media streaming over wireless sensor networks. Different physical layer resource allocation strategies (e.g., power control, interference cancellation, channel allocation and selection, Forward Error Correction (FEC) selection, modulation scaling and rate adaptation) link layer fragmentation and packing, access control, bandwidth and timeslot scheduling, Automatic Retransmission reQuest (ARQ) control and Hybrid-ARQ control; as well as network layer routing selection, traffic distribution, etc [12]-[41] [57] [58]) in combination with different stream authentication algorithms will be considered and studied. This is from the bottom-up view of the system. The stream authentication introduces extra rate (or size) overhead and selective encryption introduces extra decoding dependency overhead, leading to new network resource allocation challenges. The energy and communication resources must be allocated with regard to data urgency and decoding dependency, the perceptional importance of each packet, and the wireless channel conditions.

2.3 Generic Problem Formulation

In secure WMSNs, multimedia stream is compressed, encrypted and signed and finally transmitted in wireless channels. Figure 2.1 shows an example of such secure media streaming scenario in WMSNs. Although we use JPEG2000 digital image compression standard as an illustrative example in this figure, the theory and methodology of error resilient multimedia encryption/authentication and energy efficient network resource allocation is general, which can be seamlessly extended to other multimedia compression techniques such as zero tree codec, Position-Value (P-V) partition, and scalable video coding. We also focus our study on a single secure media flow delivery on one hop wireless link, which can be easily extended to multi-hop secure delivery by establishing end-to-end latency and energy requirements.

The digital images or picture sequences captured from the camera are first processed by tile forming. The tiled image then undergoes the Discrete Wavelet Transform (DWT, or DCT in JPEG codec) process and code block forming process. Tier-1 and tier-2 coding processes are applied to form packets and layers. Then the selective encryption or stream authentication is applied to the compressed multimedia code stream. Finally, the secret code stream is transmitted in the WMSN with resource allocation applied. At the receiver side, the received packets are verified according to the crypto-hash as well as the signature, decrypted with the secret key, and decoded in the tier-1 and tier-2 decoding processes. After Inverse Discrete Wavelet Transform (IDWT), the image/picture is eventually reconstructed from the verified, decrypted and received packets. In terms of authentication, we follow the definition of non-ambiguously authenticated image in [1] [2], where the image is reconstructed exclusively from the packets received, decoded and verified at the receiver.

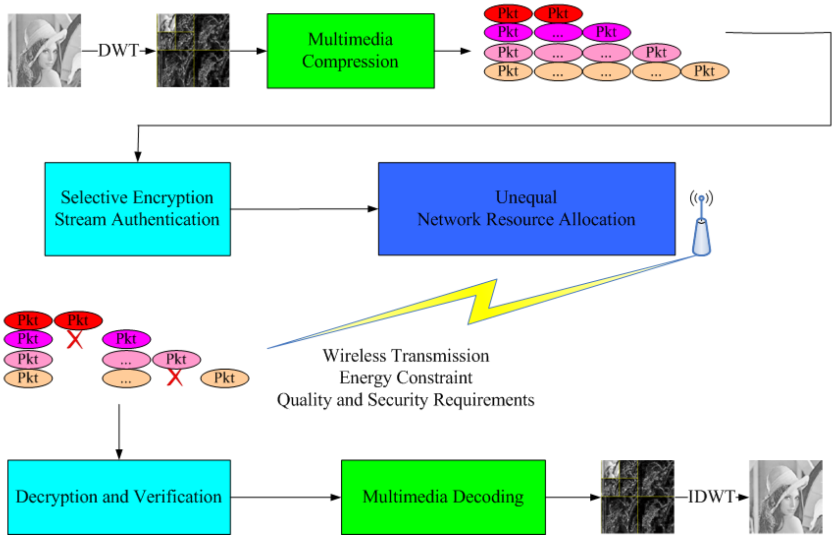

DWT
Multimedia Compression
Pkt
...
Selective Encryption Stream Authentication
Unequal Network Resource Allocation
Wireless Transmission
Energy Constraint
Quality and Security Requirements
Decryption and Verification
Multimedia Decoding
IDWT

Figure 2.1 An illustrative example of secure multimedia streaming in a WMSN

The goal of secure image transmission in WMSNs is to maximize the expected total distortion reduction (i.e., maximize the quality, or minimize the total distortion) of the reconstructed, decrypted and verified image by jointly allocating high layer security resource and scheduling network transmission strategies such as physical layer transmission data rate (achieved by modulation scaling), physical layer power level, and link layer retransmission limit. Let $\varepsilon[\bullet]$ denote the mathematical expectation operation; ΔD denote the total distortion reduction of the image after packet reception, decryption and verification; a denote the application layer security solution in terms of selective encryption and stream authentication; r denote the physical layer transmission data rate; P_t denote the physical layer transmission power; and $m_{\max}$ denote the link layer retransmission limit. Also let L denote the total number of layers in the compressed image code stream, l denote the index of the packet in each layer, and N_l denote the number of packets in layer l. Let E_{tot} denote the total energy consumption of transmitting all the packets in the image, and $E_{\max}$ denote the energy budget constraint. The generic quality-driven secure media transmission problem in WMSNs can be formulated as [3] [60]:

$$\{a_{l,i}, r_{l,i}, m_{\max_{l,i}}, P_{t_{l,i}}\}_{l\in\{0,1\ldots L-1\}, i\in\{0,1\ldots N_l-1\}} = \arg\max\{\varepsilon[\Delta D]\} \tag{2.1}$$

Subject to the total energy budget constraint:

$$E_{tot} \le E_{\max} \tag{2.2}$$

Because of the dual effect of decoding and verification dependency, an image packet must be received, decodable and verifiable to make distortion reduction contribution to the reconstructed image. Furthermore, because the packets in the compressed code stream have unequal perceptional importance and the wireless channel has a time-varying nature, authentication crypto-hash link assignment and network resource allocation need to be adjusted accordingly to achieve an optimal energy-quality performance. Finally, the network resource allocation should also consider the encryption effect since multimedia selective encryption can scramble and change the stream dependency. Thus it is clear that the problem is formulated in a cross layer fashion involving the application, link and physical layers. In later chapters of this dissertation, we will analyze this cross layer problem and propose a solution to this problem.

2.4 Summary

In this chapter we gave an overview of resource-constrained cross layer design for secure multimedia transmission in WMSNs. We summarized the three independent research objectives (media quality, security, and communication energy efficiency) and two major research components (encryption/authentication, and network resource allocation). The energy-constrained secure multimedia transmission problem in WMSNs was further generically formulated in a cross layer fashion as a quality maximization problem with energy constraint and security considerations.

Chapter 3. Literature Review and Related Works

In this dissertation, we focus our research on quality-driven multimedia security design and cross layer delivery optimization in WMSNs. We start our literature review from generic multimedia stream authentication without consideration of network resource allocation. In parallel we approach the literature review on the other side of security--encryption--and focus on the review of modern multimedia selective encryption schemes. Then we review state-of-the-art quality-driven cross layer network resource allocation schemes in generic wireless networks. Finally we survey energy-efficient design strategies in sensor networks, especially multi-rate energy efficient transmission schemes. By extensively reviewing related research, we point out the significant differences in the proposed methodologies presented in this dissertation and highlight our contribution.

3.1 Multimedia Stream Authentication

In terms of authentication, conventional binary data authentication schemes, regardless of multimedia content, can only provide data integrity in a strict sense. But these schemes are not desirable to secure WMSNs because simple bit-flips due to wireless channel errors may not change the semantic meaning of multimedia content [1] [2]. For example, a picture is still readable if a couple of unimportant packets are dropped because of the loss-tolerant feature of multimedia streaming. On the other hand, traditional watermark-based multimedia authentication schemes targeted at semantic content verification are robust against transmission bit errors and packet drops as well as compression. However, embedding security data bits (e.g., key-based pseudo random streams) in the middle frequency band coefficients (e.g., wavelet coefficients) is counter to Unequal Error Protection- (UEP) based wireless network resource allocation concepts [3]. In UEP-based network resource allocation schemes, the important packets containing low frequency wavelet coefficients and the middle frequency embedded data are both critical to the decoding and verification of the original image, leading to extra energy consumption overhead for WMSN transmission.

Stream authentication [1] [2] [3] is a desirable candidate for WMSN integrity provisions for the following reasons. First, packet authentication schemes applied in stream level after image/video compression can be adaptively designed to cope with time-varying wireless channel conditions, showing considerable advantage over traditional content-level watermarking applied to Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) coefficients before compression. Secondly, stream level authentication can offer verification results without ambiguity by directly allocating one-way hashing or signature on each packet; thus, each packet is determined as authentic/consumed or faked/discarded [4] [5] [6]. On the other hand, a decision threshold has to be defined in content-based watermarking authentication to verify the media authenticity. A high False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the common results of a non-optimized decision threshold. Finally, stream authentication algorithms and UEP-based transmission scheduling can be jointly designed to provide more efficient network resource allocation. The important packets with higher distortion reduction contribution, and, at the same time, more dependent children packets receive more authentication hash tag allocation and delivery protection. Thus, the multimedia quality optimization and multimedia authentication problems can be solved jointly within pre-defined energy budget constraints.

The joint optimization of quality-driven multimedia authentication and energy efficiency in WMSNs is a new research area, and very few research studies on this topic have been reported in literature. Sun [1] provoked and motivated the idea of designing multimedia stream authentication with quality consideration by utilizing the unequal importance feature of different image/video packets in the compressed bit stream. The quality of authenticated image or video stream rather than authentication probability was optimized by designing an acyclic authentication graph and allocating authentication resources with regard to packet distortion importance. Li [2] proposed a new concept called Unequal Authentication Allocation (UAP), in which the source/channel coding rates and total authentication bit budgets in the compressed and secure image streams are unequally allocated. In the UAP approach, the verification probability rather than the authenticated media quality over all the packets in the multimedia stream was optimized with regard to the overall authentication bit budget. Although this UAP concept explored the unequal importance of packet distortion reduction in stream authentication process, this unique characteristic and the inter-packet dependency were not utilized in low layer communication protection. Zhang [4] proposed a content-aware stream authentication scheme to optimize authenticated image quality with specific consideration of the JPEG2000 image compression standard in packet-erasing channels. An Acyclic Graph (AG) for stream authentication was also computed and optimized to trade off the total authenticated image distortion and the authentication crypto-hash tag allocation overhead according to channel characteristics (e.g., packet loss probability) and application characteristics (e.g., packet visual importance). A Rate-Distortion Optimization (RaDiO) framework with stream authentication consideration was proposed in the research [5] for secure H.264 video transmission. In this approach, a video frame transmission scheduler was devised to minimize the expected visual distortion after decoding and verification of each frame subject to the total rate budget constraints. Secure and robust digital signature schemes were also proposed in [6] and [7] for quantitative verification of image and video streaming, respectively. Other similar research studies on error robust multimedia stream authentication were found in [8] [9] [10] and [11].

However, all of these aforementioned stream authentication schemes cannot be directly applied to WMSNs for several reasons. First, although the energy constraint is critical in cross layer transmission optimization in WMSNs, it was not considered in these schemes. The rate-distortion optimization may not necessarily lead to energy-distortion optimization. Furthermore, UEP-based cross layer network resource allocation was not considered in most of these approaches. Resource allocation was confined to authentication bit allocation in the application layer only; thus, the design space of joint authentication and network resource allocation was significantly constrained. This leaded to relatively limited energy-quality performance gain. In this dissertation, we propose a new quality-driven resource management framework specifically for WMSNs to optimize the authenticated image quality, subject to total energy consumption constraints and with regard to wireless channel conditions. In the proposed approach, we consider not only the stream authentication AG design in the application layer, but also the network resource allocation strategy in the low layers of the WMSN protocol stack, which is significantly different from previous studies found in literature.

3.2 Multimedia Selective Encryption

In terms of encryption, traditional binary encryption approaches are not suitable for wireless multimedia transmission. Multimedia application is traffic-intensive and contains a lot of data bits, while the encryption/decryption algorithms are extremely slow due to high computational complexity. Thus, it is impractical to encrypt all the data bits in the multimedia stream due to high computational overhead and real-time media stream requirements. To reduce multimedia encryption overhead, many popular multimedia selective encryption approaches have been proposed to select the most important coefficients from either the transform domain or the compression domain. Other research proposes to use secret entropy coding to achieve multimedia security. Generally, the first category is referred to as selective encryption and the second category is referred to as joint compression/encryption.

Multimedia selective encryption [96] – [104] has been recently proposed to reduce the encryption and decryption overheads in media streaming applications for consumer electronics. Rather than designing and proposing new mathematical encryption algorithms, most of these approaches focus on extracting the most important coefficients/packets from either the transform domain or the compression domain.

Unfortunately, most previous research focuses on the application layer only, without considering optimal delivery of encrypted images in lossy wireless channels. Selective encryption tries to encrypt data as little as possible by controlling the most important parts of the streaming media. Research in [106] [107] proposes scrambling significant coefficients to avoid content fruition by unauthorized users. Although carefully designed scrambling alleviates the known-plain-text or chosen-plain-text attacks, it is difficult to apply UEP in compression scrambling. Promising research works in [101] – [103] combine encryption and entropy coding using Multiple Huffman Table (MHT) alternately in a secret order. Reasonably high level security and unaffected compression efficiency are achieved simultaneously. However, a recent publication in [104] presents chosen plain-text attacks on a basic MHT scheme and an enhanced method with random bit insertion. Recent reported research in [108] also performs cryptanalysis on MHT-based encryption approaches, showing it is vulnerable to known-plain-text and chosen-plain-text attacks. Other research ciphers a selected set of DCT or wavelet coefficients [98] [99] to reduce encrypted data. However, a low quality image can be reconstructed via cipher text only because energy concentration is not equivalent to image perceptibility. Quad-tree and zero-tree-based selective encryption approaches proposed in [97] cipher zero tree structure information in two highest pyramid levels which is crucial to decoding process. This selective encryption approach has thwarted all attacks to date.

In this dissertation, we propose a new selective encryption idea in a position-value manner, extending it to the entropy coding (e.g., Arithmetic Coding (AC)) stage which can be easily implemented according to EZW, SPITH and EBCOT in JPEG2000, and making resource allocation easily applied to the selectively encrypted images. Because selective encryption changes the correlation and inter-dependency between different parts in the final encrypted image bit streams, traditional UEP-based resource allocation is not desirable in this new secure image-delivery paradigm. Furthermore, most previous works in literature propose delay-constrained distortion optimization for general wireless networks, which cannot be directly applied to WSNs due to the high priority of energy efficiency and relatively low priority of end-to-end delay in WSNs. How to transmit selectively encrypted images over WSNs in an energy-efficient manner is still an open research question in literature, which is also a research focus of this dissertation.

3.3 Cross Layer Unequal Resource Allocation

With regard to cross layer wireless multimedia delivery optimization, much previous research has been performed to explore the unequal importance-based wireless image and video transmission. This research has focused on designing efficient resource allocation schemes for multimedia delivery over delay-sensitive wideband wireless networks, and some have focused on energy-constrained WMSNs. However, very few have considered security issues in such cross layer resource allocation designs. Most of these studies achieved UEP via either Forward Error Correction (FEC)- based spatial redundancy or Automatic Retransmission reQuest (ARQ)- based temporal redundancy. Joint Source Channel Coding (JSCC) and network resource adaptation were two major techniques in these designs. Research in [12] [13] preliminarily investigated the tradeoff between energy efficiency and decoded image quality in WMSNs. Research in [14] showed that rate-distortion optimized streaming can be solved via layered UEP, and the authors proposed FEC-based JSCC approaches to optimize the expectation of the reconstructed image quality. However, the rate- and delay-constrained distortion minimization cannot be applied to WMSNs due to the high priority of energy efficiency in WMSNs. The research in [15] furthered the JSCC-based UEP approaches for wireless multimedia delivery and proposed Reed-Solomon coding schemes for energy efficient optimal image transmission in WMSNs. But it took layer-based UEP approach without considering any security factors. The research proposed in [16] also furthered the JSCC approaches by exploring the layered rate-distortion characteristics for multiple images, and proposed a scalable joint source channel image coder to achieve optimal image distortion reduction in the receiver end. Other JSCC-based research such as [17] and [18] proposed layer-based UEP transmission strategies in WMSNs via Rate Compatible Punctured Convolution (RCPC)-CRC coding for JPEG2000 and Set Partitioning In Hierarchical Trees (SPIHT) coded image streaming in WMSNs, respectively. In the network resource adaptation area, research in [19] formulated the efficient network resource allocation problem as a joint optimal selection of transmission strategies across the PHY, MAC and APP layers, which maximizes multimedia quality or perceived Peak Signal Noise Ratio (PSNR) subject to rate and delay constraints. Research in [20] furthered this approach to determine optimal cross layer transmission strategies based on classification and machine learning techniques. The optimal MAC layer retry limits were adaptively predicted for various video packets transmitted over 802.11a Wireless Local Area Networks (WLANs), according to the perception distortion importance of each video packet and the time-varying channel conditions. Other research focusing on network resource adaptation such as [21] [22] proposed effective solutions for improving the performance of delay sensitive multimedia streaming over WLANs. These solutions utilized different error resilient protection techniques such as packetization and retransmission to protect different media priority layers achieving the best effort multimedia quality with rate and delay constraints.

Although those approaches extensively explored the multi-resolution and unequal importance nature of multimedia streaming, the UEP between secure data and plain information was not considered. Since both stream authentication and selective encryption may significantly change the inter-packet dependency profiles, the traditional layer-based UEP schemes cannot be directly applied to secure multimedia streaming in WMSNs. Furthermore, the delay constrained distortion minimization in most of the previous research may not be suitable for WMSNs due to the high energy efficiency requirements. In the proposed network resource allocation schemes described in this dissertation, we consider differences in inborn packet perception and inter-packet decoding dependency, as well as extra authentication dependency, which is fundamentally different from previous work.

3.4 Multi-rate MAC-PHY Transmission Control

Most of the WSN-MAC protocol designs have been well proposed and studied, but the energy efficiency advantages of multi-rate transmission and power control have not been fully utilized. For example, S-MAC [23] was proposed as a low power contention-based MAC protocol, which demonstrates high performance of energy efficiency for WSNs. But S-MAC was based on single data rate transmission and did not provide multi-rate support for upper layer application flows. T-MAC [24] further improved S-MAC's energy efficiency using an adaptive duty cycle control. But T-MAC could not provide multi-rate functionality either. B-MAC [25] was proposed with a simple MAC core and a versatile interface for upper layers, and high throughput and energy efficiency were reported as the major achievements. Z-MAC [26], which was based on B-MAC, employed CSMA as the baseline medium access scheme, and used a TDMA scheduler to improve contention resolution among neighboring sensor nodes. However, both B-MAC and Z-MAC were still based on single data rate transmission, which is not applicable for multi-rate multimedia streaming preferences in the application layer.

On the other hand, there are many research efforts on multi-rate communication networks. But the aim of that research was to improve the throughput performance and channel capacity for application flows. For example, multi-rate designs for Mobile Ad-hoc Network (MANET) [27] [28] [29] [30] were mainly oriented to throughput maximization rather than energy consumption minimization. A few considered energy efficiency issues by providing power saving modes [31] [32] [33], in which individual nodes periodically listened and slept. However, these works still did not address the goal of obtaining high energy efficiency required by WSNs. Research given in [40] and [41] performed intensive studies on energy efficient and multi-rate radio resource management. In those approaches, the communication energy was minimized by combining transmission power control and link rate adaptation for 802.11a/h wireless networks. But those works did not consider the unequal importance characteristics of multimedia application. Other research related to multi-rate and power control schemes have been conducted extensively for Code Division Multiple Access (CDMA) systems [34] [35] [36] [37] [38] [39], which aimed to reduce Multiple Access Interference (MAI) and to increase system capacity. In those research studies, lower data rate transmissions with higher channel coding redundancy were found to achieve lower power consumption, reduced channel interferences and increased channel capacity. However, besides the implementation complexity, a direct extension of these scenarios to WSNs with power efficiency does not necessarily lead to energy efficiency for loss-tolerant multimedia streaming applications in WSNs due to high communication redundancy. As a result, traditional multi-rate and power control schemes are not suitable for WSNs.

In contrast, the proposed multi-rate approach described in this dissertation fine tunes a simple WSN communication platform based on the inherent multi-rate requirement of multimedia, manipulates the power supply and achieves significant energy efficiency. The key difference between our work and the existing approaches for multi-rate networks is that we are intensively focused on improving WSN energy efficiency. This higher-priority goal leads to the following design principles: (1) WSN explores variable transmission rates demanded or desired for multimedia streaming traffic; (2) WSN provides a low-power-low-energy multi-rate communication platform at lower layers based on such explorations; and (3) WSN provides optimal transmission strategies to applications for optimal energy efficiency. While state-of-the-art MAC designs in WSNs strive to achieve energy efficiency in many aspects [23] [24] [25] [26], few approaches provide multi-rate functionality suitable for multimedia streaming applications.

To our knowledge, there have been no multi-rate transmission schemes or corresponding MAC-PHY designs proposed in WSNs for high energy efficiency purposes. Our approach is based on modifying the existing WSN-MAC protocols to accomplish the multi-rate transmission scheme while keeping their effectiveness in medium access and duty cycle management. We add the DMS (Dynamic Modulation Scaling) to achieve multiple data rates and DPS (Dynamic Power Scaling) to provide energy savings.

Chapter 4. Proposed Unequal Traffic Partitioning for Multimedia

4.1 Wavelet Zero Tree Coding

With the proliferation of traffic intensive multimedia streaming applications over resource-constrained lossy wireless networks, zero tree based embedded multi-rate coding has been proposed [46] [47] [48] to cope with time-varying wireless channel capacities. Wavelet-based image compression techniques can achieve high image compression ratios while the embedded multi-resolution multi-rate nature provides an unequal importance attribute, i.e., different parts of the compressed image code streams exhibit different perceptual importance. Important parts provide significant information for reconstruction of the original image, whereas unimportant parts may not provide much information without important parts. The compressed and embedded code stream starts with the rough image followed by quality enhancement.

The digital images are composed of low frequency objects (i.e., lighting information) as well as high frequency edges (i.e., curves, boundary information). After DWT is applied to the original image, the low frequency objects representing the flat areas will be small values close to zero, since the real world natural images mainly contain low frequency information. The high frequency information after DWT will be large value coefficients important for human visual perception. The low value coefficients (i.e., insignificant coefficients) close to zero can be efficiently compressed, and the locations of those large value coefficients (i.e., significant coefficients) are crucial for representing the original image. Consider the wavelet coefficients as a spatial tree with low frequency coefficients at the root node and with the children of each tree node being spatially-related coefficients in the next higher frequency sub-band. There is a high probability that one or more sub-trees will consist entirely of coefficients which are zero or nearly zero; such sub-trees are called zero trees [65]. The wavelet coefficient matrix and the zero tree structure are illustrated in Figure 4.1.

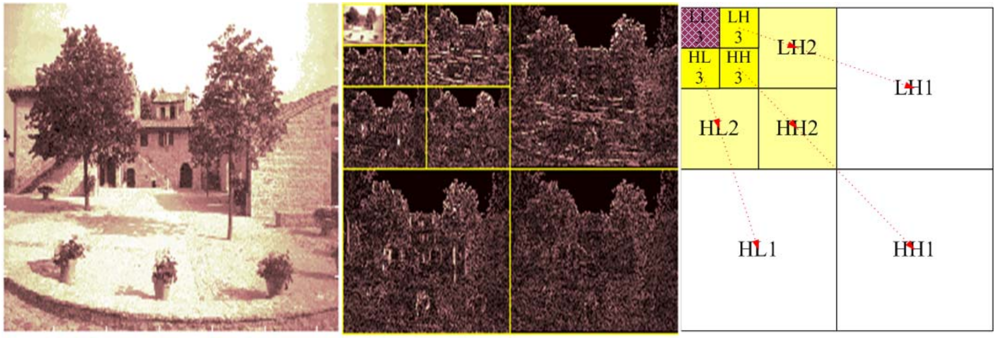


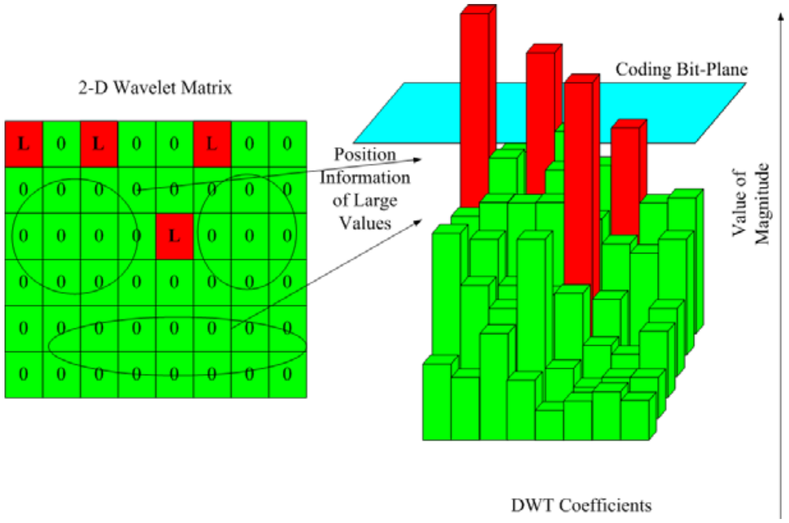
Figure 4.1 Wavelet decomposition and zero tree structure of images

The Embedded Zerotree Wavelet (EZW) [48] and Set Partitioning in Hierarchical Trees (SPIHT) [47] algorithms are the two major wavelet-based image compression techniques, where those important and significant wavelet coefficients are coded followed by refinement code stream in a progressive way. Since the locations of significant wavelet coefficients are extremely important, and the locations of the significant coefficients are determined by the locations of large amount insignificant coefficients with small values in a mutual exclusive set (i.e., wavelet coefficient matrix), the spatial positions of these significant coefficients comprise a large portion of the compressed code stream. For example, the EZW image compression algorithm is designed to effectively compress the position information of the significant coefficients. In EZW, two passes are used in the progressive image coding loops: dominant pass and subordinate pass. In dominant pass, each coefficient in the wavelet coefficient matrix is scanned and one of the four symbols “p” “t” “n” “z” is assigned according to the reference threshold, coefficient value and the values in the sub-trees rooted from this coefficient. The significant wavelet coefficient is also encoded in the subordinate pass by bit “0” or “1” denoting the magnitude significance. In practical implementation, it would be usual to use an entropy code such as arithmetic code to further improve the performance of the dominant pass, while the data bits from the subordinate pass are usually random enough that entropy coding provides no further coding gain [65].

The zero tree structure has laid a significant foundation for the position-value based code stream partition and UEP transmission paradigm, which will be discussed in details in the next section.

4.2 Position and Value Partitioning

The information of a natural digital image is typically conveyed by the shapes and objects containing low frequency flat area image pixels as well as the high frequency edges. As discussed in the previous section, wavelet-based image compression schemes such as [47] [48] can efficiently extract the high frequency shape and position information of the regions as well as the low frequency lighting magnitude information in these regions and objects. The wavelet coefficients with small magnitude values are the determination information of the significant coefficients' locations which can be desirably compressed by significance propagation, dominant encoding, and run length based cleanup coding passes. Thus, the small values of insignificant coefficients can be translated into position information while the large magnitude coefficients can be translated into value information. Position and value information have different perceptional importance, since the locations of value information depends on the correct decoding of position information. Figure 4.2 shows the illustration of wavelet coefficients, bitplane coding and the physical concept of the position – value information.



L	0	L	0	0	L	0	0
0	0	0	0	0	0	0	0
0	0	0	0	L	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 4.2 The unequal importance of position and value information

As illustrated in this figure, small-magnitude coefficients are translated into a large number of "0" bits in a bitplane according to a reference threshold and these clustered "0" bits can be efficiently compressed. The compressed small coefficients have avalanche error propagation effects since the errors in the number of consecutive “0” bits directly impacts the positions or locations of the large magnitude significant coefficients, leading to irrecoverable misalignment and decoding errors. These coefficients in small values stand for the image position information. The output of magnitude refinement bits are related to the large magnitude wavelet coefficients corresponding to the image value lightening brightness information. Although these large magnitude values themselves are relatively unimportant, their locations are crucial for decoding and perceptional distortion. Their locations are determined by the process of compressing small-magnitude coefficients. Wavelet coefficients with large magnitudes are determined according to the following criterion: either the quantized wavelet coefficient bit in the current bitplane is “1”, or at least a bit in previous bitplane is “1”. Thus, coefficients with large magnitudes are compressed into value information, and coefficients with small magnitudes are compressed into position information. The communication packet loss or bit errors in position information will have significantly higher impact on the overall quality of the received image than the loss or errors in value information. Transmission errors in position information (p-data segments) lead to high difficulties for reconstructing the original image, while errors in the value information (v-data segments) are relatively more tolerable [51].

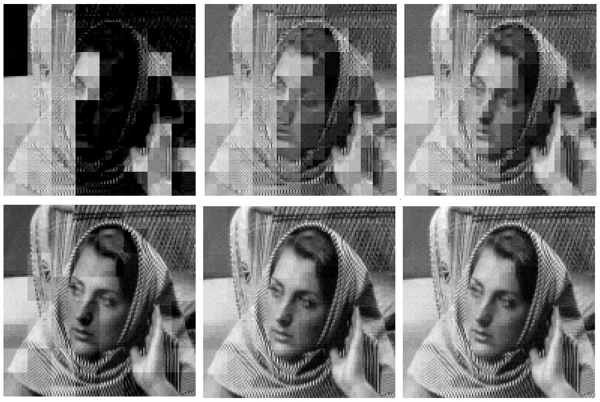


Figure 4.3 The visual importance of position and value information in error-prone wireless channel

Sub-figures of Figure 4.3 show the visual quality with erased different p-data segments and v-data segments in a P-V partitioned code stream compressed by the algorithm described in [48]. The upper row sub-figures show the decoded image with erased p-data segment from bitplane 0 (assume the bitplane index starts from 0) to bitplane 2 and bitplane 4 respectively and the lower row sub-figures show the decoded image with erased v-data segments in the same bitplane. It is clear from these experimental results that the p-data segments are much more important than the v-data segments. If the p-data segments in lower bitplanes (i.e., close to the MSB bitplane) are erased by wireless channel, the semantic content meaning in the reconstructed image is hard to be determined; even p-data segments in higher bitplanes (i.e., close the LSB bitplane) are erased, significant perception noise will be incurred. On the other hand, erasing v-data segments in the compressed code stream has no significant perception degradation. Even the v-data segments in lower bitplanes are erased by wireless channel, most of the semantic meaning in the decoded image can still be preserved. This is because the errors in the p-data segments will affect the decoding process of v-data segments in an avalanche effect, while the errors in v-data segments are more isolated.

The compressed code stream by wavelet codec can be effectively separated via significant position and insignificant value coding pass partition. As analyzed in the previous sections, the position information determining the code stream structures is more sensitive to transmission bit errors and packet losses than value information, especially in wireless channels, since the decoding of v-data segment depends on the successful decoding of p-data segments. On the other hand, wavelet-based compression algorithms organize the position and code stream structure information and magnitude value information in different coding passes, where the position information and value information can be desirably separated via coding pass partitioning. Algorithm 4.1 has been proposed in [51] to illustrate the identification and separation of position and value information from a standard wavelet codec.

Algorithm 4.1: P-V information separation via coding pass partition.

1. Initialize position information storage buffer $pBuf$ for p-data segments and buffer $vBuf$ for v-data segments value information storage. Perform DWT on the original image and store the wavelet coefficients in the Matrix X, with x rows and y columns, respectively.

2. Determine the initial magnitude quantization reference threshold T for bitplane coding iterations. The initial threshold can be determined as $T = 2^{\lfloor \log_2 (\max (|X(i,j)|)) \rfloor}$, where $0 \le i \le x-1$ and $0 \le j \le y-1$. Also determine the maximum number of bitplanes N according to user defined rate-distortion truncation indicator or compression ratio requirements.

3. Start coding loop iteration. For bitplane iteration γ = 0 to $N-1$, do steps (4) to (6).

4. Perform coding pass to determine the locations of significant position information. Scan the wavelet coefficients in the wavelet coefficient matrix X according to a certain scanning order (e.g., Morton scanning). Given the reference quantization threshold T used in the current bitplane, any coefficient in the wavelet coefficient matrix can be determined explicitly as either a large magnitude coefficient (magnitude is equal to or larger than the reference threshold T) or a small magnitude coefficient (magnitude is smaller than the reference threshold T). The clustering models of the small magnitude insignificant coefficients determine the locations and positions of the large magnitude significant coefficients. Once a coefficient is determined as a large magnitude significant coefficient, it is coded as positive (e.g., “p” symbol) or negative (e.g., “n” symbol) significant symbol according to its sign bit and the reference threshold, and its location is marked by the positive or negative symbol. Magnitude refinement coding pass will be further applied to this significant wavelet coefficient as described in Step 5. If a coefficient is determined as a small magnitude insignificant coefficient (i.e., a bit “0” in the current bitplane), it is coded as a tree structure symbol (e.g., either tree root symbol “t” or isolated zero symbol “z”). Specifically, it is encoded as a tree root symbol if all its wavelet coefficient matrix descendents of the sub-tree rooted by itself in the same spatial direction are small magnitude coefficients with regards to the threshold T. If one or more descendents are determined as large magnitude coefficients regarding to threshold T, then this coefficient is encoded as an isolated zero symbol. The positive and negative significant symbols (e.g., “p” and “n”), isolated zeros and tree roots (e.g., “t” and “z”) are identified as important position information and stored as the p-data segment in $pBuf(\gamma)$ for the current bitplane.

5. Invoke subordinate coding pass of magnitude refinement for large-magnitude coefficients. All the coefficients marked as positive or negative symbols are further

processed to refine their magnitude approximation. The most significant bit (MSB) in the current iteration denoting the magnitude of each positive or negative significant symbol is stored as the v-data segment $vBuf(\gamma)$ in the current bitplane.

6. Decrease the threshold by half as $T = T / 2$, and then go back to Step 3 for the next bitplane. The p-data segments and v-data segments in the following bitplanes are formed in the same way iteratively and progressively as shown in Steps 4-6.

7. Algorithm finishes. Output the image code stream stored in $pBuf$ containing the position information and $vBuf$ containing value information bitplane by bitplane in an embedded manner.

After wavelet-based compression and P-V partitioning, the code stream is composed of interleaving p-data segments and v-data segments in an embedded manner with a decreasing order of importance. It starts with the rough and coarse image information followed by position and value information for quality refinement. Since the image code stream structures are only stored in p-data segments, the incorrect symbols due to transmission errors in p-data segments incur the next-bitplane bits misinterpretation, while incorrect bits in v-data segments do not affect the decoding of others. Figure 4.3 shows the reconstructed images with different p-data segments and v-data segments erased in different bitplanes, where significant noise or distortion is incurred perceptually when a p-data segment is missing even in a high-level refinement bitplane; however, even when a v-data segment in a low bitplane is erased, the reconstructed image can still convey most of the information in the original image. The correct decoding of the p-data segment depends on the correct decoding of previous p-data segments only, but the correct decoding of v-data segment depends on previous bitplanes of both v-data segments and p-data segments. Thus, p-data segments are much more important than v-data segments. Also, the segments in lower bitplanes are much more important than those in higher bitplanes.

It is worth noting that, although we take zero tree based compression algorithms such as [47] [48] as examples in this dissertation, the proposed position – value partitioning scheme is general and is independent of the specific wavelet compression algorithms, since natural digital images have inherent features of position and value diversity. The reason for selecting the tree-based algorithms as baseline is that position and value information can be easily separated during the partition process, as described in Algorithm 1 [51]. The proposed P-V partitioning scheme can be easily extended to other wavelet-based image compression algorithms such as the EBCOT [49] based JPEG2000 coding standard, since the essential position-value diversity is the spatial inheritance of the digital image itself rather than the coding scheme. The clusters of small magnitude insignificant wavelet coefficients can be efficiently and effectively represented as context formation (CF) models, significant propagation (SP), clean-up passes (CP), and arithmetic codes (AC).

Chapter 5. Proposed Cross Layer Unequal Resource Allocation

In previous chapters, we discussed information identification and multimedia traffic partitioning at the application layer. Because different parts of the multimedia stream have different perceptional importance, and the decoding of some packets depends on the successful decoding of some other packets, Unequal Error Protection (UEP)- based resource allocation is proposed in this chapter to cope with the new multimedia traffic paradigm. By considering both decoding dependency and visual importance at the application layer, as well as channel information and transmission control parameters at lower layers, resource allocation efficiency in terms of energy-quality gain can be significantly improved by effective protection of visual-decoding-important packets.

5.1 Multi-rate Energy Efficiency

In digital signal processing applications such as multimedia streaming over wireless sensor networks, source data gathering nodes collect digital information and send compressed data to the base station or sink node individually or collaboratively, at different transmission data rates and possibly via different routing paths. On the other hand, current wireless network attributes such as wireless channel conditions and network routing topologies can bring optimal transmission rates in terms of energy efficiency on each path and each hop [52] [83] [86]. It is thus desirable for sensor networks to provide a support for multi-rate transmission platforms, driven by the need for upper layers of network and wireless channel information to achieve energy efficiency. This WMSN-based multi-rate adaption scheme is significantly different from traditional multi-rate link adaptation research in general wireless networks, where the focus is to increase throughput based on rate adaptation from variable channel conditions [84]. Figure 5.1 shows an illustrative example of digital signal processing applications in wireless sensor networks, where energy efficiency is achieved by low layer multi-rate transmission control.

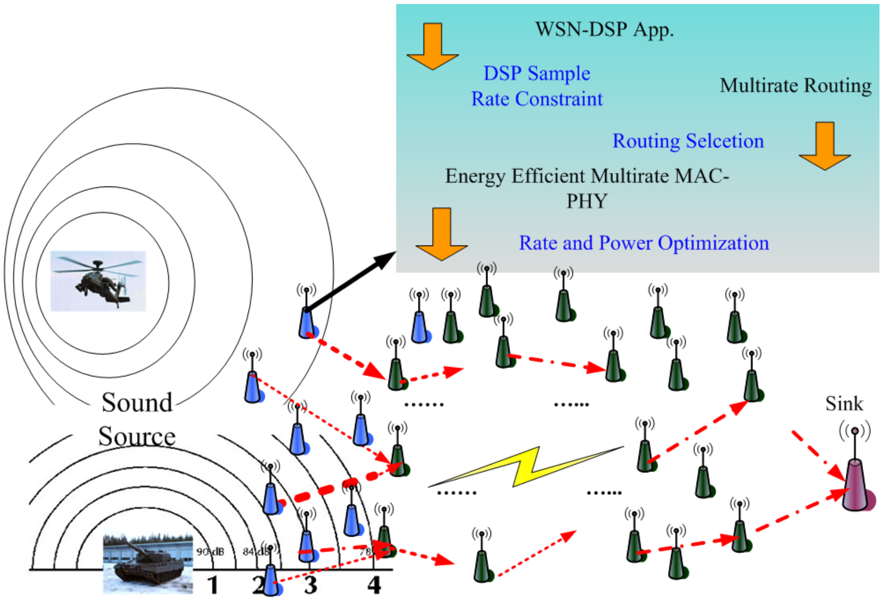


Figure 5.1 Energy efficient digital signal processing applications in multi-rate wireless sensor networks

In a wireless multimedia sensor network environment illustrated in this figure, multimedia signals (e.g., audio data or image/video information) is collected by source data gathering nodes, and transmitted via multiple routing paths in multiple hops with different transmission data rate requirements. Central to each data gathering and forwarding node is the transmission strategy scheduling for the purpose of achieving energy efficiency. In each sensor node, application data flow traffic information and wireless channel information are both acquired as the input to the transmission scheduling algorithms, and transmission parameters such as data rate and transmission power are optimized in terms of energy efficiency. Since the wireless channel information may vary significantly in different geographic locations, each sensor device has its own optimal transmission scheduling control. The transmission strategy control functionality in MAC and PHY provides optimized packet level loss rate and energy consumption performance to upper layers, which will be utilized in the overall cross layer authentication, energy and distortion optimization.

5.2 Link Layer Energy-Distortion Theory

The effects of network resource allocation in the link layer can be represented as the turning factor of energy-distortion performance tradeoff for each packet. The distortion of each packet is defined in this dissertation as the expected packet loss rate, or the probability of receiving the packet in errors. The energy here denotes the mathematical expectation of the energy consumption given the resource allocation parameter such as power, rate, and retry. Thus, we can establish the link layer (layer 2) energy-distortion performance mapping: $\{\rho, \overline{E}\} \mapsto \eta = \{e, m, R\}$ for each single media packet with length denoted by L, where the expected energy consumption and average packet loss ratio of transferring each packet is related to the desirable Bit Error Rate (BER) requirement denoted by e, ARQ retry limit denoted by m, and the scalable transmission data rate denoted by R according to our research in [51] [52] [85]-[87].

5.2.1 Bit Level Power-Rate Control

In a wireless channel environment, transmission performance such as BER at the receiver end and transmission cost such as the power consumption is an inherent tradeoff. Time-varying channel information such as wireless path loss, instantaneous channel fading, and interference causes Signal-to-Noise Ratio (SNR) and BER variations. While high data rate schemes using complicated and denser modulation encoding may significantly improve throughput and reduce active transmission time in sensor networks, a tradeoff still exists between data rates and BER.

According to well-known studies presented in [88] [89] [90], the desirable BER value e can be mapped to an optimal transmission power value P_t given the modulation scheme, especially the modulation constellation size b, frequency bandwidth (or presented in symbol rate in some research works) R_s, noise power density N_0, and channel state information factor A denoting the instantaneous wireless channel loss. Energy savings in sensor networks is primarily achieved by adjusting the transmission data rate and transmission power supply to the radio module adaptively. In wireless communication studies, the SNR required at the receiver end and the corresponding BER performance expectation can be estimated from each other given the modulation scheme. For example, the BER for simple BPSK and QPSK modulation schemes can be expressed as follows, according to [89], where $erfc$ function follows the definition in [116]:

$$e = \frac{1}{2} erfc\,(\sqrt{\frac{E_b}{N_0}}) \tag{5.1}$$

Similarly, for complex M-QAM modulation schemes, the BER performance is expressed as follows [89]:

$$e = \frac{2}{b}\left(1 - \frac{1}{2^{\frac{b}{2}}}\right) erfc\left(\sqrt{\frac{3b}{2(2^b - 1)} \times \frac{E_b}{N_0}}\right) \tag{5.2}$$

Today these simple low rate modulation schemes such as BPSK and QPSK are widely used in radio modules of sensor networks due to their robustness in error-prone wireless channels. Although complex M-QAM modulation circuits may take more physical device space and higher financial production cost, it is still feasible to be utilized in wireless sensors for further research [91]. With the intensive network bandwidth requirements of real-time video and audio sensors in advanced signal processing applications such as target tracking and intrusion detection, M-QAM modulation is an ideal candidate to improve the bandwidth utilization and latency performance [92].

Now we derive the relationship between BER and transmission power for the M-QAM scheme. Equations (5.1) and (5.2) give the theoretical relationship between BER and the ratio of energy per bit to noise power density denoted by E_b / N_0. The receiver side SNR can be acquired as follows, according to [90]:

$$SNR_{rx} = \frac{E_b}{N_0} \times b \tag{5.3}$$

Given the receiver side signal-to-noise ratio SNR_{rx}, the noise floor N, and channel state information including antenna gain A, the transmitter side power can be expressed as the following equation, according to [88]:

$$P_t = SNR_{rx} \times N \times \frac{1}{A} \tag{5.4}$$

The noise floor N can be calculated from the frequency bandwidth determined by the physical layer transmission symbol rate R_s and the noise power density N_0, as shown in [89] [90].

$$N = R_s \times N_0 \tag{5.5}$$

Thus, the minimum transmission power P_t required to maintain receiver side signal quality is quantitatively expressed as follows in terms of E_b / N_0 :

$$P_t = R_s \times b \times \frac{N_0}{A} \times \frac{E_b}{N_0} \tag{5.6}$$

Now we have the mathematical relationship between transmission power P_t and signal quality E_b / N_0. The purpose is to derive the relationship between the transmission power and the receiver side BER performance. According to Equations (5.1) and (5.2), we can straightforwardly derive the equations for transmission power expressed by desirable BER at the receiver end. The transmission power for simple BPSK and QPSK modulation schemes can be expressed as

$$P_t = R_s \times b \times \left[erfc^{-1}(2 \times e)\right]^2 \times \frac{N_0}{A} \tag{5.7}$$

The minimum transmission power required to keep a desirable BER e at the receiver side using complex M-QAM modulation schemes can be expressed as

$$P_t = \frac{2}{3} R_s \times \left(2^b - 1\right) \times \left[erfc^{-1}\left(\frac{b}{2}\left(1 - \frac{1}{2^{\frac{b}{2}}}\right)^{-1} \times e \right) \right]^2 \times \frac{N_0}{A} \tag{5.8}$$

Upon determination of the modulation scheme, the physical layer transmission symbol rate R_s and modulation constellation size b are also determined. Thus, the transmission data rate R is determined by $R = R_s \times b$. In the multi-rate energy efficient transmission systems of sensor networks, the desirable BER e is a system pre-configured parameter defined by the upper layer or the cross- layer resource allocation scheduling algorithms. The Gaussian noise power intensity N_0 is a system constant value. Channel state factor A can be measured adaptive to the time-varying wireless channel. From the above theoretical analysis, all the factors and parameters on the right sides of Equations (5.7) and (5.8) can be determined, and thus transmission power is expressed in close form. In addition, it is critical to see that a reduction in transmission data rate is disproportionate to the reduction in transmission power, since high data rate transmission requires denser modulation schemes with higher constellation size b, thus leading to less error-robustness. Transmitting data at a lower data rate with a more robust modulation scheme (i.e., a lower value of modulation constellation size b) achieves better transmission power efficiency in the physical layer than the higher data rate transmission.

5.2.2 Packet Level Retransmission Control

Based on the bit-level multi-rate power versatility analysis discussed in the previous section, the link layer distortion-energy performance can be modeled as the mapping from resource allocation strategies to the average packet level loss ratio $\overline{\xi}$ and average energy consumption $\overline{E}$. The resource allocation strategies here denote the physical layer transmission power P_t, modulation constellation size b and MAC retry limit $m_{\max}$.

Following the definition and analysis presented in our previous work [51], we define a fully ordered set $\Omega = \{r, c, d, a\}$ to express the average packet level loss probability $\overline{\xi}$

and average energy consumption $\bar{E}$, where the elements r, c, d and a denote the possible events of control packet delivery failure, i.e., RTS, CTS, DATA and acknowledgement (ACK) delivery failure. The events in the fully-ordered set Ω ($r < c < d < a$) are illustrated as follows. The delivery of CTS packet depends on the successful delivery of the previous RTS packet, and the delivery of the DATA packet depends on the successful delivery of the previous CTS. In a similar way, the delivery of the ACK packet depends on the delivery of the previous DATA packet. In other words, without successful delivery of the previous packet denoted in the fully-ordered event set, a later packet will not be transmitted. The event probability of such packet transmission is zero.

In multi-rate energy efficient WMSN transmission systems, control packets are typically transmitted using a protocol-defined transmission power (i.e., maximum power is usually used for control packet transmission) and protocol-defined transmission rate (i.e., a basic data rate using the most robust modulation scheme is applied to control packets). Let P_r denote the receive power; R_o denotes the transmission data rate of the overhead packets; l denotes the virtual packet length of the timeout event which can be easily calculated from the timeout value T_o of receiving a packet $l = T_o \times R_o$. Also let e_o denote the BER of control overhead packets such as RTS, CTS and ACK, where e_o can be simply determined given the protocol-specified fixed transmission power $P_{\max}$.

$$e_o = \frac{1}{2} erfc\left(\sqrt{\frac{P_{\max} A}{R_s b N_0}}\right) \tag{5.9}$$

Let p_i denote the packet transmission error probability of the $i-th$ packet in a single transmission round. Let S_r, S_c, S_d, and S_a denote the packet length of RTS, CTS, DATA payload and ACK, respectively. The packet loss probability for overhead packets such as RTS and CTS can be generically approximated. For example, the packet error probability of an RTS packet failure can be easily expressed as $p_r = 1 - (1 - e_o)^{S_r}$.

$$\forall i \in \Omega, i \neq d: \\ p_i = \prod_{k \in \Omega, k < i} (1 - p_k) \times \left(1 - (1 - e_o)^{S_k}\right) \tag{5.10}$$

Let e be the desirable BER for a DATA packet with the total length S including data payload, MAC header length H_o and security overhead. Since the encryption process does not change the bit length of the data chunk, the extra bit rate overhead for multimedia selective encryption is zero. Thus the security overhead in packet level analysis is confined to authentication overhead due to the introduced authentication crypto-hash tags. The authentication crypto-hash bit overhead can be calculated given the known redundancy degree $|\pi|$ (i.e., the number of incoming authentication descendents). For example, let S_{sig} denote the size of signature, and S_{hash} denote the size of a crypto-hash tag; the total packet length can be calculated straightforwardly for the signature packet.

$$S = S_d + |\pi| S_{hash} + S_{sig} + H_o \tag{5.11}$$

For other packets without an attached signature, the total packet length is reduced to

$$S = S_d + |\pi| S_{hash} + H_o \tag{5.12}$$

Given the total packet length, the packet loss probability of each DATA packet can be expressed as follows, according to [51].

$$i \in \Omega, i = d: \\ p_i = \prod_{k \in \{r,c\}} (1 - p_k) \times \left(1 - (1 - e)^{S}\right) \tag{5.13}$$

Up to now, the packet loss event probability in the fully-ordered packet delivery event set Ω has been quantitatively determined. In the following part of this subsection, we will focus on the quantitative expression and approximation of the communication energy consumption. If the RTS packet transmission fails due to transmission errors in the wireless channel, extra unnecessary energy is consumed by both the transmitter and receiver sides of the WMSN. The corresponding energy cost E_r due to RTS packet delivery failure can be expressed as follows:

$$E_r = (P_{\max} + P_r)\frac{S_r}{R_o} + P_r(\frac{S_c + 2l}{R_o}) \tag{5.14}$$

The energy cost E_c due to CTS packet transmission failure is expressed in the following equation in a similar way, by summing up both the transmitter side and receiver side energy consumption:

$$E_c = (P_{\max} + P_r)\frac{S_r + S_c}{R_o} + P_r\frac{S + 2l}{R_o} \tag{5.15}$$

The communication energy savings is achieved by power control in the DATA packet transmission. Unlike the control packets such as RTS, CTS and ACK, the DATA packets are transmitted using the scaled transmission rate R and controlled power P_t at multiple discrete levels. The total communication energy cost due to DATA packet failure, including both transmitter side and receiver side energy consumption, is expressed as follows:

$$E_d = (P_{\max} + P_r)\frac{S_r + S_c}{R_o} + (P_t + P_r)\frac{S}{R} + P_r(\frac{S_a + 2l}{R_o}) \tag{5.16}$$

Similarly, as analyzed above, the energy cost E_a due to ACK packet transmission failure can also be expressed as:

$$E_a = (P_{\max} + P_r)\frac{S_r + S_c + S_a}{R_o} + (P_t + P_r)\frac{S}{R} + P_r\frac{l}{R_o} \tag{5.17}$$

Besides the transmission failure event, the successful transmission event should also be considered in the calculation of average energy consumption. The energy cost of sending a packet successfully by means of such RTS-CTS-DATA-ACK four-way handshaking is expressed as

$$E_s = (P_{\max} + P_r)\frac{S_r + S_c + S_a}{R_o} + (P_t + P_r)\frac{S}{R} \tag{5.18}$$

Also based on the four-way handshaking nature, the probability of packet delivery failure p in a single delivery without retransmission consideration can be expressed as $p = \sum_{i\in\Omega} p_i$. Let $m_{\max}$ denote the link layer ARQ retry limit. The average retransmission round $\overline{m}$ can be expressed as a function of single round packet loss ratio and retry limit, according to [21] [22], as

$$\overline{m} = (1-p)\sum_{i=1}^{m_{\max}} i \times p^{i-1} + (m+1)p^{m_{\max}} \tag{5.19}$$

We can also approximate the average loss ratio $\overline{\xi}$ as follows, where it is eventually a function of desirable BER e and ARQ retry limit m in a way similar to [21] [22] [51]:

$$\overline{\xi} = 1 - (1-p) \times \sum_{i=1}^{\overline{m}} p^{i-1} \tag{5.20}$$

Finally, the average energy consumption $\overline{E}$ can be expressed as a close form function of different resource allocation parameters: desirable BER e, ARQ retry limit $m_{\max}$, and transmission data rate R:

$$\overline{E} = \overline{m} \times \left(\sum_{i\in\Omega} p_i E_i + \left(1 - \sum_{i\in\Omega} p_i\right) E_s \right) \tag{5.21}$$

In some scenarios requiring high transmission efficiency in WMSN, RTS/CTS-based handshaking and channel probing/reserving schemes are typically disabled due to high communication overhead. Furthermore, the duty cycles and sleep modes are typically introduced into MAC layer scheduling for energy savings. In such efficient transmission systems, the loss ratio for a packet with payload length S_d with security overhead (i.e., authentication overhead) can be expressed as follows, given incoming authentication redundancy degree $|\pi|$ and packet transmission overhead H_o and S_a:

$$p = 1 - (1 - e)^{S_d + |\pi| S_{hash} + H_o + S_a} \tag{5.22}$$

The incoming authentication redundancy degree $|\pi|$ increases both packet loss ratio penalty and energy consumption overhead. This is because the additional attached crypto-hash tags increase the bit rate overhead of each packet, which causes extra energy consumption. Considering such security overhead, the energy consumption of delivering the packet with length S_d can be approximated as follows, where T_o denotes the protocol-related transmission time overhead, P_s denotes the sleep power and T_{cyc} denotes a time cycle of sleep period.

$$\begin{aligned} E = {} & P_t \times \left(\frac{S_d + |\pi| S_{hash} + H_o}{R} + T_o \right) + P_r \times \left(\frac{S_a}{R} + T_o \right) \\ & + P_t \times \left(\frac{S_a}{R} + T_o \right) + P_r \times \left(\frac{S_d + |\pi| S_{hash} + H_o}{R} + T_o \right) \\ & + 2P_s \times \left(T_{cyc} - \frac{S_d + |\pi| S_{hash} + H_o + S_a}{R} - 2T_o \right) \end{aligned} \tag{5.23}$$

Based on the packet loss ratio and packet transmission energy consumption in a single transmission, we can derive the expressions of average packet loss ratio and expected energy consumption considering link layer retransmission. The average packet loss ratio expectation can be reduced to the following expression according to [21] [22], given the link layer retry limit $m_{\max}$:

$$\overline{\xi} = p^{m_{\max}} \tag{5.24}$$

The energy consumption expectation can be approximated as follows according to [22]

[23], given the single round transmission energy and the retry limit:

$$\overline{E} = E \times \frac{1-\xi^{m_{\max}}}{1-\xi} \tag{5.25}$$

According to the above analysis, the packet delivery energy-distortion performance can be quantitatively modeled as the average packet loss ratio $\overline{\xi}$ and the expected energy consumption $\overline{E}$ with retransmission consideration.

5.3 Disproportionate Resource Allocation

The provision of secure multimedia streaming in energy-constrained WMSNs in a cross layer fashion naturally favors disproportionate network resource allocation. In such cross layer scheduling, the security strategy in terms of multimedia selective encryption and stream authentication, as well as the network transmission strategies in terms of rate and power control, need to be jointly adjusted with regard to application attributes such as packet distortion reduction, packet decoding dependency and wireless channel conditions. Figure 5.2 illustrates the cross layer secure resource management architecture.

The multimedia stream coming from the application layer is processed with selective encryption or crypto-hash-based stream authentication, or both. The pre-processed distortion reduction of each packet denoting the packet importance is also an input of the system. The distortion reduction can be either measured or predicted using well-studied methods, and the packet decoding dependency is also analyzed for efficient resource allocation purposes. The secure multimedia stream is sent down to lower layers (e.g., the MAC layer and the PHY layer) for transmission. It is worth noting that we did not design a new medium access protocol in sensor networks, but rather used the existing sensor network MAC protocols such as T-MAC [24] or S-MAC [23]. The duty cycle management and channel access control mechanism in these protocols are not changed by our proposed approach. Our proposed resource allocation functionality serves as a plug-in to the existing protocols. The resource allocation algorithm residing in the resource allocation scheduling unit takes the packet distortion reduction of each packet and the stream decoding and dependency as the inputs. It then produces the desirable BER as the output for UEP- based transmission protection.

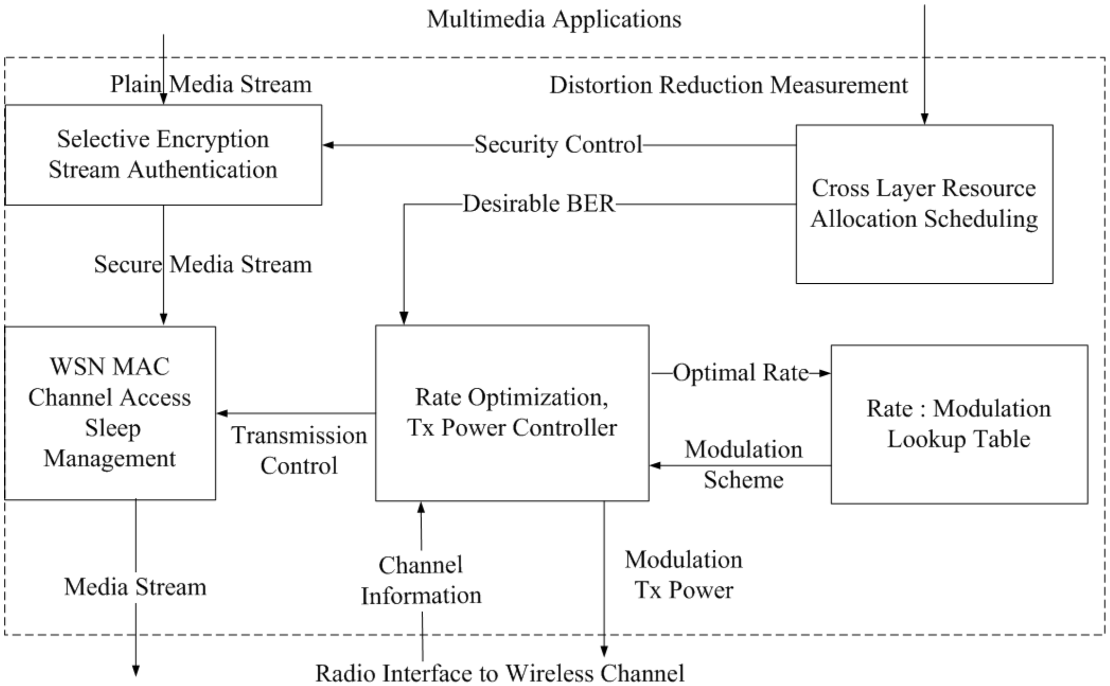


Figure 5.2 Cross layer resource management framework for secure multimedia streaming in multi-rate APP-MAC-PHY

The desirable BER is an effective intermediate system parameter to achieve UEP-based transmission protection. This parameter can be modified or updated by the cross layer resource allocation algorithm adaptively according to application layer media characteristics as well as wireless channel conditions. When the MAC layer is ready to transmit data packets to the corresponding neighbor nodes, it enables and initializes the wireless radio module, performs carrier sensing contention or clear channel assessment for the shared wireless channel, and then sends security-protected multimedia packets with optimized transmission strategies to the intended receiver. The desirable BER produced by the resource allocation algorithm is translated into physical layer transmission power according to the methodology presented in the previous section, as well as the methodology reported in [51]. Then the modulation scheme is selected by looking up the data rate and modulation mapping in the lookup table. After the computation of proper transmission power and supplying this optimized power to radio module, the transmitter side starts transferring data via the chosen modulation scheme with the properly controlled transmission power. Once the packet transmission finishes, the MAC layer resets the radio module to the basic modulation scheme (usually the simplest but most robust modulation scheme) with protocol-specified maximum transmission power, in order to make sure the control packet such as RTS and CTS can be properly transmitted.

The desirable BER translated into transmission power control is a more desirable resource allocation parameter than others such as retry limit or data rate, because it is easy to tune the energy-distortion performance in fine grain, while the transmission data rate and retransmission limits can only be controlled in coarse grain. It is true that a higher ARQ retry limit can reduce the average packet loss ratio significantly by invoking a new round of packet transmissions; however, the retransmission incurs considerable energy penalty and latency overhead. More importantly, the ARQ retry limit is discrete and only integer values are valid for real world configuration, leading to undesirable fine-tuning performance. In a practical environment such as the TinyOS platform, transmission power control is typically performed by writing an 8-bit register using NesC [94] code, for example, *PotC.setPot(uint8_t nTxPower)*, where the valid range of transmission power is [0,99] for the Micaz platform [51]. Thus, transmission power control can be performed in a near-consecutive way.

Furthermore, the transmission data rate can be independently optimized, further simplifying the overall cross layer optimization problem. This rate independency can be verified from equations presented in the previous section, where either the transmission data rate R or the constellation size b is not a variable in calculating the average loss ratio $\bar{\xi}$. In other words, changing the transmission data rate or the modulation constellation size will only affect the energy consumption but not the average packet loss ratio. This is because in our proposed resource allocation framework, adaptive power control is applied to each packet transmission in high data rate compensating for the bit-error overhead due to the increased rate. If a higher transmission data rate is applied, higher transmission power will also be applied automatically to ensure a similar receiver side signal quality as achieved by lower rate transmission. Similarly, when the packet is transmitted using a lower data rate, lower transmission power is selected to reduce energy consumption. Since the data rate R is independent of the packet loss ratio, it is also independent of the total expected multimedia quality (i.e., total distortion reduction), and the transmission rate optimization can be performed individually. On the other hand, the available choices of PHY layer transmission data rate and modulation schemes are quite limited and enumerable [19]. In this research, we only consider QPSK and M-QAM with only four available discrete transmission data rates, where similar modulation enumeration approaches are also found in latest research such as [19] and [67]. The optimal transmission data rate in terms of minimal energy consumption per information bit of pure data can be acquired by a simple enumeration search among the data rates. This simple enumeration scheme can be easily handled in a low cost radio module in sensor networks, which provides significant application impacts in low power wireless electronics.

5.4 Summary

In this chapter we have discussed unequal resource allocation strategies. The UEP-based resource allocation scheme should be performed in an application-aware manner, not only considering the throughput and latency but also targeting energy efficiency in WMSNs. First we have analyzed the multi-rate power efficiency starting in the physical layer, and formalized the quantitative relationship between transmission data rate and transmission power. We have shown the possibility of achieving reduced power consumption using low rate transmissions. Then we have stepped into the link layer and proposed a link layer energy-distortion modeling methodology. In the proposed link layer energy-distortion model, the packet transmission performance in terms of energy consumption and packet loss ratio are quantitatively expressed by network resource allocation parameters. Thus, these parameters are connected to packet delivery quality and energy consumption expectations.

Chapter 6. Proposed Unequal Control for Multimedia Selective Encryption

In this chapter, we discuss the theory and methodology of providing privacy in quality-driven WMSNs with energy efficiency assurance. The feasibility of jointly designing low cost multimedia selective encryption and energy efficient network resource allocation becomes a key challenge. The multimedia privacy protection discussed in this chapter is similar to stream authentication: stream authentication tries to verify as many packets as possible, whereas selective encryption tries to encrypt data as little as possible by controlling the most important part of the streaming media. Similar to stream authentication, selective encryption also changes the correlation and inter-packet dependency between different parts in final encrypted image code streams. Traditional UEP schemes are not desirable for such new secure multimedia delivery paradigms.

6.1 Provision of Multimedia Privacy and Quality Assurance

6.1.1 Selective Encryption Concept

Multimedia delivery applications in WMSNs have gained tremendous popularity in recent years. However, security issues for these applications have become major challenges for several reasons. First, wireless channels in WMSNs are more vulnerable to malicious intrusion attacks and packet eavesdropping than wired ones, leading to higher security sensitivity requirements. Furthermore, the low cost sensor nodes are extremely constrained in real-time encryption and online transmission capability due to the computational, memory and energy resource constraints.

Traditional cryptographic techniques have been proposed to offer binary data privacy in a strict sense, i.e., encrypting the whole data stream to achieve data security. These conventional schemes may work fine for binary data flows, but not for content sensitive and loss tolerant multimedia. Large size multimedia content requires considerable computational resources in encryption and decryption far beyond what a low cost sensor node can offer. Moreover, the processing time for encryption and decryption bottlenecks real-time secure multimedia delivery applications. Due to these limitations, the multimedia content flows have to be selectively encrypted to reduce the total computational complexity, and transferred in noisy and insecure channels with energy and bandwidth resource constraints. On the other hand, transmission bit errors and packet losses are inevitable in time-varying noisy wireless networks, especially in harsh sensor network environments. Therefore, there is a strong need to design error robust and communication efficient resource allocation schemes for secure image delivery over WMSNs, where content security, media quality and energy efficiency are all challenging tasks in these systems.

Considering security in resource allocation has received very little attention in recent literature. Multimedia encryption approaches have been proposed to cipher the important coefficients selectively from either the transform domain or the compression domain [96]-[100]. Most of these approaches focused on extracting the most crucial coefficients or packets from either the transform domain or the compression domain, rather than designing and proposing new mathematical encryption algorithms. Thus the security level is relatively high, with significant challenges in finding the dominant parts of the compressed code stream. Other research has been proposed to use secret entropy coding to achieve multimedia security in a different way [101]-[107]. Typically the entropy coding stage is slightly modified and the coded stream is ciphered by a certain pseudo random order. The implementation of these approaches is relatively simple and mathematical computational complexity is relatively low. But the disadvantage of these schemes is low level security due to the pseudo random ordering in entropy coding. The first category is typically referred to as multimedia selective encryption and the second category is generally referred to as joint entropy coding and encryption. Although they are different in design methodologies, the purpose of these two encryption categories is the same: to achieve multimedia privacy while reducing encryption overhead favoring real-time multimedia security.

Most of the previous research in literature focused on application layer encryption only without considering quality-driven energy efficient delivery of selectively encrypted multimedia in wireless channels. For example, the research in [106] [107] proposed schemes of scrambling significant transform domain coefficients to avoid content fruition by unauthorized attackers or users. Although the carefully designed scrambling techniques might alleviate the known-plaintext or chosen-plaintext attacks to the secret multimedia content, UEP-based transmission optimization can hardly be applied to the encrypted code stream because it is difficult to separate important encrypted media packets from other unimportant packets by scrambling. The research proposed in [101] [102] [103] combined multimedia encryption and entropy coding using Multiple Huffman Table (MHT) alternately in a pseudo random secret order; the authors claimed to achieve reasonable level security and unaffected compression efficiency simultaneously. However, a recent publication reported in [104] presented chosen plaintext attacks on the basic MHT scheme and the enhanced method with randomized bit insertion. Recent reported research in [108] also performed comprehensive cryptanalysis on MHT-based multimedia encryption approaches, showing their vulnerability to known-plain-text and chosen-plain-text attacks. Some other research has been proposed to encrypt the partially selected set of transform domain coefficients (such as DCT or wavelet coefficients) [98] [99] [100], in order to reduce the total encrypted data overhead. But the semantic meaning of the multimedia content can still be acquired from the low quality encrypted images, since the coefficient energy concentration is not equivalent to the image perceptibility. Wavelet zero-tree and quad-tree-based partial encryption approaches proposed in [97] encrypted and hid the tree structure information in the two highest pyramid levels, which is crucial to image decoding processes. Without these encrypted crucial parts, i.e., code stream structure information, the semantic meaning multimedia content cannot be acquired even with large amounts of plain-text unimportant data. However, none of these aforementioned multimedia encryption schemes jointly considered the application layer security and network transmission efficiency. Since multimedia selective encryption may significantly change the code stream structure and introduce a new packet decoding dependency graph, traditional UEP-based resource allocation schemes are no longer suitable for such scenarios.

6.1.2 Application of Position-based Selective Encryption

A. Position-based Selective Encryption

In this chapter, we propose a new secure resource allocation framework integrating the selective encryption idea in a position-value manner [50] [51]. We extend the selective encryption to an entropy coding stage such as Arithmetic Coding (AC), which is easily implemented according to EZW, SPITH or EBCOT in the JPEG2000 standard. This approach also makes UEP-based network resource allocation easily applied to the selectively encrypted images.

In previous chapters, we proposed a new position – value based UEP paradigm. Since P-V diversity is an inborn feature of multimedia content itself, exploring this dominant feature in selective encryption provides significant foundations for designing secure multimedia streaming in low cost sensor networks. In this dissertation, we use wavelet coded digital images as illustrative examples of multimedia. Following our previous studies proposed in [109] [110] [111], several terms used in this chapter are re-defined as follows. Figure 6.1 illustrates the concept of these basic terms.

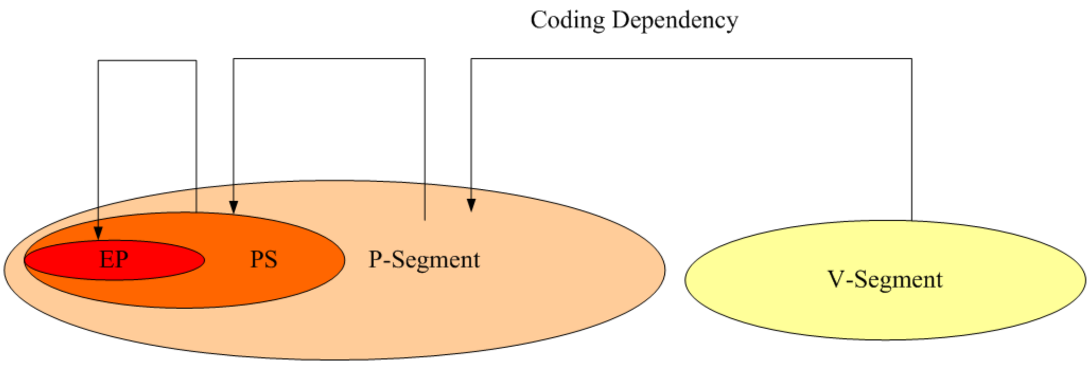


Figure 6.1 PS, EP, p-segment and v-segment in wavelet coded image code stream

Paramount Skeleton (PS): PS is defined as the symbols of the two highest pyramid levels of the significant coefficients in the wavelet coefficient matrix. PS symbols determine whether all the coefficients in the hierarchy of the wavelet tree will be encoded or not, depending on the magnitude value. Hiding PS symbols by encryption can effectively disrupt the zero tree structure or significant propagation determination, which is the paramount operation in the decoding process.

Encrypted Procession (EP): EP information is defined as several beginning PS symbols together with their lengths of runs to be encrypted in each coding bitplane. The symbols and their runlengths in PS have a unique avalanche effect of error propagation. Any single transmission bit error in the beginning of PS may cause irreversible position drift or location misalignment, leading to high difficulty of further symbol decoding. Hence, these tiny parts of EP data in the PS can strongly control the compressed image code stream structure, which has significant potential to reduce encryption overhead for real-time selective encryption. It should be noted that the maximum length of EP equals the length of residing PS.

P-segment: The output of P-V partition – symbols denoting the position information of significant coefficients created in each bitplane coding loop. P-segments determine the code stream structure that is crucial for decoding and image reconstruction. The PS in each bitplane is a subset of the p-segment in the same bitplane.

V-segment: The output of P-V partition –magnitude symbols of wavelet coefficients created in each bitplane coding loop. V-segments determine the magnitude refinement for each wavelet coefficient reconstruction. V-segments do not determine the code stream structure.

In the proposed selective encryption and resource allocation approach, the compressed code streams of one digital image are first partitioned into p-segments and v-segments according to the methodology presented in Chapter 4. Then the PS symbols in each p-segment are encrypted selectively by controlling the length of the EP blocks. Finally, the encrypted code stream is transmitted in WMSN, and encryption aware network resource allocation is applied to improve image transmission quality and enhance energy efficiency by unequally protecting the EP, p-segments and v-segments.

B. Skeleton Encryption with P-V Partitioning

In the proposed selective encryption scheme, the input digital images are first processed with wavelet based transform and P-V partitioning in compression as described in Chapter 4. Then the PS information is identified in the p-segments and EP blocks are encrypted using strong block encryption algorithms. The proposed selective encryption scheme is illustrated in Figure 6.2. Since the EP blocks only occupy a small portion of the whole compressed code stream, this selective encryption scheme can significantly reduce the encryption overhead while providing high level security via the strong block encryption algorithms. Without the structure information residing in p-segments, the magnitude value information in v-segments will be put in the wrong position of wavelet coefficients matrix upon decoding, leading to significant perception distortion. Moreover, the small portion of PS information determines the structure of each p-segment and hence the whole code stream. Modification or encryption of the PS information successfully scrambles the positions of wavelet coefficients associated with those PS symbols. Finally, due to the avalanche error propagation effects, any single crack error in EP leads to irreversible symbol position drift in PS, making the positions of further decoded wavelet coefficients erroneous and useless. In the proposed scheme, the code words of EP symbols after entropy codebook lookup are encrypted by standard encryption algorithms, rather than the encryption of EP symbols themselves, which may reduce compression efficiency. The EP after selective encryption forms encrypted EP blocks. Thus, encrypting the tiny amount EP symbols in each PS and p-segment can efficiently protect the stream structure, leading to high difficulty of image reconstruction without a cipher-key. Due to the significantly reduced encryption workload overhead, this proposed selective encryption approach can also make feasible both symmetric-key encryption algorithms such as AES [112] or TEA [113], and time-consuming public-key algorithms such as RSA [114] or ECC [115]. Thus, the proposed position-based selective encryption scheme is encryption algorithm independent and significantly reduces encrypted data bits. This approach can also address the key-exchange problem [109], since it significantly reduces overhead.

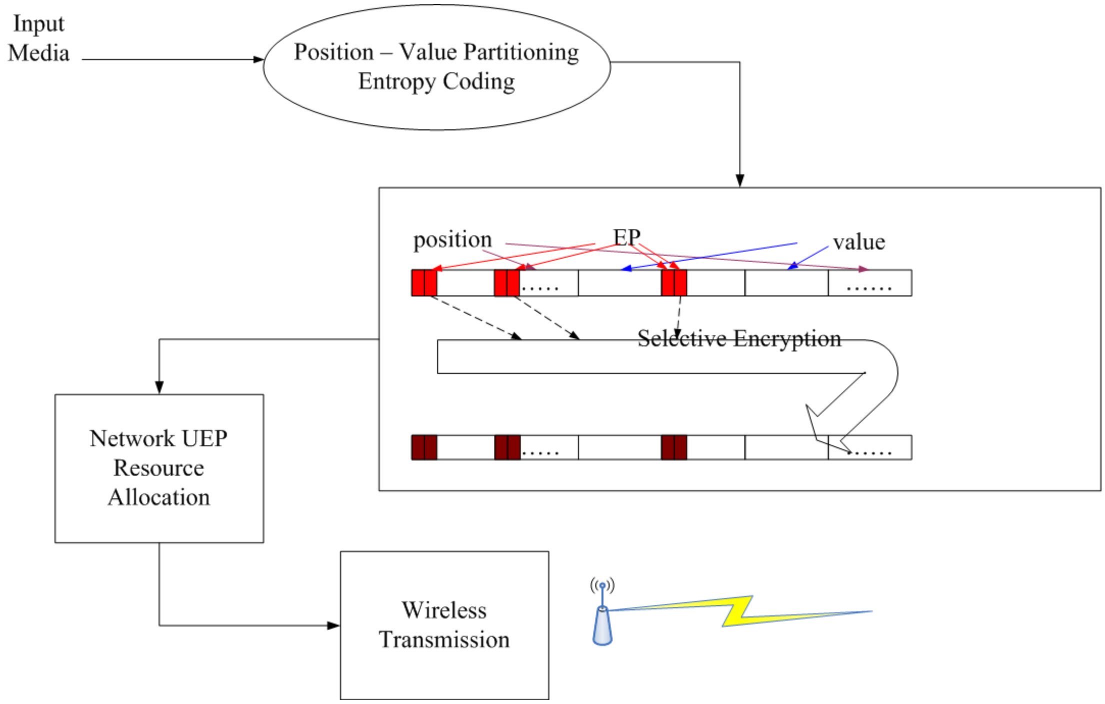

Input Media
Position – Value Partitioning Entropy Coding
position
EP
value
Selective Encryption
Network UEP Resource Allocation
Wireless Transmission

Figure 6.2 Proposed selective encryption and resource allocation framework

The original code words of EP blocks are reconstructed after EP block decryption upon decryption processes, and the symbols as well as their run-lengths are determined from the entropy code book. PS symbols are also reconstructed and p-segments are recreated according to decoded EP information in each bitplane decoding. Eventually, the p-segments and v-segments of all the bitplanes are decoded and the wavelet coefficients are reconstructed. The EP blocks are crucial for image decoding and reconstruction, and valid EP information is provided through correctly decrypted EP blocks conveyed in the encrypted code stream. Attacks using falsified and fake cipher keys may lead to significantly different code words in EP blocks, as well as erroneous PS symbols and p-segments. Decoding of this wrong location and position information provides false positions of wavelet coefficients and extremely distorted images.

6.2 Unequal Energy-Quality-Encryption Control

6.2.1 Resource Allocation with Encryption Consideration

Multimedia selective encryption reshuffles the inter-packet dependency and correlation, which significantly changes the code stream structure. The traditional layer-based packet dependency analysis and the corresponding network resource allocation schemes are not suitable for such new transmission paradigm. It is natural that selective encryption be considered in network resource allocation, because the encrypted EP blocks scramble the code stream structure. Moreover, the EP blocks, p-segments and v-segments have different perceptional distortion importance. Typically, the EP blocks are more important than p-segments, because the decoding of p-segments depends on PS symbols, and the decoding of these PS symbols depends on correct decryption of the associated EP blocks. In addition, the p-segments dictating the code stream structure are much more important than the v-segments, as the decoding of v-segments depends on the correct decoding of p-segments in the current and previous bitplanes. Figure 6.2 shows the joint privacy and quality control-based UEP framework of the secure image delivery over wireless sensor networks. Unlike traditional UEP approaches that only target media quality, energy efficiency and privacy are also considered in the proposed encryption-aware resource allocation scheme. In the proposed scheme, the transmission data rate is individually optimized for energy efficiency in a way similar to [109] [110]. The different network resource control parameters such as physical layer desirable BER requirements (translated from optimal transmission power control) and link layer packet ARQ retry limits are allocated unequally to each EP block, p-segment or v-segment, in order to further improve energy efficiency while providing image quality and security assurance. The energy consumption of transmitting this image and the distortion of the reconstructed image are both related to these parameters. By allocating more resources to EP blocks as well as p-segments, and less effort to v-segments, valuable network resources are more efficiently utilized.

The joint privacy and quality protection problem can be formulated as a distortion reduction maximization problem with energy consumption constraints, where selective encryption is considered in the distortion analysis. The total expected distortion reduction after image decoding and decryption can be expressed in terms of transmission packet loss ratios for each EP block, important p-segment and unimportant v-segment, respectively. Let N denote the number of code stream layers, and Δd_p and Δd_v denote the distortion reduction of the p-segment and v-segment. Let g denote the corresponding packet loss probability in transmission. Let N_B denote EP block count, $\overline{E_B}$, $\overline{E_p}$ and $\overline{E_v}$ denote the energy consumption of transmitting one link layer packet of EP block, p-segment and v-segment, respectively. Also, let $B_k = \{0,1,2,.....\}$ denote the *k-th* EP block set containing the indices of encrypted p-segments associated with that EP block. The total expected distortion reduction $\varepsilon[\Delta D]$ of the reconstructed image can be expressed as

$$\begin{aligned} &\varepsilon[\Delta D] \\ &= \sum_{i}^{N} \left(\begin{aligned} &\left(\sum_{j}^{i} \Delta d_p(j) \right) \cdot g_p(i+1) \\ &\cdot \prod_{j}^{i} \left((1-g_p(j)) \cdot \prod_{k|j\in B_k} (1-g_B(k)) \right) \end{aligned} \right) \\ &+ \sum_{i}^{N} \left(\begin{aligned} &\left(\sum_{j}^{i} \Delta d_v(j) \right) \cdot \prod_{j}^{i} (1-g_v(j)) \cdot g_p(i+1) \\ &\cdot \prod_{j}^{i} \left((1-g_p(j)) \cdot \prod_{k|j\in B_k} (1-g_B(k)) \right) \end{aligned} \right) \end{aligned} \tag{6.1}$$

The average packet loss ratio and distortion reduction measurement of each segment can be expressed in close forms in terms of desirable BER, ARQ retry limit [110], and thus the total expected distortion reduction can also be expressed using these resource allocation parameters. Let E_{MAX} denote the energy budget constraint. The overall optimization problem can be formulated as follows [110]:

$$\begin{aligned} &\{BER\,(i), M_{MAX}\,(i), R_{DATA}\,(i)\}_{i\in\{EP\}\cup\{p-segment\}\cup\{v-segment\}} \\ &= \arg\max \left\{\varepsilon[\Delta D]\right\} \end{aligned} \tag{6.2}$$

Subject to the energy constraint:

$$\sum_{i}^{N_B} \overline{E_B}(i) + \sum_{i}^{N} \overline{E_p}(i) + \sum_{i}^{N} \overline{E_v}(i) \le E_{\max} \tag{6.3}$$

The quality-driven secure resource allocation problem can be solved by finding the desirable BER, ARQ retry limit and transmission data rate for each EP block, p-segment and v-segment, respectively. The objective function is to achieve maximized overall distortion reduction after decryption.

6.2.2 Solutions and Simplification

In the proposed resource allocation scheme, the communication resources are allocated unequally among different image packets, and the decoding and decryption dependency analysis becomes the key component in solving this problem. Typical image packet decryption and decoding dependency are illustrated in Figure 6.3. It is clear that the EP blocks are more important than p-segments and v-segments, and the distortion reduction contributions of p-segments are much more important than that of v-segments. For example, as we have described in [110] in great detail, two EP block sets are created after selective encryption: $S_1 = \{0,1\}$ and $S_2 = \{2,3\}$. These two sets denote that the EP block1 contains the secret EP information from p-segment0 and p-segment1, and the EP block2 contains the secret EP information from p-segment2 and p-segment3. To let distortion reduction brought by p-segment2 (j=2 in this case, and $2 \in S_2$) contribute to the decrypted and reconstructed image, EP block2 must be delivered without bit errors because of decryption dependency. Regarding the decoding dependency, the p-segment0 and p-segment1 must be transmitted correctly in order for decoding of p-segment2. Otherwise, p-segment2 cannot be correctly decoded due to the decoding dependency or decryption dependency.

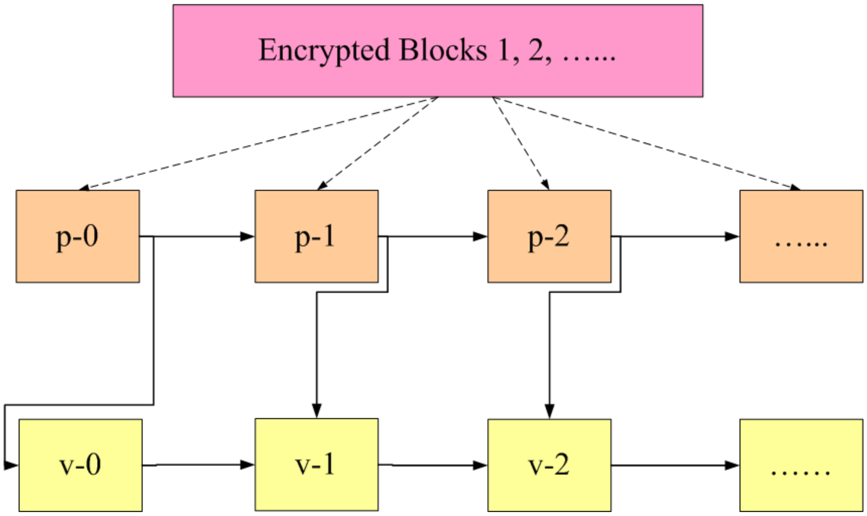


Figure 6.3 Image code stream structure with selective encryption and P-V partition applied

The reconstructed image qualities after decryption, decoding and transmission for erasing different EP blocks, p-segments or v-segment are shown in Figure 6.4. This figure illustrates the unequal importance of EP blocks, p-segments and v-segments in terms of visual distortion effects after transmission in a packet erasing channel. The EP blocks determine the PS symbols of the p-segments, the p-segments contain the structure of the code stream and position information of the wavelet coefficients, while the v-segments contain magnitude value information. The v-segments will not contribute to distortion reduction and decoded image quality alone without p-segments. The p-segments cannot be correctly decoded and reconstructed without correctly decrypting EP and PS symbols. Transmission errors and packet losses in EP blocks or their associated p-segments lead to serious distortion, especially near the important Most Significant Bit (MSB) bitplane. Even in unimportant bitplanes near the Least Significant Bit (LSB), p-segments show around 8-10dB more importance than v-segments in terms of PSNR. Thus, in UEP-based network resource allocation, those secret EP blocks and p-segments deserve more transmission error protection such as low desirable BER requirements and high ARQ retry limits than those less important v-segments. The visualized effects of erasing different EP blocks as well as p-segments and v-segments are also shown in this figure. The packet losses of p-segments or associated EP blocks cause considerable image visual distortion even near the LSB plane, while losing v-segments even near MSB plane still achieves comprehensible image visual effects.

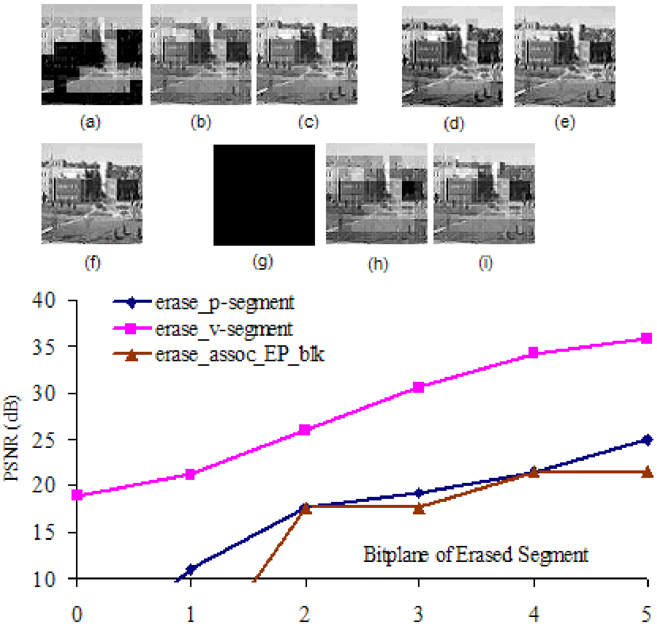


Figure 6.4 Image (“building”) quality with erasing different p-segment s, v-segments or EP blocks in different bitplanes

Note: Visual effect of reconstructed images while erasing different EP blocks, p-segment or v-segment in different bitplanes. (a): erasing p-segment in bitplane 1, PSNR = 10.9829 dB; (b): erasing p-segment in bitplane 3, PSNR = 19.2011 dB; (c): erasing p-segment in bitplane 5, PSNR = 24.8911 dB; (d): erasing v-segment in bitplane 1, PSNR = 21.1707 dB; (e): erasing v-segment in bitplane 3, PSNR = 30.4980 dB; (f): erasing v-segment in bitplane 5, PSNR = 35.8801 dB; (g): erasing EP block 0 associated with p-segments in bitplane 0 and 1, no valid image can be reconstructed (h): erasing EP block 1 associated with p-segments in bitplane 2 and 3, PSNR=17.6615; (i) erasing EP block 2 associated with p-segments in bitplane 4 and 5, PSNR=21.5339;

Given the analysis of the unequal importance in the encrypted image code stream, the UEP-based transmission protection and resource allocation strategy can be efficiently designed to enhance image transmission quality while assuring privacy and energy efficiency. The optimization problem can be effectively solved by generic methods such as genetic algorithms, but the direct application of these algorithms is time- and resource consuming, and hence inapplicable for real-time image delivery in low cost wireless sensor networks. Thus, we propose a simplified approximation methodology by exploiting the inborn unequal importance nature of p-segments and v-segments, as well as the inter-packet dependency between EP blocks and the p-segments and v-segments in the plaintext code stream.

In the proposed approach, the p-segments are grouped together as a resource allocation unit, and the v-segments are grouped into another resource allocation unit. Assigning one set of desirable BER and ARQ retry limit to the p-segment group and another set of those parameters for the v-segment group throughout all bitplanes naturally produces hierarchical packet loss ratio performance. Thus, the layer-based UEP is formed among different bitplanes. It further forms a position-value based UEP paradigm between p-segments and v-segments simultaneously. This is because the packet size in the embedded image code stream is almost naturally increasing with bitplane level. A high bitplane level segment has a larger packet loss ratio, while a low bitplane segment has a lower packet loss ratio [51]. Moreover, the lengths of EP blocks are determined by key size used in the mathematical encryption algorithms, for example, 128 bits in AES, which are typically much shorter than the lengths of p-segments packets. Thus, resource allocation parameters such as desirable BER and ARQ retry limit for EP blocks can be assigned in conjunction with those of p-segments, to reduce the solution search space for optimization [110]. Finally, the UEP between encrypted data and plaintext, the UEP between p-segments and v-segments, and the UEP between different bitplanes are jointly simplified into an output solution vector as $\left[e(p),e(v),m_{\max}(p),m_{\max}(v)\right]$. Through this non-trivial approximation, a simplified solution for providing UEP-based secure image transmission in WMSNs can be designed as Algorithm 6.1, which has been reported in our previous research [110].

Algorithm 6.1 Improve image quality using UEP with encryption and energy efficiency consideration.

Input: The distortion reduction measurement of each p-segment and v-segment packet, the packet size, the channel state factor and the energy budget.
Output: The solution vector in the form of $\left[e(p),e(v),m_{\max}(p),m_{\max}(v)\right]$.

(A): Initialization and performing chromosome coding.

Code each element in the solution vector as a gene and each solution as a chromosome. Initialize the population space size S_{pop} and maximum number of generations $G_{\max}$. Then create the first generation randomly.

(B) Fitness F evaluation of each chromosome according to the distortion reduction expectation $F = \varepsilon[\Delta]$, and sort the chromosome in descending order according to their fitness values. If the energy consumption expectation calculated from the resource allocation strategy is lower than the energy consumption budget, the distortion reduction expectation is used as the fitness evaluation. Otherwise the fitness value is assigned to zero for the corresponding resource allocation strategy.

(D) Crossover of elite parents in the current population, and produce a new population generation.

By denoting the *k-th* chromosome's fitness function as $F(k)$ where $k = 0,1,......S_{pop} - 1$, the probability that one chromosome crossover with others is expressed as $p(k) = F(k) / \sum_{k}^{S_{pop}} F(k)$. Then randomly switch chromosomes to produce a new generation of population with the same size.

(E) If maximal generation count is larger than the maximum number of generations $G_{\max}$, then go to step (F). Else go to step (B) to improve fitness of the newly produced generation.

(F) Output the best chromosome in the current population with the maximum distortion reduction and less energy consumption than the energy budget.

The proposed scheme considerably reduces the size of the possible solution space, and thus makes the solution acquisition process applicable for practical secure image delivery applications in WMSNs. Thus, more communication resources are allocated to important EP blocks containing the secret data and important p-segments containing the position information, and relatively less cost is incurred by putting fewer communication resources on unimportant v-segments containing magnitude value information. The image quality is improved and the privacy is assured while the total energy consumption is reduced.

6.3 Summary

In this chapter we have presented a new quality-driven multimedia selective encryption and resource allocation framework to provide media privacy, media quality and energy efficiency in an integrated solution. First, we have discussed the fundamental theory and methodology of multimedia selective encryption using digital image selective encryption as an illustrative example. We have further proposed a novel position-based digital image selective encryption scheme to cipher the secret positions of important coefficients and to hide the secret code stream structure. The proposed position-based selective encryption scheme significantly reduced the encryption bit overhead, making it desirable for online encryption in low cost sensor nodes.

Moreover, we have analyzed the fundamental relationship between multimedia selective encryption and quality driven network resource allocation, and proposed a new encryption-oriented resource allocation scheme to transmit the encrypted code stream in a cross layer UEP fashion. The important EP blocks and p-segments are transmitted with higher requirements of communication resources to improve the expected image quality, and the unimportant v-segments are transmitted with less communication effort to save energy. The proposed multimedia privacy protection framework is similar to the UIP framework, with stream authentication considerations as presented in the previous chapter.

Both stream authentication and selective encryption change the correlation and packet dependency among the secure code streams. Thus, those traditional UEP schemes without consideration of such additional dependency are not desirable for the new secure multimedia delivery paradigms. In the proposed encryption and resource allocation framework, privacy can be guaranteed and the image quality can be improved, while the energy consumption is bounded.

Chapter 7. Proposed Unequal Control for Multimedia Stream Authentication

With the development of network and digital signal processing, security issues become critical concerns. For example, a content sender may want to ensure that his or her content can only be viewed by authorized users, and content viewers may also want to ensure the received content is indeed from the right sender and that it is not altered maliciously [1]. Authentication answers two inter-related questions: repudiation issues, i.e., who sent the data, and integrity issues, i.e., whether the data has been maliciously modified [1] [2]. Authentication techniques can also be classified into two types: content level watermarking (before compression) and packet level stream authentication (post compression). In this chapter, we will provide an overview of these two major authentication techniques and summarize their advantages and pitfalls.

7.1 Content Watermarking and Stream Authentication

Content-based watermarking [42] [43] [44] [45] has been proposed to protect multimedia copyright and integrity over a long period of time. Watermarking can be classified into two categories according to integrity protection criteria: hard (i.e., fragile) watermarking and soft (i.e., robust) watermarking [59]: Fragile watermarking rejects any modification of multimedia signaling, and robust watermarking typically measures distortion with regard to a threshold for decision-making on the authenticity of challenged signals. It is worth noting that there is typically no sharp boundary between fragile and robust watermarking.

Figure 7.1 shows an illustrative example of the image watermarking process. In this example, the secret authentication data is composed of pseudo-random binary codes generated from a pre-distributed key. A wavelet coefficient matrix is formed after the DWT process is applied to the original digital image. The pseudo-random sequence is then embedded to the middle frequency bands of the wavelet coefficients. Since the pseudo-random sequence is composed of zeros and positive and negative ones, adding these bits to the middle frequency bands will not cause perceptional differences. If the secret data is embedded with the low frequency bands, considerable perceptional distortion will occur; if these pseudo-random bits are embedded with high frequency bands, secret data will be lost during the compression process. In the watermark extraction process, the pseudo-random bit sequence is generated from the same pre-distributed key and applied to the middle frequency band coefficients, typically by multiplicative operations. Because the pseudo-random sequence and the middle frequency band coefficients are statistically non-correlated, only the square values of the secret data are extracted. Media content repudiation can be determined by comparing the extracted watermark to a given threshold value.

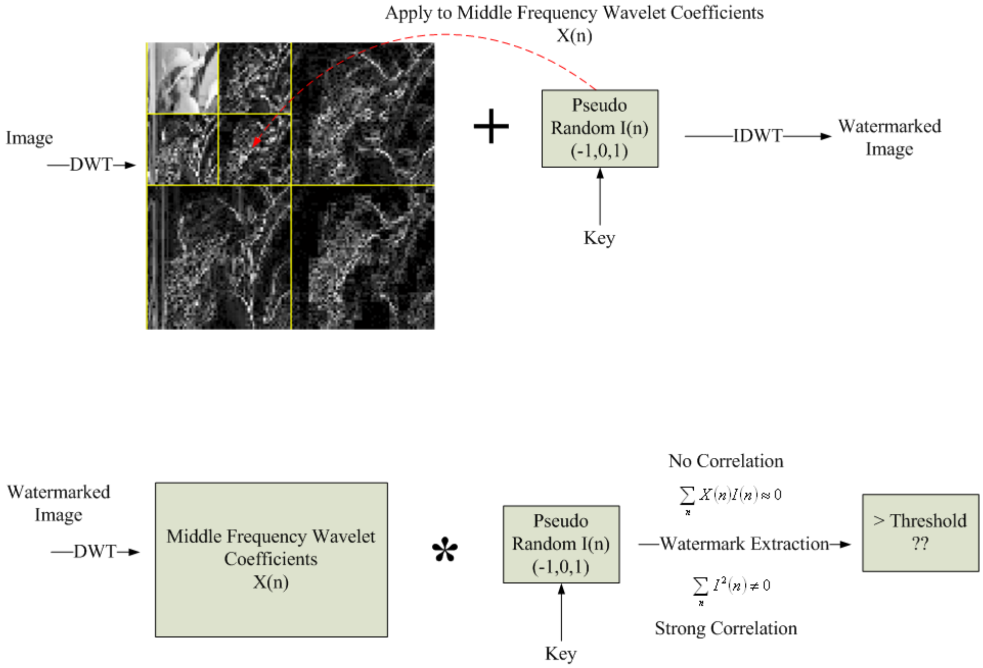

Apply to Middle Frequency Wavelet Coefficients
X(n)
Image
DWT
+
Pseudo Random I(n) (-1,0,1)
Key
IDWT
Watermarked Image
Watermarked Image
DWT
Middle Frequency Wavelet Coefficients X(n)
*
Pseudo Random I(n) (-1,0,1)
Key
No Correlation
$\sum_n X(n)I(n) \approx 0$
Watermark Extraction
$\sum_n I^2(n) \neq 0$
Strong Correlation
> Threshold ??

Figure 7.1 An example of image watermarking

It is clear that watermarking is applied before multimedia compression. Thus, adapting security to time-varying wireless channel conditions is a formidable challenge. Furthermore, watermarking-based content authentication may offer ambiguous authentication results due to the selection of the decision threshold, missing a clear cut between authenticated media and unauthenticated media. Finally, it is generally difficult to make useful and mathematical provable statements about system security, and the security of watermarking-based content authentication is typically low [1]. The advantage of watermarking-based authentication is the low computational complexity due to simple pseudo-random code calculations, as well as little additional bit rate overhead since no additional crypto-hash tags are attached to the media code stream.

Crypto-hash-based stream authentication has been recently proposed [1] [2] to provide multimedia security in lossy networks. It is different from traditional binary data authentication. Traditional binary data authentication offers data security in a strict sense, which is not suitable for wireless multimedia because a simple bit-flip may not change the semantic meaning of multimedia content [2] [3]. Crypto-hash- based stream authentication is more suitable for multimedia delivery over wireless networks, where physical layer symbol errors and link layer packet drops are inevitable. It is also different from traditional watermarking, since stream authentication applies a one-way hash or signature directly on the packets. Thus the verification results have no ambiguity [2]: each received packet is either authenticated or unauthenticated and discarded.

Figure 7.2 shows an example of crypto-hash-based stream authentication applied to multimedia streaming. The packets in the media stream are concatenated and linked together via one-way hash functions such as SHA-1, which takes variable input data length and output fixed length message authentication code. The message authentication code of one packet can be attached to any other packets in the media stream as crypto-hash tags. For packets already having incoming crypto-hash tags attached to themselves, both the packet payload data and the crypto-hash tags are regarded as the input of the outgoing crypto-hash function. A packet is regarded as valid if and only if the packet is received correctly and at least one path leads to the signature packet. Typically only one signature is applied to group of packets (e.g., an image, or a GOP in a video), because the signature signing process is computationally intensive and the signature size is large, while the crypto-hash calculation is much faster and the hash tag size is relatively small. If a packet has no path leading to the signature packet, the verification of this packet has failed. However, if an authentication ancestor packet is lost, the packet may still be verified if any other ancestor packets can bridge this packet to the signature packet.

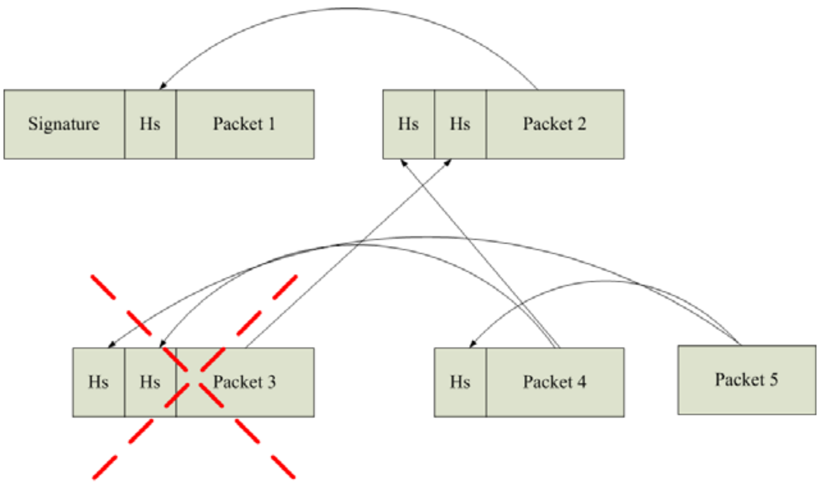


Figure 7.2 An example of crypto-hash-based stream authentication

For example, Packet 1 is the signature packet, and Packet 2 selects Packet 1 as its authentication parent by attaching an authentication crypto-hash tag to Packet 1. Packet 3 and Packet 4 select Packet 2 as their authentication parent. Packet 4 also selects Packet 3 as its authentication parent for robustness improvement. Packet 5 selects both Packet 3 and Packet 4 as its authentication parents. If Packet 3 is lost due to transmission bit errors in the WMSN, the verification of Packet 1 and Packet 2 is not affected since they are in previous authentication levels of Packet 3, i.e., the authentication of Packet 1 and Packet 2 is independent of the successful transmission and verification of Packet 3. Since Packet 4 and Packet 5 select Packet 3 as their common authentication parent, the verification of these two packets from Packet 3 fails. However, these two packets can still be verified in the following way: Packet 4 can be verified by checking the crypto-hash tag attached to Packet 2, and Packet 5 can be verified by checking the crypto-hash tag in Packet 4. This authentication scheme increases the error robustness in packet erasing networks such as WMSNs, with the tradeoff of increasing communication bit rate overhead due to the crypto-hash tags attached to the authentication parent packets, and the extra authentication dependency due to crypto-hash link allocation.

The advantages of crypto-hash based stream authentication are three-fold. First, authentication and verification are applied after compression, which can be designed adaptively to time-varying wireless channels. The authentication scheme and transmission strategy can also be designed jointly in a cross layer fashion to provide media security, media quality and energy efficiency simultaneously. In addition, the security of stream authentication can be mathematically proven since strong and standard DSA and SHA algorithms are applied to signature signing and crypto-hash verification. The stream authentication scheme design is actually allocating crypto-hash links among the packets to build an acyclic authentication graph. Last but not least, stream authentication can offer verification without ambiguity, since each packet can be determined either as authentic and consumed or faked and discarded. The media content in the image or GOP is reconstructed exclusively from these correctly received and verified packets. The disadvantages of stream authentication are the increased communication bit rate due to crypto-hash tags attached to the packet headers and the decreased error robustness due to extra authentication dependency.

Crypto-hash-based stream authentication is applied to the multimedia stream in a post-compression manner. The design of stream authentication scheme is equivalent to designing crypto-hash link allocation algorithms. Since the post compression nature, stream authentication can be generically designed according to decoding dependency with regard to specific codec.

7.2 Unequal Energy-Quality-Authentication Control

7.2.1 Application Layer Authentication

JPEG2000 has been proposed as the latest scalable image compression standard. In this section, we will start with the fundamentals of JEPG2000 coding, and then discuss the applications of stream authentication to the JPEG2000 compressed code stream. The secure image transmission problem will be formulated in a cross layer fashion, and design simplification will also be proposed for practical applications in low cost wireless sensors.

In JPEG2000 image coding, the digital image captured from the camera is first processed by tile forming, where a large image is segmented into a couple of smaller tiles of images. The advantage of this tile forming is error resilience: by means of tile forming, the data encoding and compression are independent among the tiles. If certain bit errors or packet drops occur upon transmission, the decoding errors will be localized and confined in the tile rather than propagate among all the tiles with the avalanche effect. Then the tiled image undergoes the Discrete Wavelet Transform (DWT, or DCT in JPEG codec) process with energy concentrated in the spatially low frequency bands. The wavelet coefficient matrix is further segmented into code blocks to improve error resilience. Similar to tile forming, the decoding errors due to transmission error or packet drops can be effectively confined and localized into the erroneous code block without affecting other code blocks. A tier-1 coding process is applied to each code block in the wavelet coefficients matrix bit plane by bit plane (from the Most Significant Bit, MSB, to the Least Significant Bit, LSB) after quantization. During each bitplane coding loop, each wavelet coefficient quantization sample is encoded in one of the three coding passes: significant propagation, magnitude refinement, and cleanup pass. In a significant propagation pass, if a sample is insignificant (a “0” bit in the current bit plane) but has at least one immediate significant neighbor (at least a “1” bit in the current/previous bit plane), Zero Coding (ZC) and Sign Coding (SC) primitives are invoked according to one of the 19 contexts defined in the JPEG2000 standard. In the following magnitude refinement pass, if a sample is already significant, Magnitude Refinement (MR) primitive is invoked according to the context of eight immediate neighbors’ significant states. In the final cleanup pass, all the uncoded samples in the first two passes are coded by invoking ZC and Run-Length Coding (RLC) primitives according to each sample’s context. The codeword of the samples in these three coding passes are concatenated to the code stream with a marker of rate or size and distortion reduction expectation value. Then a tier-2 coding process is applied to form packets and layers and to perform rate-distortion truncation. The code stream is organized in an embedded way, where there are multiple packets in each layer and multiple layers in the code stream. The decoding of packets is independent among the packets in the same layer, while the decoding of high layer packets depends on the successful decoding of the packets in previous layers.

7.2.2 Unbalanced Resource Allocation

With regard to specific media codec dependency, we can concretize the generic cross layer problem for secure multimedia transmission in WMSNs. Since there are a large number of image packets in the JPEG2000 image code stream, building a complete and global optimal stream authentication graph is computationally intensive, which is unsuitable for low cost WMSN sensor nodes. Furthermore, because of the overlapping graphs of decoding and verification dependency, an image packet must be received, decoded and verified/authenticated to make a distortion reduction contribution to the trustworthy image. Following the symbol definition presented in our work [60], we define the symbols as follows. Let i denote the packet index in one layer and l denote the layer index. Similar to what has been mentioned in previous chapters, let L denote the total number of layers in the compressed image code stream and N_l denote the number of image packets in layer l. Given the distortion reduction $\Delta D_{l,i}$ (i.e., the quality gain if the packet is received and consumed in the decoding process) of the $i-th$ packet in layer l, cumulative packet delivery probability $\theta_{l,i}$ (i.e., the successful delivery probability of the $i-th$ packet in layer l, multiplied by the successful delivery probability of all ancestor packets upon which it depends in decoding), and the verification probability $v(a_{l,i})$ with regard to the crypto-hash parent selection $a_{l,i}$ (i.e., the probability that a packet can be verified, including the successful reception and verification of all the decoding ancestors and authentication ancestors), the expected authenticated and decoded image quality can be re-expressed as follows according to the problem formulated in Chapter 2:

$$\varepsilon[\Delta D] = \sum_{l=0}^{L-1} \sum_{i=0}^{N_l-1} \Delta D_{l,i} \theta_{l,i} v(a_{l,i}) \tag{7.1}$$

The distortion reduction value of each image packet can be heuristically measured as the decoding quality gain in a way similar to [61] [62], or estimated according to the wavelet coefficient square error energy units in a way similar to [4] [5] [49]. Figure 7.3 shows an illustrative example of distortion and rate measure of the well-known "Lena" image, and Figure 7.4 shows the rate (or packet size) measurement. It is clear from these figures that unequal importance is dominant in multimedia streams. Some packets have very short packet size (and thus, very little rate overhead), but the quality gain in terms of distortion reduction is very high. In stream authentication and network resource allocation design, these packets deserve much more communication protection than any other packets. Some other packets with large packet size have very little distortion reduction, and thus the stream authentication and communication protection on these packets can be scaled down to save authentication and energy resources.

The total energy consumption E_{tot} of delivering the compressed and authenticated image code stream can be straightforwardly expressed as the summation of the link layer energy $E_{l,i}$ consumed in delivering each image packet:

$$E_{tot} = \sum_{l=0}^{L-1} \sum_{i=0}^{N_l-1} E_{l,i} \tag{7.2}$$

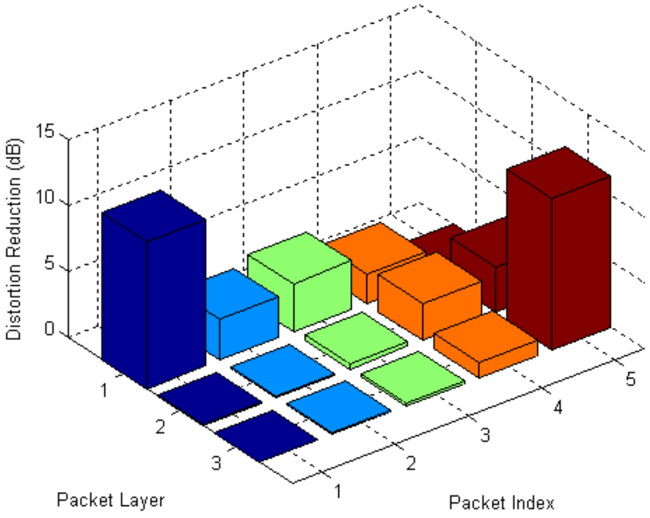


Figure 7.3 Distortion reduction measurement of "Lena" image with JPEG2000 compression

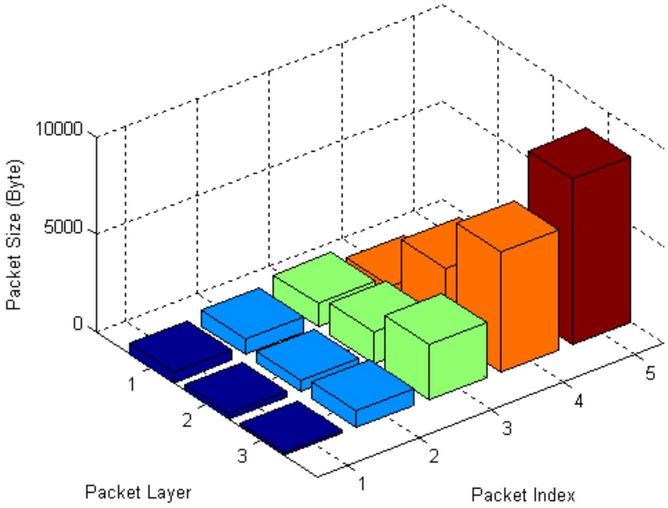


Figure 7.4 Rate (packet size) measurement of “Lena” image with JPEG2000 compression

It is clear from the cross layer problem analysis that the cross layer problem can be decomposed and solved by quantitatively studying three key components: the inborn image decoding dependency, which determines the cumulative packet delivery probability $\theta_{l,i}$ of each packet, the additional authentication dependency determining the verification probability $v(a_{l,i})$ of each packet, and the delivery energy consumption $E_{l,i}$ of each packet in link layer of a WMSN. In this chapter, we focus on the analysis of the inborn decoding dependency and the extra authentication dependency.

7.2.3 Design Simplification

As analyzed in previous chapters and sections, the image packets in the compressed image code stream are inter-dependent due to decoding dependency. It is true that the JPEG2000 decoding dependency leads to decreased error resilience overhead for secure image transmission in WMSNs; however, it also provides considerable potential to simplify the stream authentication design. In fact, the inborn decoding dependency should be considered in the crypto-hash link allocation design of a stream authentication strategy, since a useful packet in terms of authenticated distortion reduction must be decodable and verifiable simultaneously.

Due to the effects of tile forming, code block segmentation and bitplane coding in

JPEG2000 codec, there are multiple decoding independent image packets in one layer and multiple decoding dependent packets across different layers. The decoding of each high layer packet depends on the successful decoding of the packets in the same code block or precinct in previous layers. Thus, it is straightforward to match the authentication crypto-hash link assignment to the natural decoding dependency in a way similar to [4] [3] [60], while significantly reducing the stream authentication complexity: by directly attaching the crypto-hash tag of the high layer packet to the previous layer packet, the authentication rate-distortion performance is optimized [4] and no extra authentication dependency overhead is introduced. This is because the decoding of high layer packets needs the successful decoding of their ancestor packets (i.e., decoding ancestor, not authentication ancestor) anyway. This scheme matches the authentication dependency to the inborn decoding dependency in a natural way.

By means of this non-trivial simplification, the complex stream authentication problem is degraded to a crypto-hash link assignment problem only for layer 0 packets. However, there are still a large number of image packets in layer 0. Checking every possible combination of the crypto-hash link allocation between every two packets is a computational luxury for low cost wireless sensor nodes. To further simplify the stream authentication design, we assume the whole image is signed only once (i.e., only one signature packet in the compressed image code stream) and only one outgoing crypto-hash link is allocated to each packet except the signature packet, which has only incoming crypto-hash link but no outgoing ones. Thus, the outgoing redundancy degree of each packet is fixed to 1 but the incoming redundancy degree is flexible. For example, let Ω_i denote the packet index set of the entire authentication ancestors of the $i-th$ packet in layer 0 plus the packet index of itself. If the crypto-hash message authentication code tag calculated from Packet 4 (i.e., $i=4$) is attached to Packet 2 ($i=2$, i.e., Packet 2 is the authentication parent of Packet 4) and the crypto-hash message authentication code tag of Packet 2 is attached to Packet 0 ($i=0$, i.e., the root signature packet), then the authentication ancestor set of Packet 4 is $\Omega_4 = \{0,2,4\}$. By this further simplification, the authenticated image quality can be re-expressed as follows:

$$\begin{aligned}\varepsilon[\Delta D] &= \Delta D_{0,0} \times \left(1 - \varsigma_{0,0}\right) \\ &+ \sum_{i=1}^{N_0-1} \Delta D_{0,i} \prod_{j\in\Omega_i} \left(1 - \varsigma_{0,j}\right) \\ &+ \sum_{l=1}^{L-1} \sum_{i=0}^{N_l-1} \Delta D_{l,i} \prod_{k=0}^{l} \left(1 - \varsigma_{k,i}\right) \prod_{j\in\Omega_i} \left(1 - \varsigma_{0,j}\right)\end{aligned} \tag{7.3}$$

Then we further analyze the total energy consumption of delivering the authenticated and compressed image code stream. The crypto-hash link assignment in stream authentication introduces extra source bit rate overhead (i.e., packet size overhead) due to multiple attached crypto-hash tag size S_{hash} and signature size S_{sig}, as well as the extra packet authentication dependency overhead. It is clear that the extra bit rate overhead leads to more communication energy consumption due to the increased traffic. The extra authentication dependency overhead has less error resilience and decoding robustness; some successfully delivered packets may not contribute to the image decoding due to the packet loss of their authentication ancestors. Let $\left|\pi_{l,i}\right|$ denote the incoming hash link redundancy degree of the $i-th$ packet in layer l. For instance, Packet 2 in layer 0 has two authentication descendents: Packet 3 in layer 0 and Packet 4 in layer 0 (i.e., Packet 2 is an element in the authentication ancestor set of Packet 3 $\Omega_3 = \{...,2,3...\}$ and Packet 4 $\Omega_4 = \{...,2,4...\}$). The redundancy degree of Packet 2 is then expressed as $\left|\pi_{0,2}\right| = |1+1| = 2$. Based on the above analysis, the total energy consumption reification can be expressed as follows:

$$\begin{aligned}E_{tot} &= E_{0,0}\left(S_{sig} + \left|\pi_{0,0}\right| S_{hash} + S_{0,0}\right) \\ &+ \sum_{i=1}^{N_0-1} E_{0,i}\left(\left|\pi_{0,i}\right| S_{hash} + S_{0,i}\right) \\ &+ \sum_{l=1}^{L-2} \sum_{i=0}^{N_l-1} E_{l,i}\left(S_{hash} + S_{l,i}\right) + \sum_{i=0}^{N_L-1} E_{L-1,i}\left(S_{L-1,i}\right)\end{aligned} \tag{7.4}$$

Now we consider the design simplification of layer 0 packets' crypto-hash link assignment strategy with network resource allocation consideration. Here we just abstractly regard network resource allocation as a black box achieving UEP-based transmission protection for authenticated and compressed image packets. Since there are multiple independently-encoded image packets in layer 0, building a global optimal stream authentication graph is computationally intensive and extremely impractical for low cost wireless sensors. Assuming that network resource allocation is applied to the authenticated and compressed image code stream, we propose a simple greedy stream authentication scheme [3] [60] to reduce computational complexity and achieve minimal extra authentication dependency overhead. The greedy authentication scheme is illustrated in Figure 7.5.

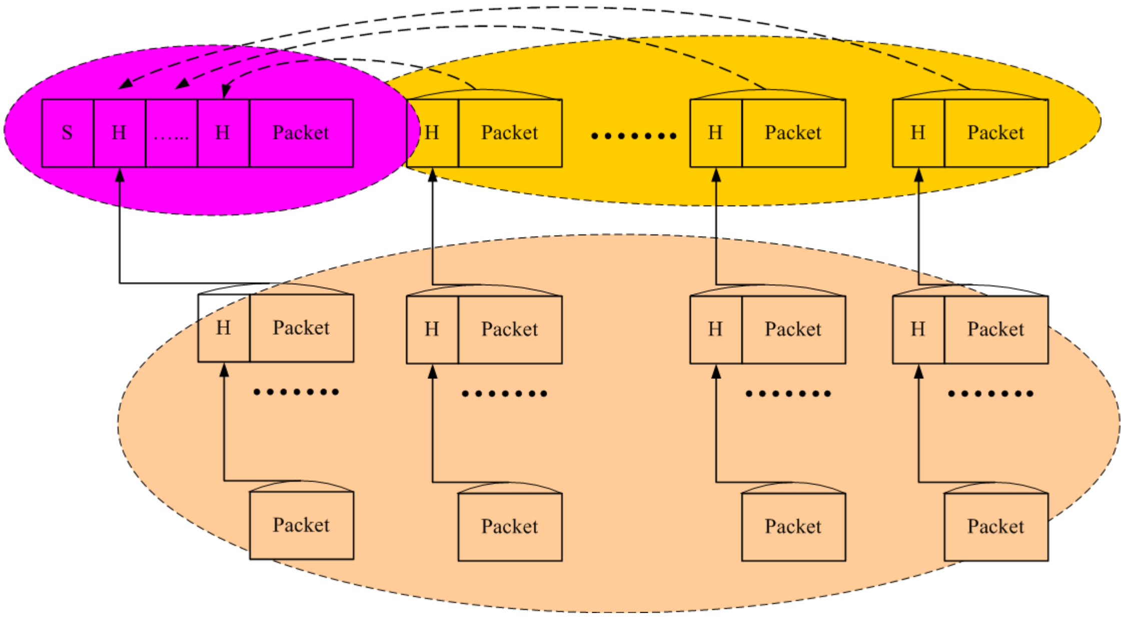


Figure 7.5 Stream authentication illustration and greedy authentication of layer 0 packets

In the proposed greedy authentication scheme as described in our previous research [3] and [60], the crypto-hash message authentication code tag of each layer 0 packet is attached to a parent packet leading to the maximum verification probability of the packet itself without considering any other layer 0 packets' choices, i.e., $Maximize\{v(a)\}$. The concept of greedy stream authentication is that the decision of authentication parent selection of each packet is simplified by overlooking other layer 0 packets, and thus the complexity is significantly reduced. Because there is no collaboration in the parent selection decision among the layer 0 packets, the extra bit rate overhead to some packets may be very high. Some packets may have a lot of authentication descendent packets, while other packets may have no authentication children or descendents. However, the extra bit rate penalty allocated to some of the packets with a large number of authentication descendents can be fully compensated for by future network resource allocation and transmission protection processes.

In the proposed greedy stream authentication scheme, the crypto-hash link assignment for the $i-th$ packet in layer 0 $a_{0,i}$ is also a recursive process, which includes finding the ancestor packet of the authentication parents until it reaches the root signature packet. Let us denote the final output result of the proposed greedy authentication $a_{0,i}$ for the $i-th$ packet in layer 0 as Ω_i. Observing the image stream structure illustrated in Figure 7.5, we can see that directly picking up the root signature packet as the authentication parent leads to the maximum verification probability of the $i-th$ packet itself, with the selfish tradeoff of decreasing the verification probability of all other layer 0 packets. For example, if the $4-th$ packet in layer 0 selects the root signature packet (i.e., Packet 0) as its direct authentication parent, then the authentication ancestor set for Packet 4 is $\Omega_4 = \{0,4\}$. Assume the wireless channel Bit Error Rate (BER) is e, the payload size (authentication packet payload, including both the protocol header and the actual data payload) of the $i-th$ image packet is S_i. Then the verification probability of the $4-th$ packet transmitted in such channels can be expressed as [60]:

$$v(a_{0,4})|_{greedy} = (1-e)^{S_{sig}+S_{hash}+S_0} \times (1-e)^{S_{hash}+S_4} \tag{7.5}$$

In this equation, the second part of $(1-e)^{S_{hash}+S_4}$ also considers the additional bit overhead S_{hash} due to the incoming crypto-hash link tag attached by high layer decoding and authentication dependent packets. If the $4-th$ packet selects any other packet in layer 0 as its direct authentication parent, for example Packet 2, then in the best case (when $\Omega_2 = \{0,2\}$) the verification probability $v(a_{0,4})$ of Packet 4 will still be lower than that shown in Equation (7.5) due to the packet authentication dependency overhead [60].

$$v(a_{0,4})|_{nongreedy} = (1-e)^{S_{sig}+S_{hash}+S_0} \times (1-e)^{S_{hash}+S_2} \times (1-e)^{S_{hash}+S_4} \tag{7.6}$$

According to the analysis presented in the context of previous equations, the proposed greedy stream authentication scheme can achieve the best effort verification probability in error-prone wireless channels for each layer 0 packet individually with extremely low complexity $O(1)$. The disadvantage of the proposed greedy authentication is the increased authentication bit rate overhead of the signature packet, which may negatively affect the verification probability of the whole image stream when the signature packet size is very large. However, this disadvantage can be easily compensated for by network resource allocation, which is discussed in the next chapter. With consideration of network resource allocation, the root signature packet deserves the best transmission protection since the image is non-verifiable if the signature is lost due to transmission errors. For all the other layer 0 packets, assigning the outgoing hash link directly to the signature packet in this greedy way introduces minimal authentication dependency, because the signature packet will be protected with best effort anyway, and no other packets are involved in the verification process.

Now we discuss how to perform UEP-based energy-constrained network resource allocation with stream authentication consideration. It is straightforward to achieve the global optimum of multimedia quality maximization with energy constraint by adjusting the network transmission parameters for each image packet in each layer. However, there are typically a large number of packets in each quality layers and there are multiple layers in the compressed multimedia stream, leading to a large search space and considerable computational complexity. Mathematical optimization in such a large space and typically high dimensions consumes time and resources, which is extremely undesirable for secure image streaming in side and energy- constrained WMSNs. Thus, reasonable simplification and approximation should be considered in designing such resource-constrained optimization problems. We can practically design a simplified evolution algorithm to approximate the global optimum, by studying the overwhelmingly dominating factors in network resource allocation and the stream authentication dependency as well as the decoding dependency in the following aspects.

First, efficient multimedia packet classification is performed according to the Quality of Service (QoS) importance and authentication dependency. Since there are a large number of packets in the code stream, and multiple packets may have similar decoding or authentication importance, these packets can be classified and grouped into the same QoS category. A single resource allocation parameter is assigned to each category instead of assigning each packet an optimization parameter. By means of QoS categorization, the dimension of search space is reduced a great deal and the optimization complexity is significantly reduced. According to the stream authentication schemes proposed in the previous section, for example, the greedy authentication, the packets in the code stream can be categorized into three QoS classes: the signature packet, the layer 0 packets without signature, and the high layer dependent packets. The packets in the same QoS class have similar transmission importance in terms of stream verification and stream decoding. In other words, the packets in the same QoS class reside in similar positions of the decoding graph and authentication graph. Thus, assigning a single network transmission parameter to the packets in the same QoS class is a fair and reasonable compromise to all the packets in the same class. This scheme can significantly reduce the dimension of the solution space and the optimization complexity. As reported in our recent research [60], the proposed greedy-based stream authentication and resource allocation algorithm is shown as follows:

Algorithm 7.1: Simplified Energy-Constrained Resource Allocation for Stream Authentication and Secure Media Transmission.

1. Definition of the algorithm I/O.

Input parameters: input media code, the number of quality layers L in the code stream, the numbers of packet N_l in each quality layer, the channel state factor A, the size $S_{l,i}$ and distortion reduction $\Delta D_{l,i}$ of each code stream packet, where $l \in \{0,1,...,L-1\}$, and $i \in \{0,1,...,N_l-1\}$.

Output parameters: Near-optimal transmission power control triplet $\{P_{t(0,0)}, P_{t(0,1)}, P_{t(1,1)}\}$ of the three packet QoS classes.

2. Crypto-hash based stream authentication. Perform greedy stream authentication to the compressed code stream. Assign signature to the first packet and crypto-hash tags to each packet except the last layer packet. Calculate the incoming redundancy degree $|\pi_{l,i}|$ for

each packet in each layer. Also let $:=$ denote the assignment operation and $=$ denote the equality judgment.

If $l = 0$ and $i = 0$ Then $\chi := 1$; Else $\chi := 0$;

Update the size of each image packet with authentication consideration.

$S_{l,i} := S_{l,i} + |\pi_{l,i}| \times S_{hash} + \chi \times S_{sig}$;

3. Packet classification. Perform packet classification, categorize packets into three QoS classes, and translate the power control triplet $\{P_{t(0,0)}, P_{t(0,1)}, P_{t(1,1)}\}$ to desirable BER expectation $\{e_{(0,0)}, e_{(0,1)}, e_{(1,1)}\}$. Associate the desirable BER triplet $\{e_{(0,0)}, e_{(0,1)}, e_{(1,1)}\}$ to the three packet QoS classes and perform genetic-based chromosome coding. Initialize the population with size K for the first iteration. Initialize the iteration indicator $g := 0$ and the maximum iteration limit $G_{\max}$. Randomly create the first population.

For $k = 0$ to K do: $\{e_{(0,0)}(k), e_{(0,1)}(k), e_{(1,1)}(k)\} := rand(0,1)$;

4. Loop iteration. Start the evolution loops to increase the fitness values of chromosomes.

```
If $g < G_{\max}$ Then:
  Perform iteration of step 5-7; $g := g + 1$;
Else:    Go to step 8.
```

5. Metric calculation. The metric here is the expectation of the authenticated distortion reduction and total energy consumption. For each element $\{e_{(0,0)}(k), e_{(0,1)}(k), e_{(1,1)}(k)\}$ in the current population K, evaluate the authenticated distortion reduction expectation $\varepsilon[\Delta D](k)$ and the energy consumption expectation $E_{tot}(k)$ of transmitting the authenticated code stream.

6. Fitness evaluation. Evaluate the fitness value $f(k)$ for each element in the current population. Let α denote a very small constant value to slightly relax the energy constraint and $f_{\min}$ denote a very small constant value of the minimum fitness limit.

If $E_{tot}(k) \le E_{\max} + \alpha$ Then: $f(k) := \varepsilon[\Delta D](k)$;

Else: $f(k) := f_{\min}$;

7. Crossover. Sort the chromosomes in the current population in descending order according to the value of $f(k)$. Calculate the crossover probability $p(k) = f(k) / \sum_{i=0}^{K-1} f(i)$ of each elite parent in the sorted population. Randomly crossover the chromosomes $\{e_{(0,0)}(k), e_{(0,1)}(k), e_{(1,1)}(k)\}_{current}$ in the current population, and produce a new population $\{e_{(0,0)}(k), e_{(0,1)}(k), e_{(1,1)}(k)\}_{next}$ for the next iteration. Go to Step 4.

8. Output results. Algorithm is finished. Output the desirable BER triplet $\{e_{(0,0)}, e_{(0,1)}, e_{(1,1)}\}$ in the final population with the highest fitness value f, and translate desirable BER in the chromosome into power control triplet $\{P_{t(0,0)}, P_{t(0,1)}, P_{t(1,1)}\}$.

7.3 Disproportionate Stream Authentication to P-V Stream

7.3.1 Problem Analysis

Following the joint stream authentication and resource allocation problem formulated in Chapter 2, the application of stream authentication and cross layer resource allocation to P-V partitioned image code stream transmission in sensor networks can be formulated as an energy-constrained quality maximization problem, where all the image packets are decoded exclusively from those authenticated packets. Let N denote the total number of bitplane layers in the embedded code stream, $\Delta_p(j)$ and $\Delta_v(j)$ denote the distortion reduction of the $j-th$ p-data segment and the $j-th$ v-data segment, respectively. A detailed discussion of generic distortion reduction acquisition and applications in cross layer optimization can be found in [4] [5] [49] [61] [62]. Also let $\rho_p(j)$ and $\rho_v(j)$ denote the packet loss ratio of the $j-th$ p-data and v-data segment, respectively. Let

$v_p(j)$ and $v_v(j)$ denote the verification probability of the $j-th$ p-data and v-data segment, respectively. Let $\varepsilon[\Delta]$ denote the expectation of total authenticated distortion reduction, which can be expressed as follows in a way similar to [16] [51] with consideration of authentication dependency:

$$\begin{aligned}\varepsilon[\Delta] = &\sum_{i=0}^{N-1}\left(\sum_{j=0}^{i}\Delta_p(j)\right)\prod_{j=0}^{i}(1-\rho_p(j))\prod_{j=0}^{i}v_p(j)\rho_p(i+1)+\\ &\sum_{i=0}^{N-1}\left(\sum_{j=0}^{i}\Delta_v(j)\right)\prod_{j=0}^{i}(1-\rho_p(j))\prod_{j=0}^{i}(1-\rho_v(j))\prod_{j=0}^{i}v_v(j)\rho_p(i+1)\end{aligned} \tag{7.7}$$

It is clear to see that each packet itself must be transmitted correctly, and all the decoding ancestors as well as all the authentication ancestors must be transmitted correctly to make a distortion reduction contribution to the reconstructed and authenticated image. Since $\rho_p(i+1)=1$ denotes the truncation end of embedded bit stream, the expected distortion reductions of p-data segments can be expressed as the summation of the weight $\sum_{j=0}^{i}\Delta_p(j)$ with the corresponding probability $\prod_{j=0}^{i}(1-\rho_p(j))$ for successful decoding and verification $\prod_{j=0}^{i}v_p(j)$ of each p-data segment, which is also related to the next layer truncation probability $\rho_p(i+1)$. Since each v-data segment depends on all p-data segments in previous and current bit planes, as well as all v-data segments in previous bit planes, the distortion reduction expectation of v-data segments part can be expressed as the summation of the weight $\sum_{j=0}^{i}\Delta_v(j)$ and the successful decoding probability $\prod_{j=0}^{i}(1-\rho_p(j))\prod_{j=0}^{i}(1-\rho_v(j))$ and the verification probability $\prod_{j=0}^{i}v_v(j)$ of each v-data segment. This equation gives the close form expression of the expected distortion reduction, which can serve as the objective function of the proposed quality-driven stream authentication and resource allocation optimization algorithm. From the decoding and verification dependency, we can roughly see that without decoded and verified p-data segments, v-data segments can hardly make any contribution to image reconstruction. This observation leads to the significant potential that putting more authentication and communication protection efforts on p-data segments and less effort on v-data segment can enhance the reconstructed image quality without excessive energy consumption overhead.

The energy budget constraint function can also be expressed in close form. Let $\varepsilon[E]$ denote the energy consumption expectation of delivering the whole compressed image code stream. Also let $\overline{E}_p(i)$ and $\overline{E}_v(i)$ denote the average energy consumption of delivering the p-data segment and v-data segment in the $i-th$ bit plane respectively. Then the total energy consumption of delivering the whole image bit stream can be expressed in the following equation [51]:

$$\varepsilon[E] = \sum_{i=0}^{N-1} \left(\overline{E}_p(i) + \overline{E}_v(i) \right) \tag{7.8}$$

The quality-driven stream authentication and resource allocation problem for P-V partitioned code stream can also be formulated in the same way as stated in Chapter 2. Let $a_p(i)$ and $a_v(i)$ denote the crypto-hash link parent selection strategy of the p-data segment and v-data segment in the $i-th$ bit plane. Let $\eta_p(i)$ and $\eta_v(i)$ denote the resource allocation strategies (such as desirable BER e , ARQ retry limit $m_{\max}$, and transmission data rate R, etc, i.e. $\eta = \{e, m_{\max}, R, ...\}$) of the p-data segment and v-data segment in the $i-th$ bitplane, respectively. The desirable BER has been widely used in wireless networking research as an optimization parameter such as [66] [67], which can be physically translated into the optimal transmission power in a certain channel loss condition. The hash-link allocation strategy a can fine-tune the additional authentication dependency and rate overhead, while the resource allocation strategy η can fine-tune the average loss ratio ρ and the average energy consumption $\overline{E}$ of each p-data and v-data segment. Let $E_{\max}$ denote the energy budget for the whole image transmission. The optimization problem can be formulated as follows:

$$\{a_p(i), a_v(i), \eta_p(i), \eta_v(i)\}_{i \in \{0,1,2,......,N-1\}} = \arg\max \left(\varepsilon[\Delta] \right) \tag{7.9}$$

Subject to the following constraint,

$$\varepsilon[E] \leq E_{\max} \tag{7.10}$$

7.3.2 Design Simplification

There are multiple packets in each bit plane and multiple bitplanes in the compressed code stream. Thus, designing a complete and accurate crypto-hash authentication graph is computationally intensive, which is unsuitable for low cost wireless sensors. However, the stream authentication design can be significantly simplified by considering the codec dependency. For an image packet (i.e., the current packet) consumed by the decoder, all the decoding ancestor packets and authentication packets must be correctly transmitted. If one of the decoding ancestor packets is corrupted due to wireless channel errors, the current cannot be decoded due to the decoding dependency. If one of the authentication ancestor packets is lost, and no other path leads the current packet to the signature packet, then the verification of this packet fails. The design of the crypto-hash link allocation problem can be simplified to the problem of designing an authentication dependency graph that matches the decoding dependency graph.

The proposed crypto-hash based stream authentication with regard to P-V partitioning dependency is illustrated in Figure 7.6. After compression and position-value partitioning, the decoding of each p-data segment depends on the successful decoding of all the p-data segments in previous bit planes. The decoding of each v-data segment depends on the successful decoding of all the p-data segments and all the v-data segments in previous bit planes, as well as the successful decoding of the p-data segment in the current bit plane. Thus, it is straightforward to assign signature to the first position packet (denoted by P0) because it is the decoding root of the whole code stream. Without Packet P0, all the other position and value packets become useless in terms of decoding.

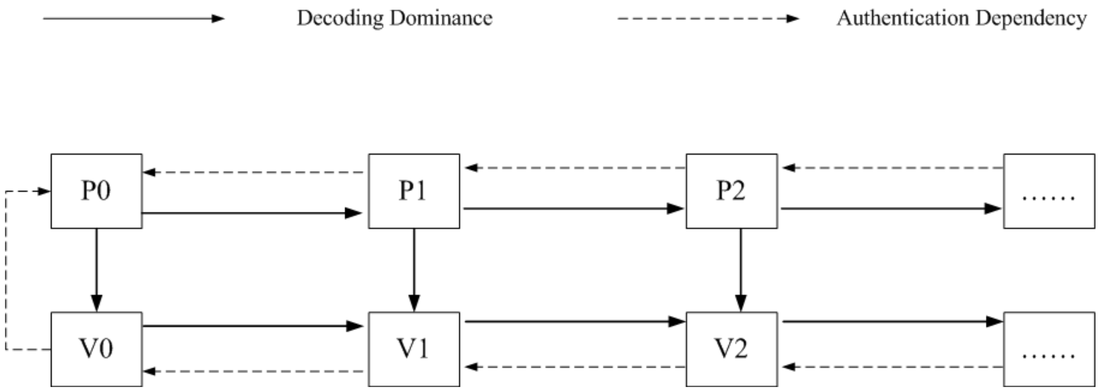


Figure 7.6 Proposed stream authentication with regard to packet decoding dependency in a position-value partitioned code stream

Since the decoding of each p-data segment depends on the successful decoding of all the p-data segments in previous bit planes, allocating the crypto-hash message authentication tag of the current packet to one of its decoding ancestors introduces no further authentication dependency. Furthermore, assigning a crypto-hash message authentication code tag to the parent node (i.e., the direct decoding ancestor node) achieves minimum error-resilience overhead to other packets. For example, consider the crypto-hash tag assignment for Packet P2. Because both Packet P0 and Packet P1 are the decoding ancestor packets of P2, assigning a crypto-hash tag to either one incurs no additional authentication dependency. Assume channel BER is e, S_{sig} and S_{hash} are the signature and crypto-hash tag sizes, and $S_p(i)$ denotes the p-data segment in the $i-th$ bit plane. If the crypto-hash tag is assigned to P0, then the verification probability of packet V0 is shown as follows:

$$v_v(0)|_{indirect} = (1-e)^{S_{sig}+3S_{hash}+S_p(0)} \times (1-e)^{S_{hash}+S_v(0)} \qquad (7.11)$$

From this equation, we can see that the verification probability of packet V0 is actually determined by the packet loss ratio of the packets in the authentication path leading to the signature packet. Signature packet P0 has two crypto-hash tags from packets P1 and V0, and one additional tag from Packet P2. If the crypto-hash tag of P2 is assigned directly to P1, the verification probability of Packet V0 can be expressed as follows:

$$v_v(0)|_{direct} = (1-e)^{S_{sig}+2S_{hash}+S_p(0)} \times (1-e)^{S_{hash}+S_v(0)} \tag{7.12}$$

It is clear that the verification probability of V0 is unnecessarily affected by indirect crypto-hash tag allocation. By directly allocating a crypto-hash tag of P2 to P1, the verification probability of V0 is improved. This simple example shows the advantages of direct assigning a crypto-hash tag to the immediate decoding ancestor packet (i.e., the parent packet) of p-data segments. For crypto-hash tag allocation of v-data segments, the analysis can be performed similarly.

Since each v-data segment has two direct decoding dependent parents (except the V0 packet which only has one decoding parent P0), the stream authentication hash tag allocation problem for v-data segments can be simplified as a choosing one from two problem: either assigning the crypto-hash tag to a p-data segment decoding parent or assigning it to the v-data decoding parent. We propose to assign a v-data crypto-hash tag to a v-data decoding parent because it involves less verification and error-resilience overhead to other p-data packets in lower bit planes. For example, consider the authentication parent selection of Packet V1. The crypto-hash tag of V1 can be attached to the p-data decoding precedent P1 or the v-data decoding precedent V0. Attach the crypto-hash tag of V1 to P1, and let $v_p(1)|_{v2p}$ denote the verification probability of P1 by attaching a crypto-hash tag from v-data segment to p-data segment, and it can then be expressed as follows.

$$v_p(1)|_{v2p} = (1-e)^{S_{sig}+2S_{hash}+S_p(0)} \times (1-e)^{2S_{hash}+S_p(1)} \tag{7.13}$$

If the crypto-hash tag of V1 is attached to V0 other than P1, then the rate overhead of P1 is reduced by S_{hash}, and the verification probability is improved to:

$$v_p(1)|_{v2v} = (1-e)^{S_{sig}+2S_{hash}+S_p(0)} \times (1-e)^{S_{hash}+S_p(1)} \tag{7.14}$$

In summary, , the crypto-hash message authentication code tag allocation in stream authentication should be designed to match the decoding dependency in a P-V partitioned code stream. The crypto-hash tags of high layer p-data segments can be attached to the immediate p-data decoding parent in the previous bit plane, and the hash tags of high layer v-data segments can be attached to the immediate v-data decoding parent in the previous bit plane. The crypto-hash tag of the first layer v-data segment is attached to the first p-data segment in the code stream, to which the signature is also attached.

7.4 Disproportionate Stream Authentication for Video

The proposed quality-driven stream authentication scheme can be seamlessly applied to scalable video coding as long as the inter-packet decoding dependency is known prior to crypto-hash tag allocation. For example, MPEG-4 introduced in 1998 was designated by the ISO/IEC Moving Picture Experts Group (MPEG) under the formal standard ISO/IEC 14496, which was primarily aimed at low bit-rate video applications over networks [68]. The layer-based quality enhancement concept has been widely applied to Scalable Video Coding (SVC) [70] [71] [72] in MPEG-4 Part 10 H.264/Advanced Video Coding (AVC) [73] [74] [75] and JPEG2000 progressive image coding standards. Versatile source coding rates have provided a significant foundation for a large number of emerging multimedia applications over bandwidth- limited wireless networks such as IPTV [76] [77] [78] [79], video on demand (VOD) [80] [81], and online video gaming [82]. The scalable video coding in MPEG-4 is similar to the quality progression in JPEG2000, which provides considerable advantages for error-robust multimedia streaming over time-varying wireless channels, especially in WMSN environments.

The video source contents are typically coded into a couple of quality layers via scalable video coding, starting with the rough pictures in low bit rates, followed by higher layer refinement data for quality enhancement in higher bit rates in a “compress once, decode many times” embedded manner. The rough pictures in the base quality layers are much more important than the refinement data in the quality enhancement layers in terms of perception distortion. Thus the rough pictures deserve more protection upon transmission in wireless channels; the refinement data in enhancement layers can be discarded during transmission when communication resources such as bandwidth or energy are constrained.

Furthermore, the multimedia streaming is composed of inter-dependent packets, and the crypto-hash-based stream authentication can be desirably designed so that the authentication dependency graph matches the decoding dependency graph as close as possible. Typically, the dependency graph of the video stream is composed of packetized group of pictures (GOPs), and the multimedia packet decoding is inter-correlated involving complex dependency among those packets [69]. If a group of video packets is received upon decoding, only the packets whose ancestors have all been received can be decoded. For example, Figure 7.7 illustrates the typical code stream dependency for a layer-based embedded media stream as well as the typical IBBPBBPBBP video stream structure [61] [69].

The inter-packet dependency provides opportunities for stream authentication and resource allocation for secure multimedia streaming over WMSNs, where the packets with more decoding descendents are much more important than those descendents. For example, in the decoding ancestors of the first two B-frames (B0 and B1), the preceding I-frame (I) and the next P-frame (P0) must be successfully transmitted and decoded in order for successful decoding of the first two B-frames. For the successfully decoding of the third and the fourth B-frames (B2 and B3), the I-frame (I) as well as the second and the third P-frames (P0 and P1) must all be successfully decoded.

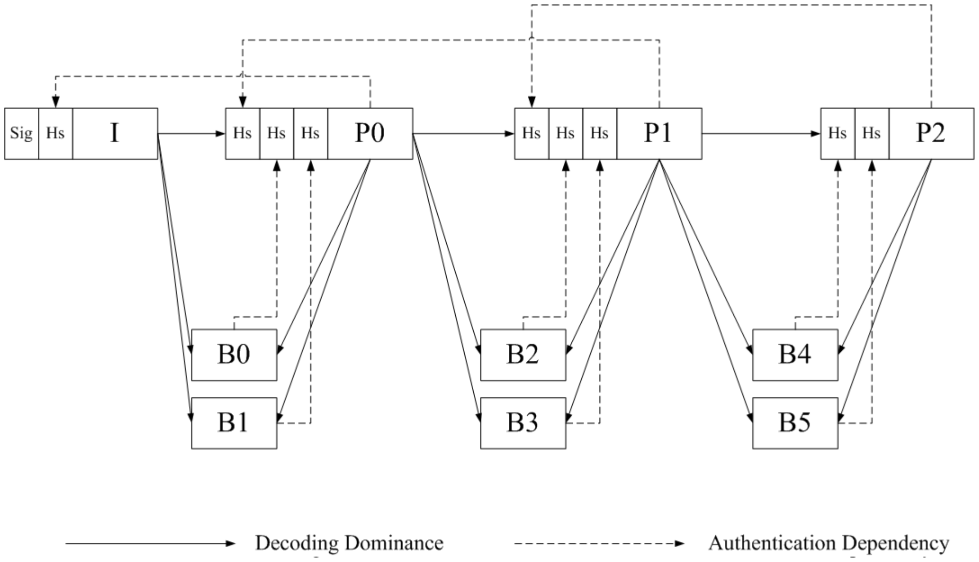


Figure 7.7 Proposed stream authentication for typical packet dependency of the IBBPBBPBBP video stream structure

Based on the analysis of unequal importance and inter-packet dependency, the crypto-hash-based authentication strategies can be efficiently designed to match the decoding dependency. In the proposed stream authentication scheme for video, the crypto-hash message authentication code tag of each P-frame can be allocated to the previous P-frame decoding ancestor. In the first P-frame, however, the crypto-hash tag is directly attached to the I-frame. The signature is also attached to the I-frame, since the decoding of this GOP primarily relies on the successful decoding of this important I-frame. The crypto-hash authentication tag of each B-frame can be allocated to the immediate P-frame decoding parent. For example, the I-frame is selected as the authentication parent of P0, and P0 is selected as the authentication parent of P1, and so on. Frame P0 is selected as the authentication parent of both B0 and B1, and P1 is selected as the authentication parent of B2 and B3.

Network resource allocation will be applied to the hash-chained media streaming according to the distortion reduction (visual importance) of each packet, inter-packet decoding dependency, and authentication dependency. In terms of decoding and authentication, the ancestor packets with more dependent authentication and decoding children packets will be protected with more communication resources, including stronger FEC error correction capability, robust modulation schemes and higher ARQ retry limits, and so on. The authentication and decoding descendent packets with fewer dependent children packets have less protection to save communication energy.

7.5 Summary

In this chapter, we have discussed the stream authentication scheme design at the application layer. We have proposed a cross layer framework with two major components: unbalanced stream authentication and authentication unequal resource allocation. Resource allocation efficiency in terms of energy-quality gain has been improved considerably by considering both decoding dependency and authentication dependency at the application layer as well as channel information and transmission control parameters at lower layers. The stream authentication scheme design has been equivalently translated to the algorithm design of the crypto-hash-based message authentication code tag allocation problem. In this chapter, we have discussed the stream authentication crypto-hash tag allocation using three illustrative codec examples: JPEG2000 image codec, P-V partitioned zero tree codec, and scalable video codec with IBBPBBPBBP coding structure. The decoding dependency of each codec has been analyzed in detail, and the crypto-hash tag allocation algorithm for each codec has been formulated. The proposed stream authentication has also been generalized according to decoding dependency with regard to specific codec due to its post compression feature.

Chapter 8. Results, Analysis and Discussion

8.1 Multi-rate Power and Energy Optimization

Figure 8.1 shows the quantitative relationship between transmission power and the desirable BER in a certain channel environment. Figure 8.2 shows the relationship between transmission power and channel state factors with a certain BER requirement. To achieve lower BER, higher transmission power is needed to increase the receiver- side SNR. On the other hand, if higher BER is acceptable, i.e., the communication quality requirement is relatively low, the required minimum transmission power decreases considerably. From these results we can see that increasing the data rate also increases the required transmission power. However, the power increases much more than the data rate because of the non-linear effect of data rate and power. This illustrates the philosophy that transmitting at a relatively low data rate can achieve transmission power efficiency. Multi-rate power versatility also spurred a revolutionary effort to achieve energy efficient multi-rate transmission in WMSNs through adaptive rate and power control.

Figure 8.3 illustrates that multi-rate transmission with power control can achieve energy savings in different channel conditions, because the optimal transmission data rate is very sensitive to channel state information A. Energy consumption is measured for a TinyOS [94] packet delivered with desirable BER 1e-5 as the communication requirement. In relatively harsh channel conditions, such as subfigures (a)-(c) with larger A values, lower data rate transmissions achieve less normalized energy consumption. On the other hand, in relatively good channel conditions such as subfigures (d)-(f) with smaller A values, higher data rate transmissions are favorable for energy savings. This figure also shows that the desirable transmission data rate with optimally controlled transmission power achieves significant energy efficiency improvement compared with other non-optimized transmission data rates and non-optimally control power supplies in various wireless channel conditions. For example, given the channel state factor -60dB, the worst case transmission rate incurs 5.7271e-5 mJ energy consumption and the sub-optimal rate leads to 5.3999e-5 mJ energy consumption, while the optimal transmission rate achieves 5.3641e-5 mJ energy consumption [51]. Let E_{opt} denote the energy consumption achieved by using the optimized transmission data rate, and let E_{ref} denote the packet transmission energy consumed by using the referenced transmission data rate. Let $\beta = E_{ref} / E_{opt} - 1$ denote the energy efficiency improvement. In this channel condition, the optimized transmission date rate achieves 6.7% and 0.67% energy efficiency improvement with regard to the worst case and the sub-optimal case, respectively [51].

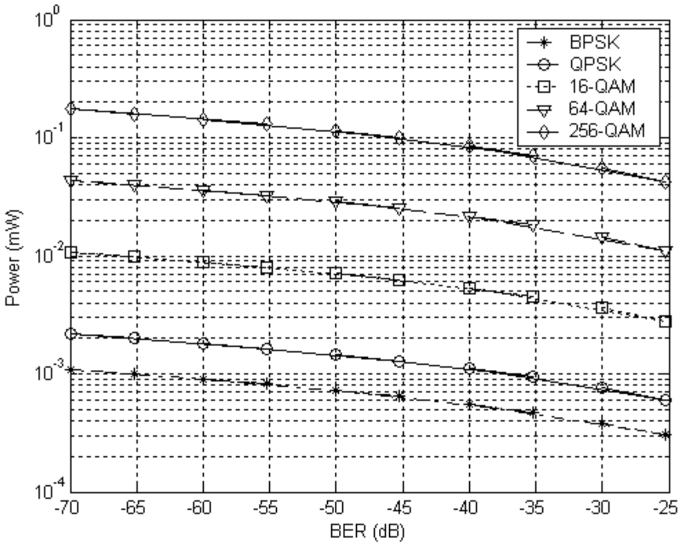


Figure 8.1 Transmission power for different modulation schemes and desirable BER; channel state factor equals -90dB

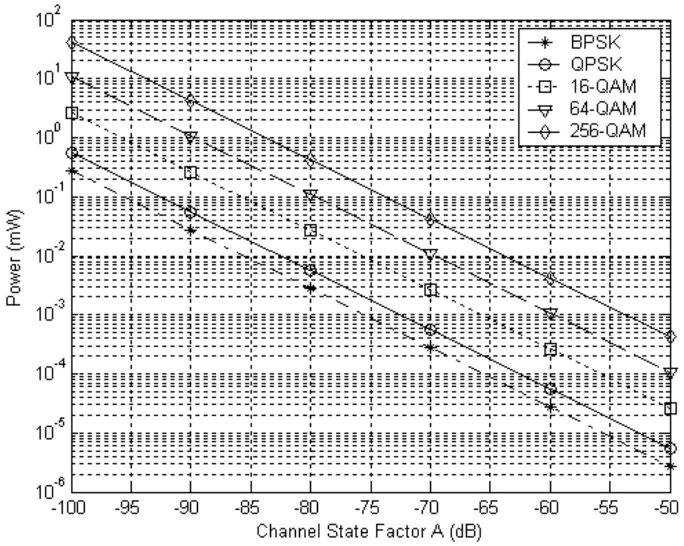


Figure 8.2 Transmission power for different modulation schemes and channel state factors. The desirable BER equals 1e-4

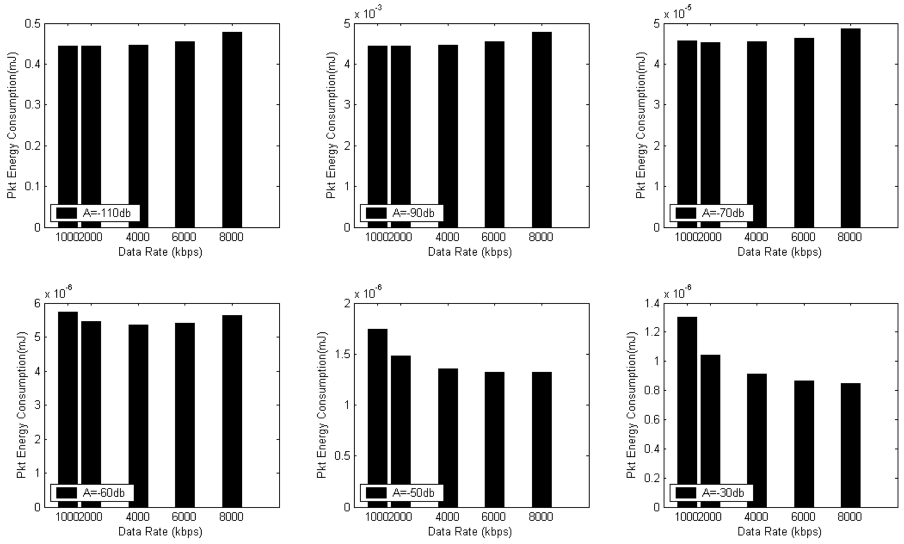


Figure 8.3 Optimal transmission data rate in various channel conditions. Energy consumption is measured for a TinyOS packet delivered with desirable BER 1e-5

From the above analysis, we can see that multi-rate transmission with power control is an effective way to achieve energy efficiency in wireless sensor networks. The layer 2 distortion-energy performance for each packet's delivery can also be fine-tuned by the controlling parameters P_t , b and $m_{\max}$ adaptively to the wireless channel and application attributes. In different wireless channel conditions with various channel loss/gain, the optimal transmission date rate in terms of minimal transmission energy consumption may be quite different. Rate and power, as well as packet retransmission limits, can all be used in network resource allocation for energy-quality performance improvement.

8.2 Position-Value based Unequal Resource Allocation

We have designed simulation scenarios to illustrate the unequal importance of p-data and v-data segments transmitted in wireless channels. We first perform an empirical study to demonstrate the unequal importance between position information and value information. We apply wavelet-coded P-V partitioning to the well-known digital image “Lena” and measure the distortion reduction contribution of each image packet. In the image compression process, there are a total of 8 bitplane layers applied, and position information is separated from value information in each bitplane layer. Hence, there are a total of 16 image packets, with distortion reduction measurements shown in Figure 8.4. It is clear from this figure that the position information is much more important than value information. In general, position packets are the major contributors to decoded image quality. Thus, in network transmission, position information needs more communication resources to improve the decoded image quality, and value information needs fewer communication resources to save total energy consumption in WMSNs.

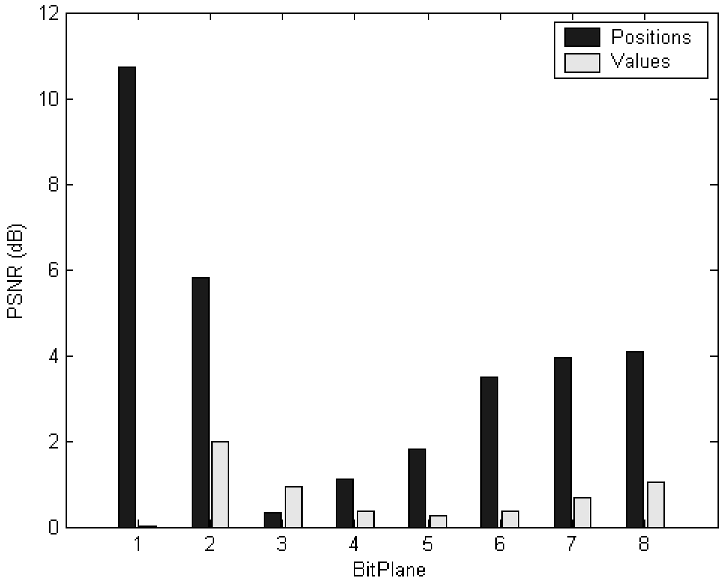


Figure 8.4 Distortion reduction contribution of various position and value packets in the picture of “Lena”

By applying the P-V-based UEP scheme, p-data segments are effectively protected to enhance image quality, while v-data segments are less protected to improve energy efficiency, as shown in Figure 8.5. In this figure, the average loss ratios of all p-data segments and v-data segments with 1:0.3 compression ratio and 0.08mJ energy budget constraint are illustrated in each sub-figure. It is clear that by applying unequal transmission error protection between p-data and v-data segments, the loss ratios of p-data segments containing code stream structure and position information are reduced, while the loss ratios of v-data segments containing magnitude value information are increased compared to traditional layer-based UEP approaches. By applying the packet loss ratios in Figure 8.5 to p-data and v-data segments, we can get the energy-quality performance shown in Figure 8.6 for various compression conditions. Details of the P-V UEP transmission scheme can be found in our previous work [51]. From these simulation results we can see that the energy consumption penalty overhead of more protection on important p-data segments is fully compensated for by less protection on unimportant v-data segments. However, the distortion reduction (i.e., the quality gain) can be enhanced considerably by P-V- based unequal protection.

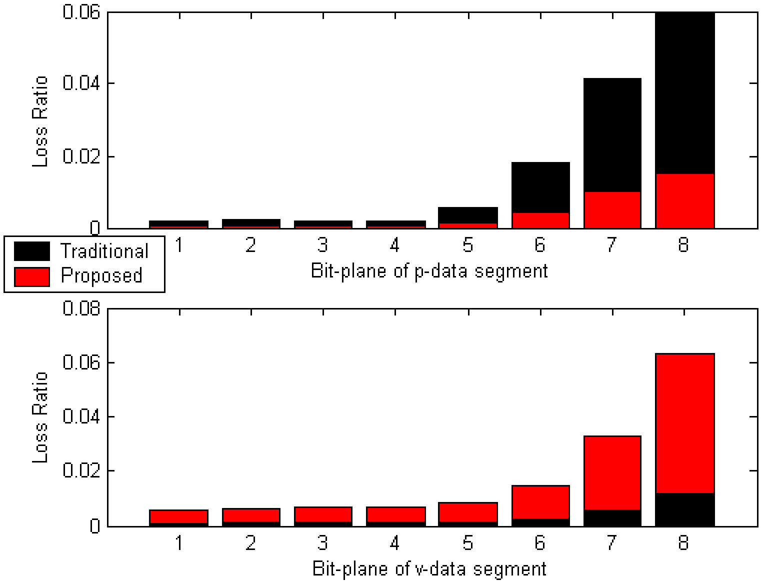


Figure 8.5 Average loss ratio of different p-data segments and v-data segments, with compression ratio 1:0.3 and energy budget 0.08mJ applied to both approaches

The P-V-based UEP approach not only explores unequal importance among different bit planes of the code stream, but also explores the unequal importance between p-data and v-data segments in the same bit plane. As shown in Figure 8.6, the P-V-based UEP scheme can achieve significantly improved distortion reduction gain and reduced energy consumption simultaneously compared to traditional layer-based UEP approaches. Drawing a horizontal line in these figures, we can see that the proposed approach consumes less energy to achieve the same PSNR. With the same energy consumption, the proposed approach can achieve higher distortion reduction [51]. This is because the difference between p-data segments and v-data segments is not considered in a traditional layer-based UEP scheme. These results also strongly support the claim that the p-data segments of higher importance deserve more network resource allocation than less important v-data segments, and the distortion penalty for losing some of the v-data segments can be fully compensated for by applying more communication protection efforts to p-data segments.

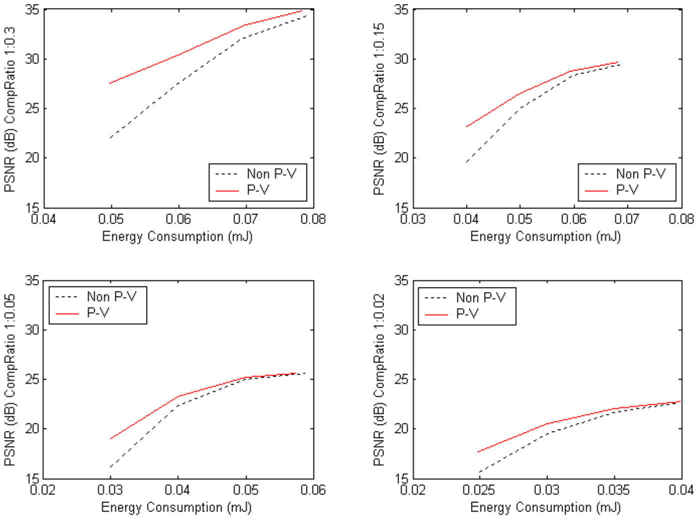


Figure 8.6 PSNR vs. energy consumption for various image compression ratios

In addition, the P-V-based UEP paradigm is especially favorable for strict energy budget constraints with low energy consumption and scarce network resources as well as low compression ratios. For instance, the distortion reductions are very close for both approaches with 0.08mJ energy budget constraint (for compression ratio 1:0.3); with 0.05mJ energy budget constraint, the proposed approach can achieve around 5 dB distortion reduction gain over traditional approaches with regards to our research [51]. This is because the P-V- based UEP can allocate scarce resources on position information other than magnitude value information with strict energy budget constraints. As illustrated in these figures, the image quality gains for the strictest energy budget constraints decrease when the compression ratios increase. The reason is that less magnitude value information and more position information is produced for image code streams with higher compression ratios. P-V-based UEP becomes more efficient with lower compression ratios and less efficient with higher compression ratios.

8.3 Unequal Selective Encryption

The proposed position-based selective encryption has a couple of advantages. First, it considerably reduces encrypted bit overhead. In the proposed approach, the unequal importance between position information and magnitude value information is extensively explored without modifying the compression code stream syntax. All the p-segments conveying position information are identified through the coding pass partition process, but only part of those p-segments is encrypted, significantly reducing the encrypted data. In addition, the entropy coding process in source coding and compression domain can be unaware of the existence of the selective encryption engine, making the selective encryption format compliant. The p-segments containing position information, the PS dictating the structure and the EP information denoting the run-lengths are identified directly from the code stream. The code words of EP symbols are encrypted after looking up the entropy code book. Thus, the compression process is unaltered by selective encryption, and the decryption process is invoked before decompression. Finally, the proposed selective encryption scheme is robust against key space reduction and Bruce-Force attacks. It is independent of mathematical encryption algorithms, and thus strong block-based encryption algorithms using large key-space such as AES can be seamlessly applied to it. It also solves the challenge of the key exchange problem in a wireless network environment by using public-private key systems, because the significantly reduced encrypted bit overhead makes the time-consuming public-key encryption algorithms feasible for low cost sensor nodes.

Figure 8.7 shows the correctly decoded images with encryption keys. The original images are composed of 64*64 or 128*128 pixels and 8 bits per pixel (bpp). The AES standard encryption algorithm is employed with 128 bits block cipher. The number of AES EP blocks can be scaled, with the EP information in coarser bit plane encrypted first, followed by encrypted EP information in finer bit planes [109]. In this simulation, each EP contains the encrypted code words of the first four symbols and their lengths of runs in that bit plane, in the same way as presented in [109] and [110]. Encryption performance evaluation of the proposed selective encryption shows superiority in terms of efficient image protection, compared with sub-band selection algorithms.

Figure 8.7 Sample images used in this study. 64*64 “Building” image, 128*128 “Lena” image, and 128*128 “Barbara” image

The blindly decoded images (without knowledge of the encryption key) are shown in Figure 8.8 – Figure 8.10, for both sub-band selection encryption and P-V based selective encryption in a comparative manner. From these illustrated figures, it is clear that without the correct cipher key for decryption, the blindly decoded images are either unintelligible or reconstructed with considerable distortion. The traditional sub-band selective encryption renders very coarse images by hiding or scrambling low frequency wavelet coefficients. However, the energy concentration in the wavelet coefficient matrix is not directly related to intelligibility, since the decoding code stream structure is not protected. The middle and high frequency coefficients in these schemes are unprotected, which can still provide quite useful information for decoding the images, such as the contours and borders of the objects in the images. On the other hand, the proposed position-based selective encryption significantly reduces encrypted data bit overhead while achieving considerable privacy protection. The proposed scheme protects the code stream structure and the positions of wavelet coefficients in all frequency bands, instead of protecting the large value magnitudes of low frequency coefficients. According to our simulation study, the original image can be effectively protected with encrypting only one block of EP information. The upper row of subfigures show the blindly decoded images via encrypting one to two blocks of coarse bitplane EP information. Those mosaic blocks in the decoded images are due to erroneous position information on significant wavelet coefficients. Without the correctly decoded EP information in coarser (important, close to MSB) bit planes, the correct EP information in finer (unimportant, close to LSB) bit planes can hardly make any quality improvement contributions to distortion reduction [109]. This is the reason why encrypting one or two EP blocks in coarser bit planes can effectively protect the image using the proposed selective encryption scheme. Encrypting more EP blocks in finer bit planes can improve image protection.

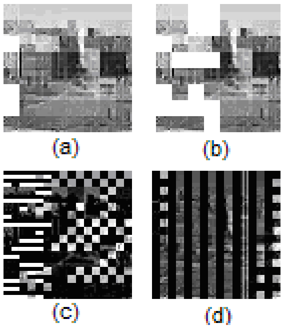


Figure 8.8 Blindly decoded images “Building” without key
(a)-(b) sub-band selection encryption encrypting 1 and 4 AES blocks, respectively. (c)-(d) position-based selective encryption encrypting 1 and 4 AES blocks, respectively.

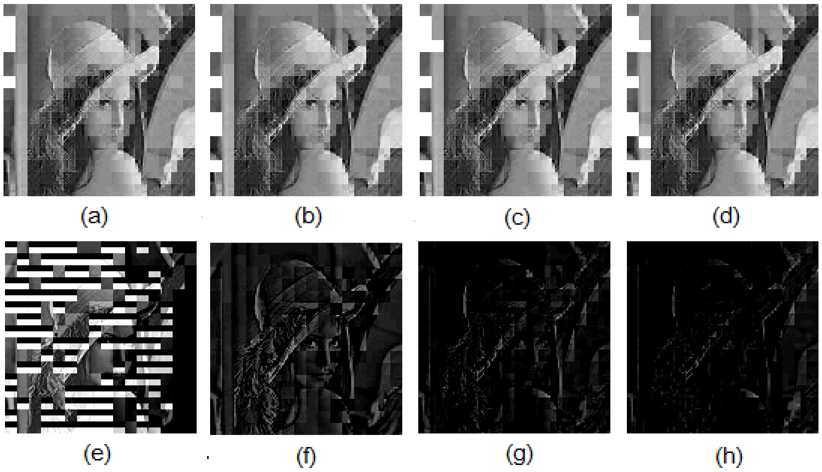


Figure 8.9 Blindly decoded images “Lena” without key
(a)-(d) sub-band selection encryption encrypting 1 to 4 AES blocks, respectively. (e)-(h) position-based selective encryption encrypting 1 to 4 AES blocks, respectively

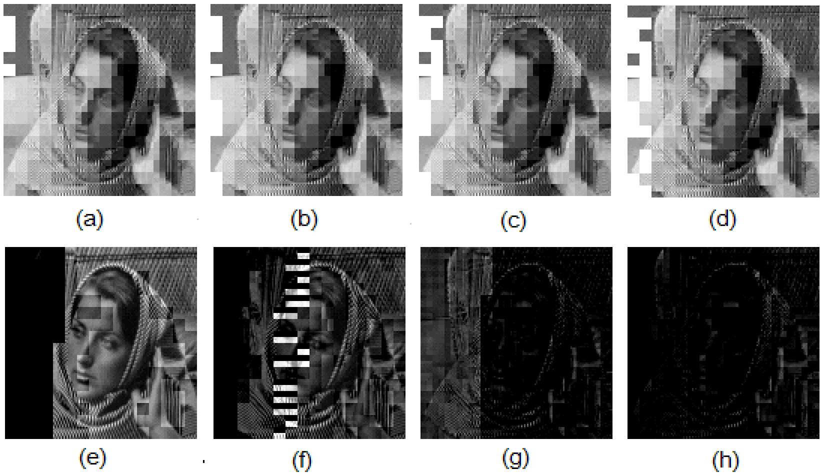


Figure 8.10 Blindly decoded images “Barbara” without key
(a)-(d) sub-band selection encryption encrypting 1 to 4 AES blocks, respectively. (e)-(h) position-based selective encryption encrypting 1 to 4 AES blocks, respectively

The decoded (both blind decoding and decoding with secret key) image PSNR curves for sub-band selective encryption and position-based selective encryption are shown in Figure 8.11. It is clear from this figure that the blindly decoded image PSNR of the proposed position-based selective encryption is lower than that of the traditional sub-band selection-based approach with the same encrypted blocks. This is because the position-based selective encryption scheme effectively protects the code stream structure by hiding PS and EP symbols in a secret manner, and the unimportant information in plaintext cannot make distortion reduction contributions alone without encrypted coefficient position and code stream structure information. In the traditional sub-band-based selective encryption scheme, the code stream structure is left in plaintext without secret protection. The middle and high frequency wavelet coefficients in the coefficient matrix carrying the contour and object boundary information can still render an image with content semantic meanings. These results show that the proposed position-based selective encryption scheme effectively protects the image semantic meaning by hiding a tiny part of the code stream structure. The encryption bit overhead of the proposed scheme is significantly reduced, making in-networking secure image delivery practical in WMSNs.

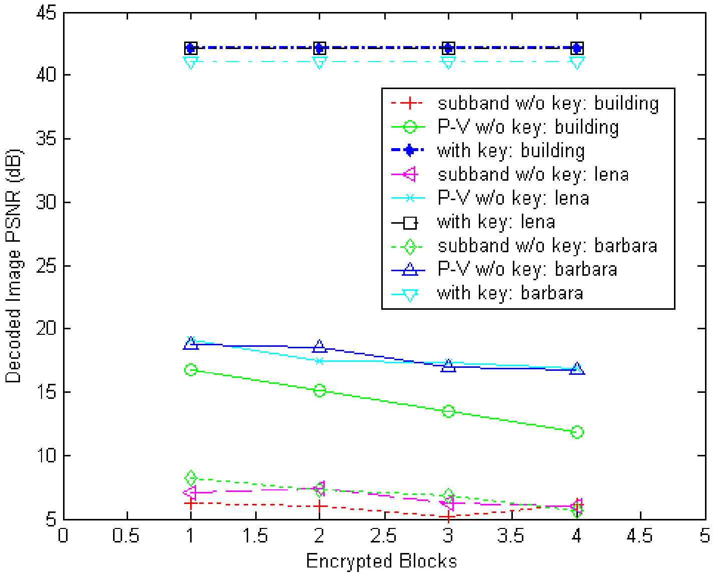


Figure 8.11 Position-based selective encryption and sub-band selective encryption performance: reconstructed image quality with and without AES key

Image quality can be improved considerably while energy consumption is still limited within the budget requirements with the proposed encryption aware resource allocation, compared with traditional layer-based UEP approaches. The quantitative relationship between energy consumption and image quality after transmission is illustrated in Figure 8.12. In this figure, the vertical y-axis denotes the image quality distortion reduction and the horizontal x-axis represents the communication energy consumption. This figure illustrates that the proposed encryption- oriented UEP-based resource allocation can achieve both energy efficiency and enhanced image quality, compared with traditional layer-based UEP approaches. Moreover, the proposed security-aware UEP can further fine-tune the transmission control parameters in network resource allocation more efficiently, especially with strict energy budget constraints. For example, with strict energy budget constraints illustrated in the x- axis in this figure, such as 6e-3mJ and 6.5e-3mJ, the distortion reduction gain of the proposed security-aware UEP approach is around 3dB to5dB, as reported in our research [110].

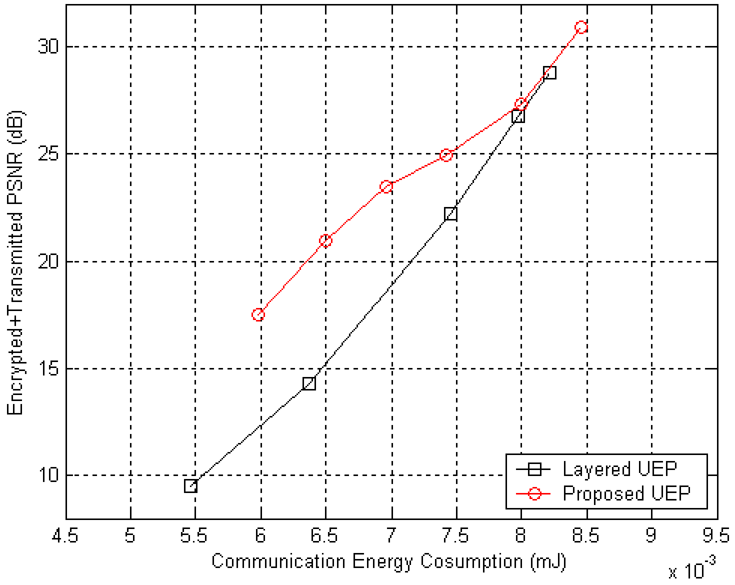


Figure 8.12 Image quality with energy consumption

8.4 Unequal Stream Authentication

To show the energy-quality performance gain of the proposed joint stream authentication and resource allocation schemes, we have evaluated the energy consumption and authenticated distortion reduction performances. We also compare the authenticated energy distortion performance with simple crypto-hash chain-based authentication scheme without resource allocation awareness and Equal Error Protection (EEP) applied. The well-known 256 by 256 pixel "Lena" image is used as an example, and a C/C++ implementation variant of the open source JPEG2000 image compression codec [95] is also utilized in the simulation. Three quality layers are produced in the image stream with compression ratio 30, 35, 40 applied in the JPEG2000 codec. The default progression order is Layer Resolution Component Precinct (LRCP). The SHA-1 scheme is used for crypto-hash tag with a size of 20 bytes, and digital signature scheme is applied to sign the root packet with a 128 byte signature size overhead. The physical layer symbol rate is 1000 kHz and the default channel state factor is -130 dB; the MAC layer frame overhead is 6 bytes and acknowledgement overhead is 8 bytes. The sleep-wake interval in the MAC layer is 0.1 seconds. For transmission power, the control packets transmit at 20 mW, receive power is 15 mW, and the sleep power is 10 uW. For other details, please refer to our recent work reported in [60].

Figure 8.13 illustrates the authenticated image energy-quality performance of the proposed scheme with greedy-based stream authentication and UEP-based network resource allocation. This scheme is shown in comparison with simple crypto-hash chain-based stream authentication and EEP resource allocation schemes. The proposed stream authentication and resource allocation schemes achieve considerable energy-quality performance gain in different scenarios with various energy consumption budgets. In this figure, we can see that the authenticated image quality increases when the energy budget increases for all of these approaches. However, the energy-quality gain of the proposed approach is especially prominent with strict energy budgets. When strict energy budgets are applied to resource-constrained secure image transmission, the UEP-based schemes can schedule communication resources more efficiently by allocating more communication resources to authentication, and decoding important packets such as the root signature packet and other layer 0 packets. In the EEP-based scheme, all the packets in the code stream are equally protected without differentiating importance. When loose energy budgets constraints are applied to the system, communication resources become abundant. The energy-quality performance of the proposed greedy authentication plus UEP resource allocation approaches, and traditional chain-based authentication plus EEP-based approach, is similar.

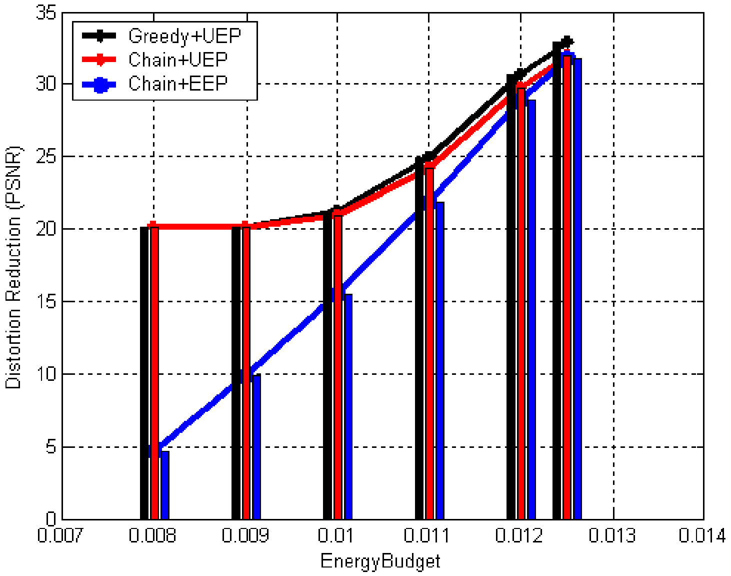


Figure 8.13 Authenticated image quality and energy budget for compression ratio 30:1

The relationship between different energy consumption budgets and the actual energy consumption for all these schemes is shown in Figure 8.14. It is clear from this figure that for different energy budget scenarios, the actual energy consumption is close to the energy budget for all the compared approaches, illustrating the fairness of the comparison. All these compared algorithms can maximize their authenticated distortion reduction performance by approaching their energy consumption limits. Although the energy consumption costs are close in this figure, the authenticated image quality gains are quite different: the energy-quality gain of the proposed stream authentication and resource allocation scheme is attributed to the robust greedy authentication with resource allocation awareness and the UEP-based resource allocation that efficiently and smartly allocates communication resources.

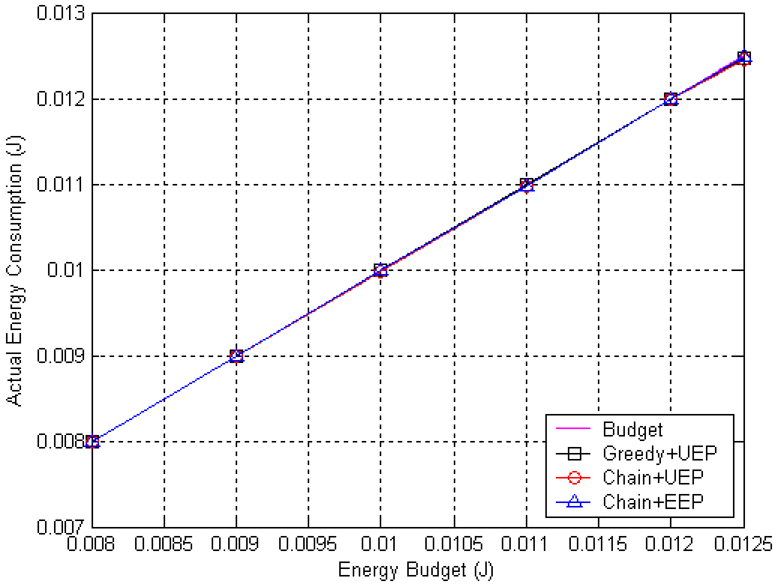


Figure 8.14 Actual energy consumption and energy budget for compression ratio 30:1

Stepping forward into the cross layer secure resource allocation schemes, we can state that there are two major reasons for overall energy-quality performance improvement. First, the proposed greedy-based stream authentication is error robust and resource-allocation aware. The additional packet authentication dependency overhead is much lower than simple chain-based authentication. The packet verification of the proposed greedy-based authentication only depends on the root signature packet. Although the size or bit rate overhead of the root signature packet is increased due to multiple attached hash tags from other layer 0 packets in the proposed greedy authentication, the inter-packet authentication dependency overhead in greedy authentication is reduced considerably, which effectively compensates for the increased bit rate overhead of the root packet. On the other hand, the verification of each image packet depends on the successful decoding and verification of both the root signature packet and the precedent authentication packets in the simple crypto-hash chain-based authentication scheme. If any one of these precedent packets is lost due to transmission error, the current packet will be discarded due to decoding or verification failure. Secondly, the proposed UEP-based network resource allocation scheme can desirably protect the crypto-hash signed code stream by exploring both the inborn decoding dependency and the extra authentication dependency. The root signature packet and other layer 0 packets are protected with more communication energy effort to ensure successful delivery, thus increasing the expectation of authenticated image quality. The other less important high layer packets are less important in terms of both decoding and verification. These packets are protected with less communication effort to save energy resources without too much image quality scarification or degradation.

Figure 8.15 and Figure 8.17 show the energy consumption and authenticated distortion reduction performances for different image compression ratios. Figure 8.16 and Figure 8.18 show the corresponding energy consumption in comparison to the energy budgets. In these figures, we can see that the proposed authentication aware UEP-based resource allocation scheme is very effective in achieving energy-quality performance gain. This performance gain is even large in combination with the simple crypto-hash chain-based stream authentication scheme. In the UEP-based scheme, the packet distortion importance and the packet decoding dependency, as well as the additional authentication dependency, are all studied. Although the simple crypto-hash chain-based stream authentication scheme introduces much more authentication dependency overhead, the proposed UEP-based transmission in cross- layer fashion still compensates for the robustness disadvantages. It is also clear from these figures that the total energy consumption of the image transmission is close but within limits of the energy budget. By utilizing a similar amount of communication energy, the energy-quality performance can be significantly improved by the proposed stream authentication and resource allocation scheme.

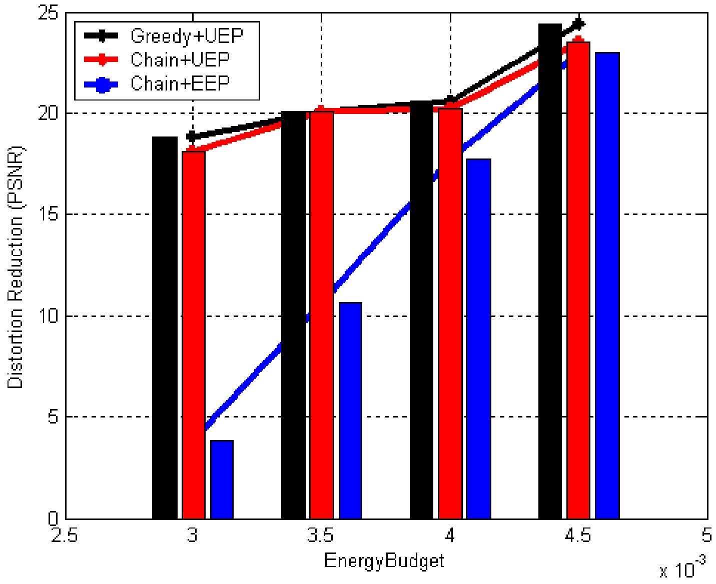


Figure 8.15 Authenticated image quality and energy budget for compression ratio 35:1

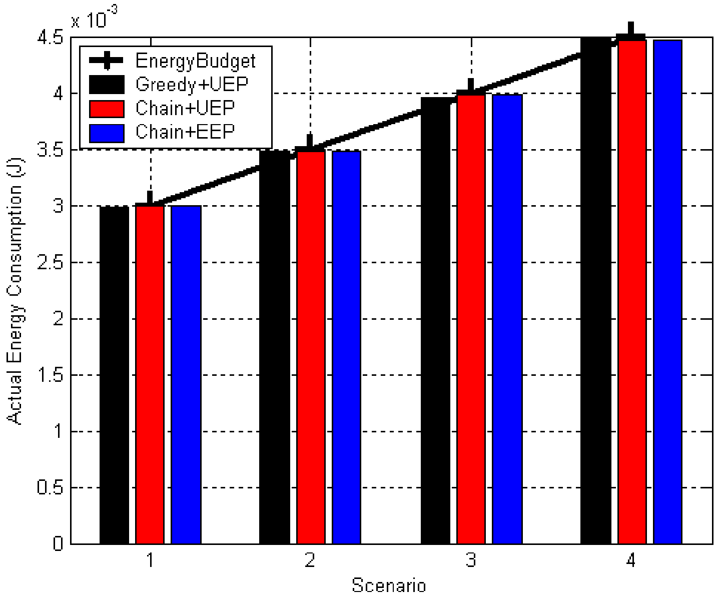


Figure 8.16 Actual energy consumption and energy budget for compression ratio 35:1

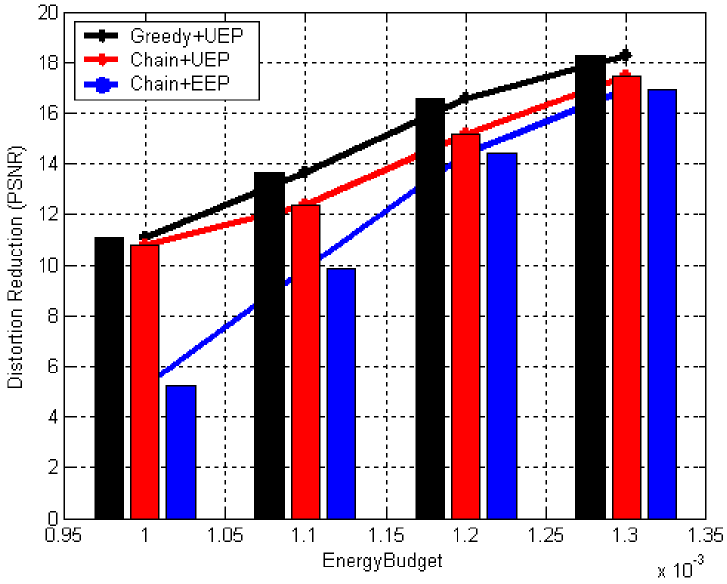


Figure 8.17 Authenticated image quality and energy budget for compression ratio 40:1

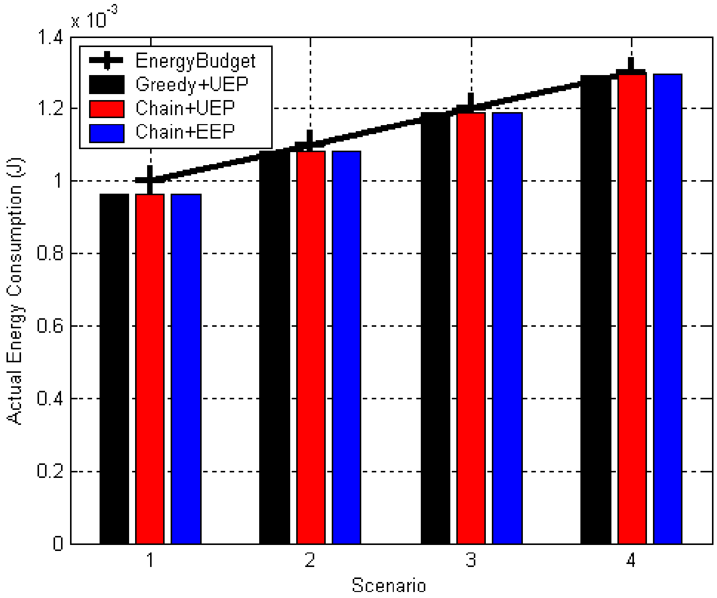


Figure 8.18 Actual energy consumption and energy budget for compression ratio 40:1

Chapter 9. Conclusion

In this dissertation, we have addressed the resource-constrained secure multimedia transmission problems in wireless multimedia sensor networks. The major focus of this dissertation is on providing quality-driven multimedia privacy/integrity protection by means of network resource allocation with energy efficiency assurance.

We have generically formulated the quality-driven secure multimedia transmission problem in WMSNs as a quality maximization problem with security requirements and energy budget constraints. The secure quality expectation maximization in lossy wireless channels is achieved by means of selective encryption and stream authentication design at the application layer, and the network transmission control including rate and power adaptation at low layers. Then we have started solving this generic-formulated problem with the fundamental analysis of the recently proposed multimedia encryption and authentication techniques.

The quality maximization problem has been analyzed with the consideration of encryption/authentication dependency and decoding dependency. The theory and methodology of selective encryption and stream authentication application to various multimedia codec have been discussed in detail. In the compressed multimedia code stream, different packets have different decoding perceptional importance in terms of distortion, and the decoding of some packets depends on the successful decoding of their ancestor packets. Stream authentication introduces extra packet verification dependency in addition to packet decoding dependency due to crypto-hash tag allocation. Traditional UEP-based resource allocation schemes are not desirable for the new secure media transmissions in WMSNs due to the introduced verification dependency. In the proposed stream authentication and network resource allocation framework described in this dissertation, this new verification dependency has been extensively studied with regard to JPEG2000 image codec, P-V partitioned zero tree codec, and typical video codec, respectively. We have also studied the fundamental relationship between multimedia selective encryption, and proposed a new position-based selective scheme to reduce encryption bit overhead. We have proposed a new encryption-aware resource allocation approach to improve media quality with privacy and energy consumption budget assurance.

In the proposed cross layer network resource allocation scheme, the link layer energy consumption and packet delivery performance have been modeled with regard to network transmission strategies such as transmission data rate and transmission power control. The packet transmission distortion and transmission energy consumption have been modeled to represent the transmission data rate and transmission power of each packet. Thus, the important packets in terms of distortion and decoding are transmitted with higher communication efforts to improve the media quality, and the unimportant packets are transmitted with fewer protection strategies to save energy consumption.

Multimedia security and service quality, as well as sensor network energy efficiency, are all challenging issues in cross layer design. The quality-driven energy efficient secure communication framework proposed in this dissertation has a significant impact on the applications of secure multimedia-based wireless sensor network technologies, such as battlefield surveillance and assistance, ubiquitous healthcare monitoring, transferring sensitive media-enriched data, and so on. The design space of network resource allocation algorithms has also been expanded from the network transmission domain to the media quality domain and the security domain as well. By considering multimedia stream authentication and selective encryption, as well as the importance of inborn multimedia packet decoding dependency packet distortion reduction, media service quality can be significantly improved and multimedia security can be provided with bounded communication energy consumption overhead.

Contributed Academic Publications Resulting from the Dissertation Research:

The research results in this dissertation have been published in the following IEEE transactions, journal and conference papers:

- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "A Multimedia Quality-Driven Network Resource Management Architecture for Wireless Sensor Networks with Stream Authentication," *IEEE Transactions on Multimedia (TMM)*, In Print. 2009.
- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "Cross layer Multi-rate Interaction with Distributed Source Coding in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications (TWC)*, vol. 8, no. 2, pp. 787-795, Feb. 2009.
- W. Wang, D. Peng, H. Wang, H. Sharif, "An Adaptive Approach for Image Encryption and Secure Transmission over Multi-rate Wireless Sensor Networks," *Special Issue on Distributed Systems of Sensors and Applications, Wireless Communications and Mobile Computing Journal (WCMC)*, John Wiley & Sons, vol. 9, pp. 383-393, 2009.
- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "Energy-Constrained Distortion Reduction Optimization for Wavelet-based Coded Image Transmission in Wireless Sensor Networks," *IEEE Transactions on Multimedia (TMM)*, vol. 10, no. 6, pp. 1169-1180, Oct. 2008.
- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "Energy-Constrained Quality Optimization for Secure Image Transmission in Wireless Sensor Networks," *Advances in Multimedia (AM), Hindawi Publishing Corporations*, vol. 2007, Article ID 25187, 9 pages, 2007.
- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "Matching Stream Authentication and Resource Allocation to Multimedia Codec Dependency with Position-Value Partitioning in Wireless Multimedia," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 5pp, Dec. 2009.
- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "Energy-Distortion-Authentication Optimized Resource Allocation for Secure Wireless Image Streaming," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, **BEST PAPER AWARD** (Selected from 573 accepted papers/ 1253 submitted papers), pp.2810-2815, Apr. 2008.
- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "Optimal Image Component Transmissions in Multi-rate Wireless Sensor Networks," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, pp.976-980, Nov. 2007.
- W. Wang. D. Peng, H. Wang, H. Sharif, "A Cross layer Resource Allocation Scheme for Secure Image Delivery in Wireless Sensor Networks," in *Proc. ACM International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp.152-157, Aug. 2007.
- W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, "Energy Efficient Multi-rate Interaction in Distributed Source Coding and Wireless Sensor Network," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, pp.4091-4095, Mar. 2007.

References

[1] Q. Sun, J. Apostolopoulos, C.-W. Chen, S.-F. Chang, “Quality-optimized and secure end-to-end authentication for media delivery,” *IEEE Proceedings,* vol. 96, no. 1, pp.97-110, Jan. 2008.

[2] Z. Li, Q. Sun, Y. Lian, C.-W. Chen, “Joint source-channel-authentication resource allocation and unequal authenticity protection for multimedia over wireless networks,” *IEEE Trans. Multimedia*, vol.9, no.4, pp.837-850, Jun. 2007.

[3] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Energy-distortion-authentication optimized resource allocation for secure wireless image streaming,” in *Proc. IEEE WCNC*, pp.2810-2815, Apr. 2008.

[4] Z. Zhang, Q. Sun, W. Wong, J. Apostolopoulos, S. Wee, “An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks,” *IEEE Trans. Multimedia*, vol. 9, no. 2, pp.320-331, Feb. 2007.

[5] Z. Zhang, Q. Sun, W. Wong, J. Apostolopoulos, S. Wee, “Rate-distortion-authentication optimized streaming of authenticated video,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 5, pp.544-557, May. 2007.

[6] Q. Sun, S.-F. Chang, “A secure and robust digital signature scheme for JPEG2000 image authentication,” *IEEE Trans. Multimedia*, vol. 7, no. 3, pp.480-494, Jun. 2005.

[7] Q. Sun, D. He, Q. Tian, “A secure and robust authentication scheme for video transcoding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 10, pp.1232-1244, Oct. 2006.

[8] C. Tzeng, W. Tsai, “A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement,” *IEEE Commun. Letters*, vol.7, no.9, pp.443-445, Sept. 2003.

[9] D. Skraparlis, “Design of an efficient authentication method for modern image and video,” *IEEE Trans. Consumer Electronics*, vol. 49, no. 2, pp.417-426, May. 2003.

[10] Z. Zhang, J. Apostolopoulos, Q. Sun, S. Wee, W-C. Wong, “Stream Authentication Based on Generalized Butterfly Graph,” in *Proc. IEEE International Conference on Image Processing,* vol. 6, pp.121 - 124, Sept. 2007.

[11] T. Li, Y. Wu, “Adaptive Stream Authentication for Wireless Multimedia Communications,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC),* pp.2613 - 2618, Mar. 2007.

[12] L. Ferrigno, S. Marano, V. Paciello, A. Pietrosanto, “Balancing computational and transmission power consumption in wireless image sensor networks,” in *Proc. IEEE Int. Conf. on Virtual Environments, Human-Computer Interfaces and Measurement Systems,* Jul. 2005.

[13] C. Chiasserini, E. Magli, “Energy consumption and image quality in wireless video-surveillance networks,” in *Proc. IEEE Int. Symposium on Personal, Indoor and Mobile Radio Commun.*, vol. 5, pp.2357 – 2361, Sept. 2002.

[14] R. Hamzaoui, V. Stankovic, Z. Xiong, “Optimized error protection of scalable image bit streams,” *IEEE Signal Process. Mag.*, vol.22, no. 6, pp.91-107, Nov. 2005.

[15] H. Wu, A. Abouzeid, “Error resilient image transport in wireless sensor networks,” *Int. J. Comp. Telecommun. Netw.*, vol. 50, no. 15, pp.2873-2887, Oct. 2006.

[16] Z. Wu, A. Bilgin, M. Marcellin, “Joint source/channel coding for multiple images,” *IEEE Trans. Commun*., vol.53, no. 10, pp.1648-1654, Oct. 2005.

[17] W. Yu, Z. Sahinoglu, A. Vetro, “Energy efficient JPEG 2000 image transmission over wireless sensor networks,” in *Proc. GLOBECOM,* pp.2738 - 2743, Dec. 2004.

[18] M. Wu, C. Chen, “Multiple bitstream image transmission over wireless sensor networks,” in *Proc. ICSENS*, vol. 2, pp.727-731, Oct. 2003.

[19] M. van Der Schaar, Sai Shankar N, “Cross layer wireless multimedia transmission: challenges, principles, and new paradigms,” *IEEE Wireless Commun.*, vol.12, no. 4, pp.50-58, Aug.2005.

[20] M. van de Schaar, D. Turaga, R. Wong, “Classification based system for cross layer optimized wireless video transmission,” *IEEE Trans. Multimedia*, vol. 8, no. 5, pp.1082-1095, Oct. 2006.

[21] L. Qiong, M. van der Schaar, “Providing adaptive QoS to layered video over wireless local area networks through real-time retry limit adaptation,” *IEEE Trans. Multimedia*, vol. 6, no. 2, pp.278-290, Apr. 2004.

[22] M. van der Schaar, D. Turaga, “Cross layer Packetization and Retransmission Strategies for Delay-Sensitive Wireless Multimedia Transmission,” *IEEE Trans. Multimedia*, vol. 9, no. 1, pp.185-197, Jan. 2007.

[23] W. Ye, J. Heidemann, D. Estrin, “Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks,” *IEEE/ACM Trans. Networking*, vol. 12, no. 3, pp.493 – 506, Jun. 2004.

[24] T. van Dam and K. Langendoen. “An adaptive energy efficient MAC protocol for wireless sensor networks,” In *Proceedings of the First ACM Conference on Embedded Networked Sensor Systems (SenSys)*, Los Angeles, CA, Nov. 2003.

[25] J. Polastre, J. Hill, and D. Culler, “Versatile low power media access for wireless sensor networks,” In *Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys)*, Baltimore, MD, Nov. 2004.

[26] I. Rhee, A. Warrier, M. Aia, and J. Min, "Z-MAC: a hybrid MAC for wireless sensor networks,” *Proceedings of the 3rd international conference on Embedded networked sensor systems*, San Diego, California, pp.90 – 101, 2005.

[27] B. Sadeghi, V. Kanodia, A. Sabharwal, E. Knightly. "OAR: A Multi-rate Media Access Protocol for Wireless Ad Hoc Networks," *ACM Mobile Networking and Applications*, 2003.

[28] V. Kanodia, A. Sabharwal, E. Knightly, "MOAR: a multi-channel opportunistic auto-rate media access protocol for ad hoc networks," *First International Conference on BroadNets*, pp.600-610, 2004.

[29] N. AbouGhazaleh, P. Lanigan, S. Gobriel, D. Mosse, R. Melhem, "Dynamic rate-selection for extending the lifetime of energy-constrained networks," in *Proc. IEEE International Conference on Performance, Computing, and Communications*, pp.553 – 558, 2004.

[30] *IEEE STD 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Technical report, IEEE, Jul. 1997.

[31] M. Zawodniok, Jagannathan Sarangapani, "Energy-efficient rate adaptation MAC protocol for ad hoc wireless networks," in *Proc. IEEE International Conference on Performance, Computing, and Communications*, pp.389 – 394, Apr. 2005.

[32] D. Qiao, S. Choi, A. Soomro, K Shin, “Energy-efficient PCF operation of IEEE 802.11a wireless LAN,” in *Proc. IEEE INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies.* vol. 2, pp.580 – 589, Jun. 2002.

[33] J. Zhao, Z. Guo, W. Zhu, “Power Efficiency in IEEE 802.11a WLAN with Cross layer Adaptation,” in *Proc. IEEE ICC*, pp.2030–2034, May 2003.

[34] S. L. Kim, Z. Rosberg, J. Zander, “Combined power control and transmission rate selection in cellular networks,” in *Proc. Vehicular Technology Conference*, vol.3, pp.1653 – 1657, 1999.

[35] C. Sung, W. Wong, “Power control and rate management for wireless multimedia CDMA systems,” *IEEE Transactions on Communications*, vol. 49, no. 7, pp.1215 – 1226, Jul. 2001.

[36] D. Kim, E. Hossain, V. K. Bhargava, "Downlink joint rate and power allocation in cellular multi-rate WCDMA systems," *IEEE Trans. Wireless Commun.*, vol. 2, no. 1, pp.69 – 80, Jan. 2003.

[37] S. Kandukuri, S. Boyd, “Simultaneous rate and power control in multi-rate multimedia CDMA systems,” in *Proc. IEEE Sixth International Symposium on Spread Spectrum Techniques and Applications*, vol. 2, pp.570 – 574, Sept. 2000.

[38] S.-M. Shum, R.-S. Cheng, “Power control for multi-rate CDMA systems with interference cancellation,” in *Proc. Global Telecommunications Conference*, vol. 2, pp.895 – 900, Nov. 2000.

[39] J.-W. Mark, S. Zhu, “Power control and rate allocation in multi-rate wideband CDMA systems,” in *Proc. Wireless Communications and Networking Conference, (WCNC)*, vol. 1, pp.168 – 172, Sept. 2000.

[40] D. Qiao, S. Choi, A. Jain, K. Shin, “Miser: an optimal low-energy transmission strategy for IEEE 802.11a/h,” in *Proc. ACM MobiCom*, pp. 161-175, Sep. 2003.

[41] D. Qiao, K. Shin, “Energy-efficient airtime allocation in multi-rate multi-power-level wireless lans,” in *Proc. ACM QShine*, Aug. 2007.

[42] S. Voloshynovskiy, S. Pereira, T. Pun, J.-J. Eggers, J.-K. Su, “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks,” *IEEE Commun. Mag.*, vol. 39, no. 8, pp.118 - 126, Aug. 2001.

[43] J.-R. Hernandez Martin, M. Kutter, “Information retrieval in digital watermarking,” *IEEE Commun. Mag.*, vol. 39, no. 8, pp.110 - 116, Aug. 2001.

[44] L. Ghouti, A. Bouridane, M.K. Ibrahim, S. Boussakta, “Digital image watermarking using balanced multiwavelets,” *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp.1519 - 1536, Apr.2006.

[45] H. Yuan, X.-P. Zhang, “Multiscale Fragile Watermarking Based on the Gaussian Mixture Model,” *IEEE Trans. Image Process.*, vol. 15, no. 10, pp.3189 - 3200, Oct. 2006.

[46] J. In, S. Shirani, F. Kossentini, “On RD optimized progressive image coding using JPEG,” *IEEE Trans. Image Process.*, vol.8, no.11, pp.1630 - 1638, Nov. 1999.

[47] A. Said, W.Pearlman, “A new, fast, and efficient image codec based on set partitioning in hierarchical trees,” *IEEE Trans. Circuits Syst. Video Technol*., vol. 6, no. 3, pp.243–250, Jun. 1996.

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

[49] D. Taubman, “High performance scalable image compression with EBCOT,” *IEEE Trans. Image Process*., vol.9, no. 7, pp.1158–1170, Jul. 2000.

[50] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Optimal image component transmissions in multirate wireless sensor networks,” in *Proc. IEEE GlobeCom*, pp.976-980, Nov. 2007.

[51] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Energy constrained distortion reduction optimization for wavelet-based coded image transmission in wireless sensor networks," *IEEE Trans. Multimedia*, vol. 10, no. 6, pp. 1169-1180, Oct. 2008.

[52] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Cross layer Multi-rate Interaction with Distributed Source Coding in Wireless Sensor Networks,” *IEEE Trans. Wireless Commun. (TWC),* vol. 8, no. 2, pp. 787-795, Feb. 2009.

[53] S.-M. Yen, C.-S. Laih, “Improved digital signature algorithm,” *IEEE Trans. Computers*, vol. 44, no. 5, pp.729 – 730, May. 1995.

[54] L. Harn, M. Mehta, W.-J. Hsin, “Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA),” *IEEE Commun. Letters*, vol. 8, no. 3, pp.198 – 200, Mar. 2004

[55] H.-M. Elkamchouchi, A.-A. M. Emarah, E.-A. Hagras, “A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes,” in *Proc. IEEE Twenty Third National Radio Science Conference*, vol. 0, pp.1 – 9, Mar. 2006.

[56] R. Chaves, G. Kuzmanov, L. Sousa, S. Vassiliadis, “Cost-Efficient SHA Hardware Accelerators,” *IEEE Trans. Very Large Scale Integration (VLSI) Systems*, vol. 16, no. 8, pp.999 – 1008, Aug. 2008.

[57] H. Wang, D. Peng, W. Wang, H. Sharif, H.-H. Chen, “Image Transmission with Security Enhancement Based on Region and Path Diversity in Wireless Sensor Networks,” *IEEE Trans. Wireless Commun. (TWC).* vol. 8, no. 2, pp. 757-765, Feb. 2009.

[58] H. Wang, D. Peng, W. Wang, H. Sharif, H.-H. Chen, “Cross layer Routing Optimization in Multirate Wireless Sensor Networks for Distributed Source Coding based Applications,” *IEEE Trans. Wireless Commun. (TWC),* vol. 7, no. 10, pp. 3999-4009, Oct. 2008.

[59] B. Zhu, M. Swanson, A. Tewfik, “When seeing isn’t believing,” *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 40 – 49, Mar. 2004.

[60] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “A Multimedia Quality-Driven Network Resource Management Architecture for Wireless Sensor Networks with Stream Authentication," submitted to *IEEE Trans. Multimedia*, in print, 2009.

[61] P. Chou, Z. Miao, “Rate-distortion optimized streaming of packetized media,” *IEEE Trans. Multimedia.*, vol.8, no. 2, pp.390-404, Apr. 2006.

[62] T. Ozcelebi, A. Tekalp, M. Civanlar, “Delay-distortion optimization for content-adaptive video streaming,” *IEEE Trans. Multimedia*, vol. 9, no. 4, pp. 826-836, Jun. 2007.

[63] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Optimal Image Component Transmissions in Multi-rate Wireless Sensor Networks,” in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Nov. 2007.

[64] W. Wang, D. Peng, H. Wang, H. Sharif, “Image Component Transmissions in Wireless Sensor Networks,” in *Proc. IEEE Sarnoff Symposium*, May. 2007.

[65] http://en.wikipedia.org/wiki/Embedded_Zerotrees_of_Wavelet_transforms

[66] Y. Yuan, Z. He, M. Chen, “Virtual mimo-based cross layer design for wireless sensor networks,” *IEEE Trans Vechicular Technology*, vol.55, no.3, pp.856-864, May.2006.

[67] S. Cui, A. Goldsmith, A. Bahai, “Energy-constrained modulation optimization,” *IEEE Trans. Wireess Commun.*, vol. 4, no. 5, pp. 2349-2360, Sept.2005.

[68] http://en.wikipedia.org/wiki/MPEG-4

[69] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H.Chen, “Multimedia over Mobile WiMAX,” *A Chapter in the Book of WiMAX Network Planning and Optimization*, Edited by Dr. Yan Zhang, Auerbach Publications, CRC Press. Apr. 2009.

[70] R. Xiong, J. Xu, F. Wu, “In-Scale Motion Compensation for Spatially Scalable Video Coding,” *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 18, no. 2, pp.145 - 158, Feb. 2008

[71] H.-M. Radha, M. van der Schaar, Y. Chen, “The MPEG-4 fine-grained scalable video coding method for multimedia streaming over IP,” *IEEE Transactions on Multimedia,* vol. 3, no. 1, pp.53 - 68, Mar. 2001.

[72] M. Wien, H. Schwarz, T. Oelbaum, “Performance Analysis of SVC,” *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 17, no. 9, pp.1194 - 1203, Sept. 2007

[73] T. Wieg, H. Schwarz, A. Joch, F. Kossentini, G.-J. Sullivan, “Rate-constrained coder control and comparison of video coding standards,” *IEEE Transactions on Circuits and Systems for Video Technology,* vol.13, no. 7, pp.688 - 703, Jul. 2003

[74] N. Krishnan, R.-K. Selvakumar, P. Vijayalakshmi, K. Arulmozhi, “Adaptive Single Pixel Based Lossless Intra Coding for H.264 / MPEG-4 AVC,” in *Proc. IEEE International Conference on Computational Intelligence and Multimedia Applications,* vol. 3, pp.63 - 67, Dec. 2007

[75] I. Amer, W. Badawy, G. Jullien, “A VLSI prototype for Hadamard transform with application to MPEG-4 part 10,” in *Proc. IEEE International Conference on Multimedia and Expo,* vol. 3, pp.1523 - 1526, Jun. 2004

[76] A.-R. Acosta, G. Vazquez, S. Mireya, C.-V. Juan, “MPEG-4 AVC/H.264 and VC-1 Codecs Comparison Used in IPTV Video Streaming Technology,” in *Proc. IEEE Electronics, Robotics and Automotive Mechanics Conference,* pp.122 - 126, Sept. 2008

[77] P. Siebert, “Implementation of H.264/MPEG-4 AVC in low cost set top boxes,” in *Proc. the Ninth IEEE International Symposium on Consumer Electronics,* pp.310 - 314, Jun. 2005

[78] M. Volk, J. Guna, A. Kos, J. Bester, “IPTV Systems, Standards and Architectures: Part II - Quality-Assured Provisioning of IPTV Services within the NGN Environment,” *IEEE Communications Magazine,* vol. 46, no. 5, pp.118 - 126, May 2008

[79] X. Hei, C. Liang, J. Liang, Y. Liu, K.-W. Ross, “A Measurement Study of a Large-Scale P2P IPTV System,” *IEEE Transactions on Multimedia,* vol. 9, no. 8, pp.1672 - 1687, Dec. 2007

[80] C.-C.-Y. Choi, M. Hamdi, “A scalable video-on-demand system using multi-batch buffering techniques,” *IEEE Transactions on Broadcasting,* vol. 49, no. 2, pp.178 - 191, Jun. 2003

[81] J.-W. Ding, C.-T. Lin, S.-Y. Lan, “A Unified Approach to Heterogeneous Video-on-Demand Broadcasting,” *IEEE Transactions on Broadcasting,* vol. 54, no. 1, pp.14 - 23, Mar. 2008

[82] K. Wu, Y. Cao, B. Sun, Y. Xiao, “Experimental Study of an Online Game over Wireless Networks,” in *Proc. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing,* pp.86 - 89, Aug. 2007

[83] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Taming Underlying Design for Energy Efficient Distributed Source Coding in Multi-rate Wireless Sensor Network,” in *Proc. IEEE Vehicular Technology Conference (VTC),* pp.124-129, Apr. 2007.

[84] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Energy Efficient Multi-rate Interaction in Distributed Source Coding and Wireless Sensor Network,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC),* pp.4091-4095, Mar. 2007.

[85] H. Wang, D. Peng, W. Wang, H. Sharif, “Cross layer Optimization in Wireless Sensor Network with Rate Distribution,” in *Proc. IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS),* Nov. 2006.

[86] W. Wang, D. Peng, H. Wang, H. Sharif, T. Wysocki, B. Wysocki, “An Energy Efficient MAC-PHY Approach to Support Distributed Source Coding in Wireless Sensor Network,” in *Proc. the 5th Workshop on the Internet, Telecommunications and Signal Processing (WITSP),* Dec. 2006.

[87] H. Wang. D. Peng, W. Wang, H. Sharif, H.-H. Chen, “Interplay between routing and distributed source coding in wireless sensor network,” in *Proc. IEEE ICC,* pp.3776-3781, Jun.2007.

[88] C. Schurgers, O. Aberthorne, M. Srivastava, “Modulation scaling for energy aware communication systems,” in *Proc. Int. Symposium on Low Power Electronics and Design*, pp.96 – 99, Aug. 2001.

[89] Simon Haykin, *Communication System*, 3-rd edition, Wiley, New York, pp.510-553, 1994.

[90] William Stallings, *Data and Computer Communications*, 7-th edition, Prentice Hall, Upper Saddle River, N.J., pp.85-86, 2000.

[91] J. Xiao, S. Cui, Z. Luo, A. Goldsmith, "Power scheduling of universal decentralized estimation in sensor networks," *IEEE Trans. Signal Process.*, vol.54, no. 2, pp.413-422, Feb. 2006.

[92] W. Webb, "QAM: the modulation scheme for future mobile radio communications," *Electronics & Communication Engineering Journal*, vol. 4, no. 4, pp.167-176, Aug. 1992.

[93] http://www.tinyos.net

[94] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, D. Culler, “The nesC Language: A Holistic Approach to Networked Embedded Systems,” *in Proceedings of Programming Language Design and Implementation (PLDI),* Jun. 2003.

[95] http://www.openjpeg.org/

[96] T. Lookabaugh, D.-C. Sicker, “Selective encryption for consumer applications,” *IEEE Commun. Mag*., vol.42, no.5, pp.124-129, May.2004.

[97] H. Cheng, X. Li, “Partial encryption of compressed images and videos,” *IEEE Trans. on Signal Process*., vol.48, no.8, pp.2439–2451, Aug.2000.

[98] L. Tang, “Methods for encrypting and decrypting MPEG video data efficiently,” in *Proc. Int. Conf. ACM Multimedia*, pp.219-229, Nov.1996.

[99] M. Grangetto, E. Magli, G. Olmo, “Multimedia Selective Encryption by Means of Randomized Arithmetic Coding,” *IEEE Trans. Multimedia*, vol.8, no.5, pp.905-917, Oct.2006.

[100] M. Grangetto, A. Grosso, and E. Magli, “Selective encryption of JPEG 2000 images by means of randomized arithmetic coding,” in *Proc. IEEE Int. Workshop on Multimedia Signal Processing,* 2004.

[101] C.-P. Wu, C.-J. Kuo, “Design of integrated multimedia compression and encryption systems,” *IEEE Trans. Multimedia*, vol.7, no.5, pp.828-839, Oct.2005.

[102] C.-P. Wu, C.-J. Kuo, “Efficient multimedia encryption via entropy codec design,” in *Proc. SPIE Security and Watermarking of Multimedia Content III*, vol. 4314, Jan. 2001.

[103] C.-P. Wu, C.-J. Kuo, “Fast encryption methods for audiovisual data confidentiality,” in *Proc. SPIE Int. Symp. Information Technologies 2000,* Boston, MA, pp. 284–295, Nov. 2000.

[104] O. Au, J. Zhou, Y. Chen, Z. Liang, “Security Analysis of Multimedia Encryption Schemes Based on Multiple Huffman Table,” *IEEE Signal Process. Letters*, vol. 14, no. 3, pp.201-204, Mar. 2007

[105] J. Wen, H. Kim, and J.-D. Villasenor, “Binary arithmetic coding with key-based interval splitting,” *IEEE Signal Process. Letters*, vol. 13, no. 2, pp. 69–72, Feb. 2006.

[106] W. Zeng, S. Lei, “Efficient frequency domain selective scrambling of digital video,” *IEEE Trans. Multimedia*, vol.5, no. 1, pp.118-129, Mar.2003.

[107] M. Kankanhalli, T. Guan, “Compressed domain scrambler/descrambler for digital video,” *IEEE Trans. Consum. Electron.*, vol.48, no.2, pp.356-365, May.2002.

[108] G. Jakimoski, K. Subbalakshmi, “Cryptanalysis of some multimedia encryption schemes,” *IEEE Trans. Multimedia*, vol.10, no. 3, pp.330-337, Apr.2008.

[109] W. Wang. D. Peng, H. Wang, H. Sharif, “A cross layer resource allocation scheme for secure image delivery in wireless sensor networks,” in *Proc. ACM International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 152-157, Aug. 2007.

[110] W. Wang, D. Peng, H. Wang, H. Sharif, H.-H. Chen, “Energy-Constrained Quality Optimization for Secure Image Transmission in Wireless Sensor Networks,” *Special Issue on Multimedia Transmission over Emerging Wireless Technologies (MTWT), Hindawi Advances in Multimedia Journal.* 2007.

[111] W. Wang, D. Peng, H. Wang, H. Sharif, “An Adaptive Approach for Image Encryption and Secure Transmission over Multirate Wireless Sensor Networks,” *Special Issue on Distributed Systems of Sensors and Applications, Wireless Communications and Mobile Computing Journal (WCMC),* John Wiley & Sons, vol. 9, pp. 383-393, 2009.

[112] National Institute for Standard and Technology (NIST), *Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES),* Washington DC, Nov. 2001

[113] D. Wheeler, R. Needham, “TEA, a tiny encryption algorithm,” in *Proc. Fast Software Encryption of LNCS*, vol.1008, pp.14-16, 1994

[114] T. Cormen, C. Leiserson, R. Rivest, C. Stein, *The RSA public-key cryptosystem: Introduction to Algorithms, Section 31.7,* Second Edition. MIT Press and McGraw-Hill, pp.881–887, 2001.

[115] K. Lauter, “The advantages of elliptic curve cryptography for wireless security,” *IEEE Wireless Commun*., vol.11, no. 1, pp.62–67, Feb. 2004.

[116] http://mathworld.wolfram.com/Erfc.html