Wireless Pers Commun (2009) 51:5–16
DOI 10.1007/s11277-008-9595-x

A Scalable Information Security Technique: Joint Authentication-Coding Mechanism for Multimedia over Heterogeneous Wireless Networks

Liang Zhou · Baoyu Zheng · Anne Wei · Benoît Geller · Jingwu Cui

Published online: 10 October 2008

Abstract There have been increasing concerns about the security issues of wireless transmission of multimedia in recent years. Wireless networks, by their natures, are more vulnerable to external intrusions than wired ones. Therefore, many applications demand authenticating the integrity of multimedia content delivered wirelessly. In this work, we propose a framework for jointly authenticating and coding multimedia to be transmitted over heterogeneous wireless networks. We firstly provide a novel graph-based authentication scheme which can not only construct the authentication graph flexibly but also trade-off well among some practical requirements such as overhead, robustness and delay. And then, a rate-distortion optimized joint source-channel coding (JSCC) approach for error-resilient scalable encoded video is presented, in which the video is encoded into multiple independent streams and each stream is assigned forward error correction (FEC) codes to

L. Zhou
Electronic Engineering Department, Shanghai Jiao Tong University, Shanghai 200240, China

L. Zhou (✉) · B. Zheng · J. Cui
Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
e-mail: zking@sjtu.edu.cn

B. Zheng
e-mail: zby@njupt.edu.cn

J. Cui
e-mail: cuijw@njupt.edu.cn

A. Wei
CEDRIC, Conservation National des Arts et Métiers, Paris 75003, France
e-mail: anne.wei@cnam.fr

B. Geller
SATIE, Ecole Normale Supérieure (E.N.S.), Cachan 94230, France

B. Geller
LEI, Ecole Nationale Supérieure des Techniques Avancées, Paris 75015, France
e-mail: benoit.geller@ensta.fr

avoid error propagation. Furthermore, we consider integrating authentication with the specific JSCC scheme to achieve a satisfactory authentication results and end-to-end reconstruction quality by optimally applying the appropriate authentication and coding rate. Simulation results show the effectiveness of the proposed authentication-coding scheme for multimedia over wireless networks.

Keywords Multimedia security · Authentication · Joint source-channel coding · Wireless networks

1 Introduction

As multimedia is expected to be a major traffic source on the next-generation wireless networks, the demand for transmitting the multimedia content over wireless networks has increased. In contrast to the abundance of methods have been proposed to design robust and efficient schemes for delivering multimedia content over error-prone wireless networks, there are only very few works paying attention to the security aspect of such transmission. In fact, as more and more applications require authenticated multimedia streams, it is important to protect the authenticity of the streams in the aspects of integrity and non-repudiation.

The authentication problem has been attempted mainly using two approaches: a naive solution of authenticating a potential long stream is to sign each network packet using digital signature. However the problem is that signing algorithms nowadays are computationally expensive, and it is not worthy to compute and verify one signature for each packet [1]; since it is too expensive to sign every packet of the stream, we can organize packets into groups and sign only one packet within each group [2]. This approach can be further classified into graph-based approach [3–6] and erasure-code-based approach [7]. Gennaro and Rohatgi [3] proposed an authentication scheme using a simple hash chain. It has low overhead and low receiver delay, but it cannot tolerate any packet loss; Peffig et al. [4] provided EMSS, which uses a hash chain where each packet contains the hashes of previous packets and the signing is on the last packet. Obviously, it easily leads to a high receiver delay; Song et al. [5] presented an authentication scheme based on the expander graph and theoretically derived the lower bound of authentication probability (AP). However, it has a very large Miner and Staddon communication overhead which is unacceptable for real applications; Miner and Staddon [6] was based on the random graph. The signing is on the first packet, and each packet contains the hashes of every subsequent packet with certain probability. Therefore, it also has high communication overhead; Park et al. [7] was proposed to use erasure code for stream authentication. For each block, the digital signature is coded with erasure code and then scattered into the packets. As long as the number of loss packets is less than a threshold, all received packets can be authenticated. This scheme has a high computation overhead due to the erasure coding. In addition, it also suffers from a high receiver delay, because the receiver has to wait for a minimum number of the received packets before authentication.

The main contributions of this paper are as follows: firstly, we present a novel graph-based authentication (NGBA) approach which can not only construct the authentication graph (AG) flexibly but also trade-off well between the aforementioned practical requirements. Secondly, we propose an analytical joint source-channel coding (JSCC) approach for error-resilient scalable encoded video for lossy transmission, in which the video is encoded into multiple independent sub-streams based on 3D SPIHT (3D set partitioning in hierarchical trees) algorithm to avoid error propagation. Furthermore, the final realization of joint authentication-coding (JAC) system is the highlight of the proposed scheme because the ultimate goal of such scheme is to achieve an optimal end-to-end multimedia quality under the overall limited resource budget.

2 System Description

The proposed joint authentication and coding system is shown in Fig. 1. At the sender, the multimedia content is firstly passed to the JAC control unit, where it runs the JAC scheme and outputs the optimal source code rate, channel code rate, and authentication rate. The JSCC unit encodes the multimedia according to both the source rate and outputs the compressed code stream. In the packet signing unit, AG is constructed using the proposed NGBA approach. Therefore, the main task at the sender is to sign and protect the code stream by joint authentication and coding before transmission.We assume that the source decoder is error-resilient, where techniques such as synchronization mark and CRC (cyclic redundancy check) are applied to the code stream. Note that bit errors would trigger verification false alarms, and thus it is important to skip packets with bit errors during authentication. The verifiability information passes to the source decoding unit, so that during multimedia decoding, those non-verifiable packets are skipped [8].

2.1 Definitions and Notations

Considering a sender transmitting consecutive packets $\{P_1, \ldots, P_n\}$ in a broadcast data stream, we construct an AG to authenticate received packets. In particular, we construct a directed acyclic graph of n vertices where a vertex i corresponds to the packet P_i. Let $e(i, j)$ denotes a directed edge starting from i and ending at j. An edge $e(i, j)$ in the graph indicates the authentication relationship between packet P_i and P_j: upon receiving packet P_i and P_j, if a receiver can authenticate both the contents and the source of P_i, then it can authenticate the contents and source of P_j. One of the packets, denoted by P_{sig}, is signed with a public key signature algorithm. Hence, packet P_i can be authenticated if and only if

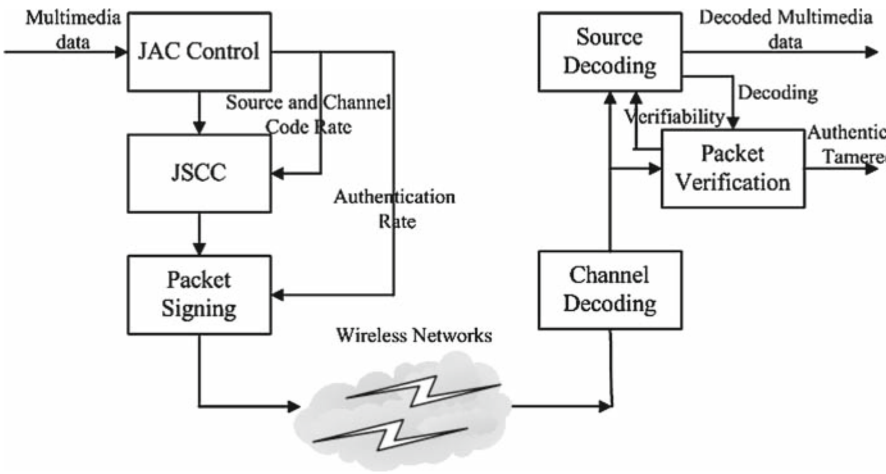


Fig. 1 Architecture of the joint authentication and coding scheme

there is a path from P_i to the signature packet that only includes nodes corresponding to the received packets [9]. We denote the probability that P_i is linked to P_{sig} via such a path by $Pr[P_i \to P_{sig}]$.

2.2 Novel Graph-Based Authentication

In order to obtain lower overhead and higher AP while maintain the same level of delays and robustness against packet loss, we propose a novel graph-based authentication approach where one signature is amortized among a group of packets connected with some regular graphs.

2.2.1 Authentication Graph Construction

Assume the stream is divided into a number of blocks and each block contains $M+1$ ($M \geq 0$) packets, where only one signature is generated for each block, and the M packets and the signature packet P_{sig} are connected using the regular graph. Assuming $M = n \times m + t$ ($n, m, t \geq 0$), the definition of the graph is given below.

The M data packets are divided into m stages, and each stage has n packets, and the t is the remaining packets. The packet is denoted as $P(u, v)$, where $u \in \{0, 1, \ldots, m-1\}$ indicates the horizontal stage and $v \in \{0, 1, \ldots, n-1\}$ indicates the packet in a stage. In this graph, there exists a directed edge $e(P(u_1, v_1), P(u_2, v_2))$ from packet $P(u_1, v_1)$ to packet $P(u_2, v_2)$, if either of the following conditions is met: (1). $u_1 = u_2 + 1$ and $v_1 = v_2$; (2). $u_1 = u_2 + 1$ and $v_1 = v_2 \pm 2^{m-1-u_1}$. In addition, there also exists a directed *edge from all packets* in stage 0 to the signature packet P_{sig} [10].

AG Construction

- If there exists $m = \log_2 n + 1$ and $t = 0$. Each directed edge $e(P(u_1, v_1), P(u_2, v_2))$ is realized by appending the hash of the packet $P(u_1, v_1)$ to $P(u_2, v_2)$. For every $P(u, v)$ in the authentication graph (except stage 0), there are two directed edge to connect another one. In order to guarantee the authentication probability, we set one hash for each directed edge.
- If there exists $m = \log_2 n + 1$ but $t \neq 0$, the remaining packets t are constructed using the following units (shown in Fig. 2). Note that all packets in stage 0 to $m-1$ have two hashes, and the packets in the last stage (just for the t) do not have any hash. Figure 3 gives an example of the constructed AG when $M = 34 = 8 \times 4 + 2$. Because the remaining packets t are random, in order to give a uniform bound of authentication probability, we do not set hash for them. It is should be noted that, the remaining packets t can still be authenticated because there are directed edges which connects to signature packet P_{sig}.

2.2.2 Lower Bound of AP

For all pairs of nodes (i, j), we include a directed edge from node i to node j with probability p ($0 < p \leq 1$), we call a graph constructed in this way a p-random graph. For notational convenience, we note $P_{sig} = P_1$.

Theorem *With a p-random authentication approach in a lossy network, in which each packet is lost independently at random with probability q, packet P_i, $i \geq 2$, can be authenticated with probability:*

$$Pr[P_i \to P_{sig} | P_i \ is \ received] \geq 1 - (1-p)(1-(p(1-q))^2)^{i-2} \tag{1}$$

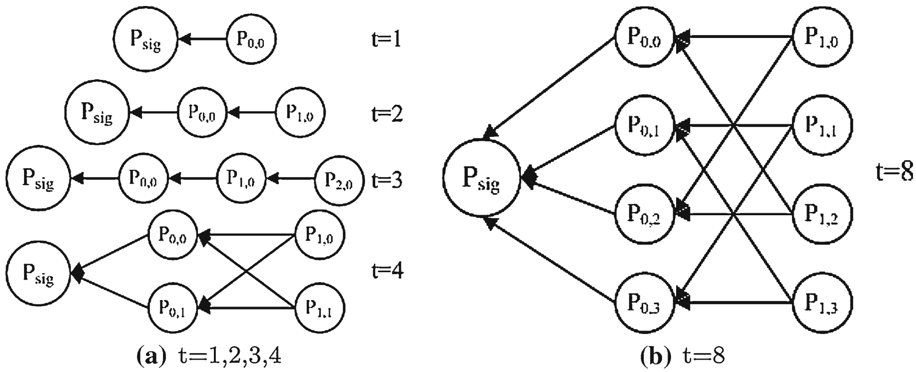


Fig. 2 Basic units of constructing authentication graph

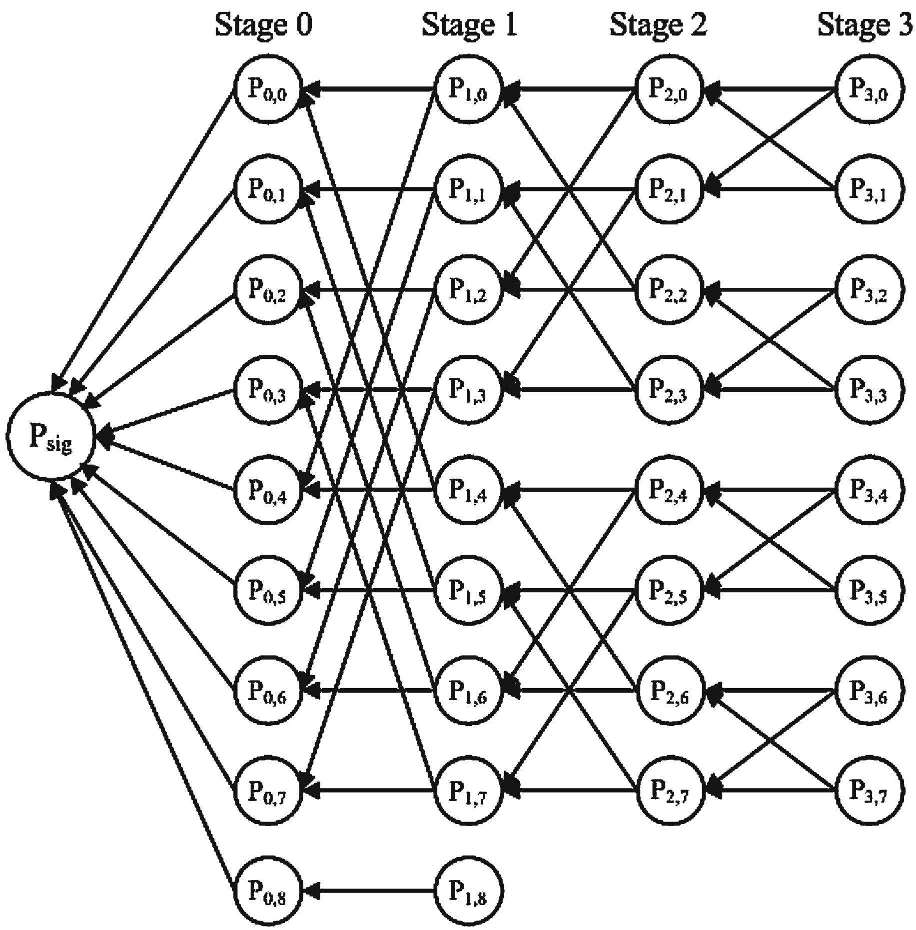


Fig. 3 An example of authentication graph ($M = 34$)

Proof We assume that P_1 is always received (this may be accomplished with high probability by transmitting it multiple times, or empowering receivers to request re-transmission if it is not received). First, we calculate the probability that node i connects to signature node (node 1) in the corresponding p-random graph with no packet loss ($q = 0$) as follows: (1) with probability p, $e(i, 1)$ exists and so, node i connects to the signature node; (2) with probability $(1-p)p$, $e(i, 1)$ does not exists but $e(i, i-1)$ does, so i can connect to signature node via a path from $i-1$ to signature node [11]. Proceeding in this way, we get the following expression:

$$\begin{aligned} Pr[P_i \rightarrow P_{sig}|P_i] \geq p + (1-p)pPr[P_{i-1} \rightarrow P_{sig}|P_{i-1}] + \cdots \\ + (1-p)^{i-2}pPr[P_2 \rightarrow P_{sig}|P_2] \end{aligned} \tag{2}$$

Apply the induction assumption for $1, \ldots, i-1$, to the right hand side of the inequality above, we have:

$$p + (1-p)p(1-(1-p)(1-p^2)^{i-3}) + \cdots + (1-p)^{i-2}p(1-(1-p)) \tag{3}$$

We simplify this expression by factoring out terms of the form $(1-p)$. As a first step, we have:

$$\begin{aligned} &1-(1-p)\Big[1-p+(1-p)p(1-p^2)^{i-3}-(1-p)p+(1-p)^2p(1-p^2)^{i-4}-\cdots \\ &-(1-p)^{i-2}p+(1-p)^{i-3}p(1-p^2)-(1-p)^{i-3}p+(1-p)^{i-2}p\Big] \end{aligned} \tag{4}$$

Continuing to factor in this way, we eventually get:

$$\begin{aligned} &1-(1-p)^{i-1}\Big[p(1+p)^{i-3}+p(1+p)^{i-4}+p(1+p)^{i-5}+\cdots+p(1+p)+1+p\Big] \\ &=1-(1-p)^{i-1}\left[p(\frac{1-(1+p)^{i-2}}{1-(1+p)}-1)+1+p\right] \end{aligned} \tag{5}$$

This simplifies to: $1-(1-p)(1-p^2)^{i-2}$. Then, taking into account the packet loss q, we follow the same type of argument as used in no packet loss case, we have:

$$\begin{aligned} Pr[P_i \rightarrow P_1|P_i] \geq p + (1-p)p(1-q)Pr[P_{i-1} \rightarrow P_1|P_{i-1}] + \cdots \\ + (1-p(1-q))^{i-2}p(1-q)Pr[P_2 \rightarrow P_1|P_2] \end{aligned} \tag{6}$$

Let $a_i(p) = 1-(1-p)(1-p^2)^{i-2}$, from the equality above, it follows that

$$Pr[P_i \rightarrow P_1|P_i] \geq \left(\frac{a_i(p(1-q))-p}{1-p}\right)(1-p(1-q))+p(1-q) \tag{7}$$

The statement of the theorem follows from substituting in the expression for $a_i(p(1-q))$. □

In the case of the proposed NGBA, a packet $P(u, v)$ can not be authenticated unless there is a path to the signature packet at the receiver. The authentication probability $Pr[P(u, v)]$ is equivalent to probability that such path exists

$$Pr[P(u, v)] \geq 1-(1-p)(1-(p(1-q))^2)^u, \quad u \geq 0 \tag{8}$$

We can see that $Pr[P(u, v)]$ depends only on u and q, and all packets in the same stage have the same $Pr[P(u, v)]$. As we travel from stage 0 to stage $m-1$, the authentication probability decreases, because a packet in the later stage has more independency than that in the earlier stage. However, this trend is slowed down by the proposed graph where a packet in the later stage has more paths to the signature packet. Therefore, the minimum authentication probability Pr_{min} under random packet loss can be achieved as follows

$$Pr_{min} = 1 - (1-p)(1-(p(1-q))^2)^m \tag{9}$$

2.3 Joint Source Channel Coding

The proposed coding architecture contains two parts: Unit-1 uses the 3D SPIHT codec that generates independent embedded streams, while Unit-2 uses the coding constraints and channel condition to pack the bit-streams into pack-streams of quality layers. This two-units structure collects incremental contributions from the various streams into SNR scalable quality layers in a way similar to that of embedded block coding with optimized truncation. The streams and rate-distortion functions generated by Unit-1 can be processed independently to channel conditions. The source and channel allocation algorithm in Unit-2 must be efficient to cope with the time varying channel conditions [12].

We use Reed-Solomon (RS) code as the channel coding strategy because it is effective for recovering erased symbols when their locations are known [13]. Here, a two-state Markov model (i.e. Gilbert model) is employed to simulate the bursty packet loss behavior [14]. The two states of this model are denoted as G (good) and B (bad). In state G, packets are received correctly and timely, whereas, in state B, packets are assumed to be lost. This model can be described by the transition probabilities P_{GB} from state G to B and P_{BG} from state B to G. The then the average P_B is given by

$$P_B = \frac{P_{GB}}{P_{GB} + P_{BG}} \tag{10}$$

The Markov model is a renewal model, and such models are determined by the distribution of error-free intervals, known as gap. Let gap of length σ be the event that after a lost packet, $\sigma - 1$ packets are received and then again a packet is lost. The gap density function $g(\sigma)$ gives the probability of a gap length σ. The gap distribution function $G(\sigma)$ gives the probability of the gap length greater than $\sigma - 1$. These functions can be derived as [12]

$$g(\sigma) = \begin{cases} 1 - P_{BG}, & \sigma = 1 \\ P_{BG}(1-P_{GB})^{\sigma-2}P_{GB}, & \sigma > 1 \end{cases} \tag{11}$$

$$G(\sigma) = \begin{cases} 1 - P_{BG}, & \sigma = 1 \\ P_{BG}(1-P_{GB})^{\sigma-2}, & \sigma > 1 \end{cases} \tag{12}$$

Let $R(n,m)$ be the probability of $m-1$ erroneous symbols within the next $n-1$ symbols following an erroneous symbol. It can be calculated using the recurrence

$$R(n,m) = \begin{cases} G(n), & m = 1 \\ \sum\limits_{\sigma=1}^{n-m+1} g(\sigma)R(n-\sigma, m-1), & 2 \le m \le n \end{cases} \tag{13}$$

Then the probability of errors within m a block of n symbols is

$$P'(n,m) = \begin{cases} \sum\limits_{\sigma=1}^{n-m+1} P_B G(\sigma) R(n-\sigma+1, m), & 1 \le m \le n \\ 1 - \sum\limits_{\sigma=1}^{n} P'(n,m), & m = 0 \end{cases} \tag{14}$$

3 Optimization for Joint Authentication and Coding

The purpose of joint authentication and coding is to achieve two objectives: (1) optimize the source and channel coding bits for minimizing the end-to-end distortion, and (2) optimize the authentication bits for achieving satisfactory AP. Notice that AP determines the probability that a packet is non-verifiable, which should be skipped during reconstruction. Since the skip will result in distortions to the multimedia content, we may find that it is possible to unify the two objectives into one single form, i.e., maximizing the end-to-end PSNR (Peak Signal-to-Noise Ratio) at the receiver relative to the original sequence [8]. It can be defined as

$$PSNR(dB) = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{15}$$

where MSE is the mean-square error between the original and the decoded luminance frame.

For notational convenience, we define the bit-plane 1 as the highest bit plane and the bit-plane I_s as the lowest bit plane to be sent for sub-streams [15]. Let N_s be the number of packets that are used to send the combined source data and redundancy for sub-stream-s in a GOP (Group of Pictures) and L be the packet size in bytes. In this scheme, the bits belonging to bit-plane i $(1 \leq i \leq I_s)$ are filled into $k_{s,i}$ packets and the remaining $c_{s,i} = N_s - k_{s,i}$ packets are filled with channel coding redundancy. In other words, the source data for bit-plane i is protected by RS code $(N_s, k_{s,i})$.

We propose the JAC scheme which is performed on GOP basis. We define the total number of packets to be sent from all sources for a GOP period N as

$$N \leq \left\lceil \frac{R \times N_{GOP}}{F \times L} \right\rceil \tag{16}$$

where R is the total coding rate in bytes/s for the combination of source coding (r_s), channel coding (r_c) and authentication (r_a) for all sources, N_{GOP} is the number of frames in a GOP, F is the frame rate in frames/s. In this framework, we assume that are n_s sources and source-s transmits sub-stream-s to the receiver for $s = 1, 2, \ldots, n_s (n_s \geq 1)$. Then the proposed algorithm divides N into $N_1(t_i), N_2(t_i), \ldots, N_{n_s}(t_i)$ so as to maximize the expected quality at the receiver, where $N_s(t_i)$ represents the total number of packets transmitted by source-s at GOP period t_i for $s = 1, 2, \ldots, n_s (n_s \geq 1)$. Taking account into the effective rate of source s, $N_s(t_i)$ should satisfy the following condition:

$$N_s(t_i) \leq \left\lceil \frac{R_s(t_i) \times N_{GOP}}{F \times L} \right\rceil \tag{17}$$

where $R_s(t_i)$ is the total rate of source-s at the GOP period t_i. In typical transform coding, each coefficients is quantized independently. The overall distortion is exactly the summation of the distortion at each source. The probability for an authentic packet P_i to be decodable and verifiable is $Pr_i(1-P_B)$. In this case, the distortion is merely due to source coding. If the packet is either non-decodable or non-verifiable, the distortion depends on the specific error-concealment scheme. Here, we consider setting the values to zeros when a packet is either non-decodable or non-verifiable. Therefore, we can state our source and channel allocation algorithm as follows: Given N, $R_s(t_i)$ and the tolerated minimum authentication probability Pr_{thr}, the proposed algorithm finds $N_s(t_i)$ and $K_s(t_i) = (k_{s,1}(t_i), k_{s,2}(t_i), \ldots, k_{s,I_s}(t_i))$ for $s = 1, 2, \ldots, n_s$, that maximize the expected quality at the receiver given by

$$PSNR(t_i) = \sum_{s=1}^{n_s} (Pr_s(1-P_B)) \sum_{l=1}^{I_s} \left(\sum_{j=N_s-k_{s,l}+1}^{N_s-k_{s,l-1}} P'(j, N_s) \sum_{i=l}^{I_s} PSNR_s(i) \right) \quad (18)$$

$$\textit{subject to} \quad \sum_{s=1}^{n_s} N_s = N,$$

$$N_s \le \left\lceil \frac{R_s(t_i) \times N_{GOP}}{F \times L} \right\rceil$$

$$Pr_s \ge Pr_{thr}, s = 1, 2, \ldots, n_s$$

where Pr_s is the average AP of source-s; $P'(j, N_s)$ is the probability that j packets are lost out of N_s packets sent by source-s; $PSNR_s(i)$ is the expected quality at the receiver when the receiver decodes up to the ith bit-plane for sub-stream-s; I_s is the last bit plane to be sent for source-s.

Each source independently runs the proposed rate allocation algorithm to get its optimal number of packets to transmit for a GOP period, using the information contained in the control packets that the receiver sends to all sources. The proposed algorithm tries all possible combinations of (N_s, K_s) that satisfy the constraints in (18) and choose one that maximizes the expected quality. Once the optimal (r_s, r_c) value is found, the source code rate, channel code rate and authentication rate are determined.

4 Simulation Results and Discussion

For these experiments, we use the QCIF Weather Forecast test sequence at $F = 30 frames/s$, $N_{GOP} = 16$ and $n_s = 2$. A three-level wavelet decomposition is applied to a group of 16 frames and the 3-D wavelet coefficients are divided into two groups using the method proposed in [13]. We use RS(15,9) as the channel coding in the following simulations.

In order to provide a representative evaluation of system performance, for each simulation run we generate a random topology on the disc of unit area as a 2D Poisson point process with total number of nodes equal to 25. The transmission range r for each node is kept constant during the simulation at the value of $r = 0.2 \times (1/\sqrt{\pi})$ such that the sum of the transmission regions for all the 25 nodes (i.e., $25 \times \pi r^2 = 1$) almost completely covers the unit disc, thus ensuring a high degree of connectivity. Each node is assigned the fixed transmission rate $W_i = 2Mbps$, which is a basic rate available in the IEEE 802.11b standard.

In most approaches, the authentication probability and communication overhead conflict with each other, that is, increasing the overhead will increase the authentication probability, and vice versa. Figure 4 shows the authentication probabilities under different communication overheads. Assuming the loss probability is 30%, the total number of packet is 1,024, each hash has 16 bytes and each signature has 128 bytes. For EMSS approach, the length of each edge is uniformly distributed in the interval [1,128]; Figure 5 shows that our proposed approach outperforms other approaches except the Erasure Code in terms of overhead and authentication probability. From the above figures, we can see that the NGBA outperforms existing approaches in terms of integrating overhead, robustness, authentication probability and receiver delay.

And then, to demonstrate the effectiveness of our proposed joint scheme, we plot the end-to-end rate-distortion curves for the test sequence at packet loss rate equal to 5% and 15%, respectively. The proposed resource allocation scheme (JAC+NGBA) is benchmarked against other two schemes:1) JAC+EMSS, in which the overall resource allocation is performed between source channel coding and authentication, but the resource within authentication

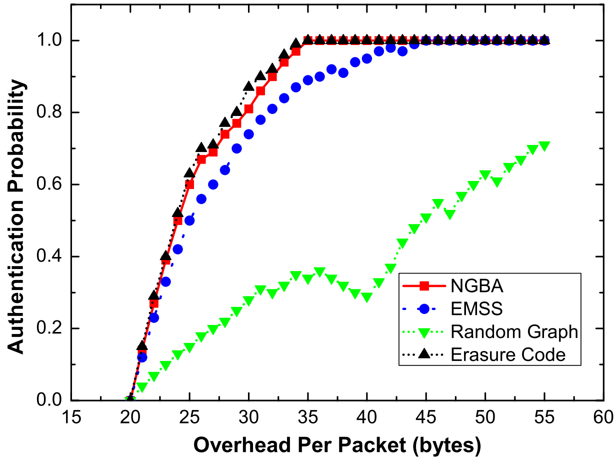


Fig. 4 Authentication probabilities at different overheads. (Packet loss probability is fixed at 30%)

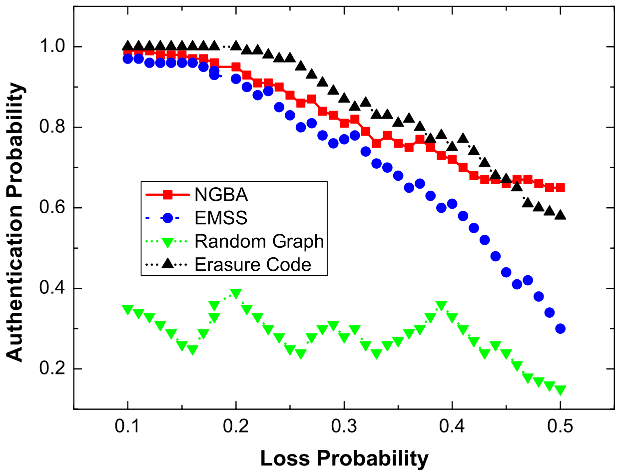


Fig. 5 Authentication probabilities at different loss probabilities. (The overheads is 30 bytes per packet)

is equally allocated using the basic EMSS scheme 2) JSCC+EMSS, in which the resource for source and channel coding is jointly allocated whereas that for authentication is fixed, and the basic EMSS is applied. Figure 6 shows the performance comparison between our proposed scheme and the competing schemes. The proposed JAC+NGBA scheme can be seen to achieve a much higher performance in terms of end-to-end PSNR compared to the competing schemes. When the packet loss rate is 5% and the overall rate ranges from 0.5 to 3, the average PSNR using the proposed scheme is 37.85 dB while it is 34.60 dB and 34.26 dB for the case of JAC+EMSS and JSCC+EMSS, thus, around 3.2–3.6 dB performance gain can be achieved on average using the proposed scheme. Similarly, when the packet loss rate is 15%, around 2.6–5.6 dB performance gain can be achieved on the average. It should be noted that JAC+EMSS also outperforms JSCC+EMSS, especially when the packet loss rate is high. For example, when the packet loss rate is 5%, the average performance gap is only 0.34 dB; while packet loss rate is 15%, the gap increases to 3.05 dB.

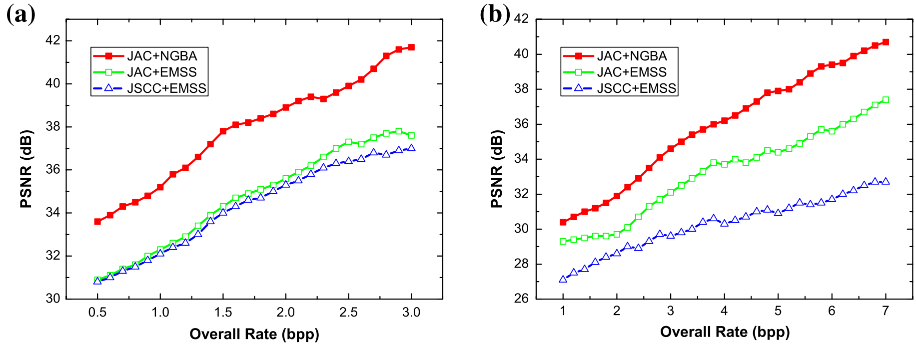


Fig. 6 End-to-end rate-distortion curves. (**a**) Packet loss rate is 5% ($r_a = 0.4$ for JSCC+EMSS). (**b**) Packet loss rate is 15% ($r_a = 0.25$ for JSCC+EMSS)

Table 1 JAC Rate under different P_B (overall rate=3bpp)

P_B	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
r_s	0.54	0.52	0.51	0.48	0.46	0.41	0.38	0.35	0.33	0.29	0.25
r_c	0.04	0.13	0.16	0.21	0.24	0.31	0.38	0.42	0.48	0.53	0.59
r_a	0.42	0.35	0.33	0.31	0.30	0.28	0.24	0.23	0.19	0.18	0.16
PSNR(dB)	41.7	41.1	40.6	40.1	39.3	38.8	37.8	36.9	36.0	35.4	34.6

Moreover, to examine how the JAC is affected by the channel condition, we fix the overall code rate and examine how r_s, r_c and r_a vary, as the packet loss rate increases from 5% to 15%. Table 1 illustrates the unitary results for the test sequence. From the table, we observe that when the channel condition is good, most of the bits are allocated for source coding and authentication. When the channel condition is poor, the large portion of bits is allocated for channel coding. As expected, the PSNR of reconstructed image decreases as packet loss rate increases.

5 Concluding Remarks

In this paper, we have been focusing on designing a joint authentication and coding system in order to achieve satisfactory authentication results and end-to-end reconstruction quality under the overall limited resource budget. The simulation results show the effectiveness of our joint authentication-coding scheme for multimedia over wireless networks.

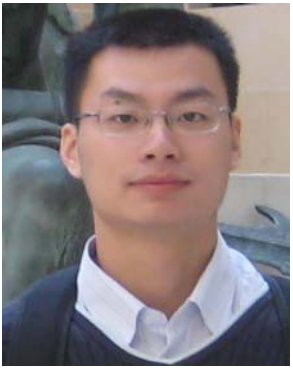
Acknowledgments This work is supported by the Key Project of Nature Science Foundation of Jiangsu (China) under Grant BK2007729 and the Climbing Plan in Nanjing University of Posts and Telecommunications under Grant NY207061. Moreover, we also thank the anonymous reviewers for insightful comments and suggestions.

References

1. Zhang, Z., Sun, Q., Wong, W.-C., et al. (2007). An optimal content-aware authentication scheme for streaming JPEG-2000 images over lossy networks. *IEEE Transactions on Multimedia, 9*(2), 320–331.
2. Wu, Y., & Deng, R. H. (2006). Scalable authentication of MPEG-4 Streams. *IEEE Trans. on Multimedia, 8*(1), 152–161.
3. Gennaro, R., Rohatgi, P. How to sign digital streams. In Advances in Cryptology-CRYPTO'97.

4. Peffig, A., Canetti, R., Tygar, J., et al. (2000). Efficient authentication and signing of multicast streams over lossy channels. In Proceedings of IEEE Symposium on Security and Privacy, 56–73.
5. Song, D., Zuckerman, D., & Tygar, J. (2002). Expander graphs for digital stream authentication and robust overlay networks. Proc. of IEEE Symposium on Research in Security and Privacy, 258–270.
6. Miner, S., & Staddon, J. (2001) Graph-based authentication of digital streams. Proc. of IEEE Symposium on Research in Security and Privacy, 232–246.
7. Park, J. M., Chong, E. K. P., & Siegel, H. J. (2003). Efficient multicast stream authentication using erasure codes. *ACM Transactions on Information System Security, 6*(2), 233–245.
8. Li, Z., Sun, Q., Lian, Y., & Chen, C. W. (2007). Joint source-channel-authentication resource allocation and unequal authenticity protection for multimedia over wireless networks. *IEEE Transactions on Multimedia, 9*(4), 837–850.
9. Zhang, Z., Sun, Q., Wong, W.-C., et al. (2007). Rate-distortion-authentication optimized streaming of authenticated video. IEEE Trans. *Circuits and Systems for Video Technology, 17*(5), 544–557.
10. Zhang, Z., Sun,Q., & Wong, W.-C. (2005). A proposal of butterfly-graph based stream authentication over lossy networks. IEEE International Conference on Multimedia and Expo, 4–10.
11. Miner, S. K., Staddon, J. (2001). Graph-based authentication of digital streams. IEEE Symposium on Security and Privacy, 232–246.
12. Fu, C.-M., Hwang, W.-L., et al. (2006). A joint source and channel coding algorithm for error resilient SPI-HT-Coded video bitstreams. *Journal of Visual Communication & Image Representation, 17*, 1164–1177.
13. Kim, J., Mersereau, R. M., & Altunbasak, Y. (2005). Distributed video streaming using multiple description coding and unequal error protection. *IEEE Transactions on Image Processing, 14*(7), 849–861.
14. Qu, Q., Pei, Y., et al. (2005). Cross-layer QoS control for video communications over wireless ad hoc networks. *EURASIP Journal on Wireless Communications and Networking, 5*, 743–756.
15. Sungdae, C., & Pearlman, W. A. (2002). A full-featured, error-resilient, scalable wavelet video codec based on the set partitioning in hierarchical trees (SPIHT) algorithm. *IEEE Transactions on Circuits and Systems for Video Technology, 12*(3), 157–171.

Author Biographies



Liang Zhou received B.S. and M.S. degrees in signal and information processing from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2003 and 2006, respectively, and now he is pursuing his Ph.D. degree in Shanghai Jiao Tong University, Shanghai, China. In 2007, he won the Eiffel Doctor Scholarship financed by France Government to study and research in Ecole Normale Superiéure (E.N.S.), Cachan, France. His research interests include wireless multimedia communication, cross-layer design etc.

Baoyu Zheng is currently the professor and doctor tutor both in Nanjing University of Posts and Telecommunications, Nanjing, China and Shanghai Jiao Tong University, Shanghai, China. His research interests include wireless communication and signal processing.

Anne Wei is HDR professor at the University of Paris XII. She has engaged in research on computer networks and mobile systems.

Benoît Geller is a professor at the LEI laboratory (E.N.S.T.A ParisTech). His research interests include information theory, and computer networks.

Jingwu Cui is the associate professor in Nanjing University of Posts and Telecommunications, Nanjing, China. Her research interests include signal processing and wireless communication.