RATE-DISTORTION-AUTHENTICATION OPTIMIZED STREAMING WITH MULTIPLE DEADLINES

Zhishou Zhang[1,2]*, Qibin Sun*[1]*, Wai-Choong Wong*[1,2]

[1]Institute for Infocomm Research, Singapore
[2]National University of Singapore, Singapore
{zszhang, qibin, lwong}@i2r.a-star.edu.sg;

John Apostolopoulos, Susie Wee

Hewlett-Packard Labs, USA
japos@hpl.hp.com, susie.wee@hp.com

ABSTRACT

Video streaming with authentication is practically important, where a packet is decoded only when it is both received and authenticated. Recent work examined the problem of Rate-Distortion-Authentication (R-D-A) optimized streaming of authenticated video. The original R-D-A technique assumes that each packet has only one deadline, its display deadline, and that a packet is not considered for transmission after its deadline. However, for video protected with an inter-packet graph-based authentication technique, a video packet can still be useful for verification of other packets even if it misses its own display deadline. We formulate the problem of multiple-deadline R-D-A optimized streaming and also propose ways to reduce the complexity. Simulation results using H.264 and NS-2 demonstrate that multiple-deadline R-D-A optimization achieves performance improvements of up to 4dB over single-deadline R-D-A optimization.

Index Terms**—**Video streaming, authentication, R-D-A optimization, authenticated video

1. INTRODUCTION

Video streaming is becoming increasingly important and popular, as well as the security issues related to video streaming. For instance, authentication is an important aspect of video streaming, as receivers require assurance for the integrity and the source origin of the received video. In particular, for authenticated video a packet is decoded only when it is both received and verified. Generic graph-based stream authentication methods like [1-5] usually impose overhead and dependency among packets for verification. Therefore, the application of conventional Rate-Distortion Optimized (RaDiO) [6] streaming technique, which do not account for the overhead and dependencies introducted by authentication, produce highly sub-optimal R-D performance for authenticated video. To tackle this problem, Rate-Distortion-Authentication (R-D-A) optimized streaming technique for authenticated video are proposed [8]. The R-D-A optimization is defined as the rate-distortion optimization for authenticated video, where the distortion is measured by the difference between the original video and the authenticated video, and the rate includes the rate used for both the coded video data and the authentication data. Given a video stream protected with a graph-based authentication method, the R-D-A optimized streaming technique computes a packet transmission schedule to optimize the video quality at the receiver, subject to a constraint on channel bandwidth. This is done by considering *authentication importance* and authentication *overhead size*, in addition to the original R-D dependency and parameters from the source used in [6].

The R-D-A optimization technique in [8] assumes each packet is associated with only one deadline, i.e., its display deadline, after which the packet will not be considered for transmission. However, using graph-based authentication, when a packet misses its display deadline, it might still be useful for verification of other packets which depend on it for authentication. As such, each packet is actually having multiple deadlines: the first one is its own display deadline, while the others are the display deadlines of those packets with authentication dependency on it.

In this paper, we extend the R-D-A Optimized Streaming technique by accounting for multiple deadlines. We formulate the multiple-deadline problem by computing the error probability and the resulting distortion with respects to every deadline. However, the optimization process has high complexity, due to the increased space over which we search for the best transmission policy. Therefore, we also propose ways to restrict the search to provide a useful tradeoff between performance and complexity.

This paper continues in Section 2 with a brief overview of the R-D-A Optimized streaming technique. Section 3 describe the formulation of the multiple-deadline problem, and also proposes ways to reduce the complexity. Section 4 presents experimental results and performance analysis. Finally, Section 5 concludes the paper.

2. RATE-DISTORTION-AUTHENTICATION OPTIMIZED STREAMING

An important recent advance in media streaming is the RaDiO framework [6] for streaming that compute the optimized packet transmission policy based on packets' size B, distortion increment Δd and display deadline T. The distortion increment is the amount by which the overall distortion will decrease if the packet is received before its display deadline. A packet received after its deadline will be not used for display.

In [8], we proposed an R-D-A optimized framework for streaming of authenticated video over a lossy network, which extends the RaDiO framework to incorporate another dimension for authentication. In addition to the original parameters considered in [6], the R-D-A optimized technique accounts for the authentication dependency and overhead size O. Here a packet is decoded only when it is both received and verified before its display deadline. In addition, similar to RaDiO, the R-D-A optimized technique also assumes a simple additive distortion model.

Suppose a packet P_l has M transmission opportunities before its deadline T_l, it is assigned a transmission policy π_l, an M-dimensional vector dictating whether or not it will be sent at each transmission opportunity. Associated with each π_l are the cost function $\rho(\pi_l)$ and the error function $\varepsilon(\pi_l)$, where the former is the expected number of transmissions and the latter is the probability that P_l is not received by its deadline.

Given a group of N packets consisting of one signature packet P_{sig} and N-1 normal packets connected by an authentication graph, the goal is find the optimized policy $\prod = [\pi_{sig}, \pi_0, ..., \pi_{N-2}]$ that minimizes the Lagrange cost function.

$$J(\prod) = D(\prod) + \lambda R(\prod) \qquad (1)$$

The expected distortion $D(\prod)$ is computed by accounting for packets' distortion increments, display deadline, packet loss probability, and authentication dependency. The expected rate $R(\prod)$ accounts for both the coded video data and authentication overhead.

Similar to [6], the R-D-A optimization problem is solved with an iterative descent algorithm, i.e., optimizing the policy for one packet at a time while keeping the other packets' policy fixed, until the Lagrange value converges. For instance, the policy for packet P_l can be decided by (2).

$$\pi_l^* = \arg\min_{\pi_l} \varepsilon(\pi_l) + \lambda_l' \rho(\pi_l) \qquad (2)$$

In this case, the multiplier $\lambda_l' = \lambda(B_l + O_l)/(SA_l + SD_l)$ controls the trade-off between the error and cost, where the term SD_l, the *decoding importance*, is the expected distortion increments due to the unsuccessful decoding of packet P_l itself, while the term SA_l, the *authentication importance*, is the expected distortion increments due to reduced verification probability of other packets with authentication dependency on P_l.

There are a number of popular graph-based authentication methods [1-5] and each has a unique dependency structure and authentication overhead. Some authentication methods [1-3] enable closed-form computation of verification probability and it is straightforward to use them within the R-D-A optimization framework. However, other methods [4-5] do not allow closed-form computation of verification probability. Nevertheless, one can still take a simulation-based approach to estimate the verification probability. In this paper we employ the Butterfly Authentication method [1].

The main high-level differences between RaDiO [6] and R-D-A optimized framework [8] are briefly summarized. First R-D-A is an extension of RaDiO designed for streaming of authenticated video where a packet received but not verified is not decoded or used for display. While RaDiO accounts for coding dependencies and R-D parameters only from the source, the R-D-A framework also accounts for the authentication graph dependencies and associated overhead.

3. R-D-A OPTIMIZED STREAMING WITH MULTIPLE DEADLINES

This section describes how to formulate the R-D-A optimization problem with multiple deadlines. The multiple-deadline problem for conventional streaming in RaDiO framework was examined in [9]. Here we highlight the difference for authenticated video. Considering the high complexity that comes with the multiple-deadline problem, we also propose how to reduce the complexity.

3.1. Problem Formulation

Using graph-based authentication, a packet P_l may be used to verify a number of other packets, which are referred to as the *dependent set* Φ_l of P_l. Therefore, assuming all packets in Φ_l have a later display deadline, packet P_l is associated with $|\Phi_l|+1$ deadlines, the first one is its own display deadline and the others are display deadlines of the packets in Φ_l. Accordingly, packet P_l will have $|\Phi_l|+1$ error probabilities and $\varepsilon(\pi_l, l')$ is used to denote the probability that P_l does not arrive by the display deadline of packet $P_{l'}$.

As in the existing R-D-A optimized framework, we still use iterative descent algorithm to search for the optimized policy. For each packet, the optimized policy is determined by (3).

$$\pi_l^* = \arg\min_{\pi_l} \rho(\pi_l) + \sum_{P_{l'}=P_l \ \text{or} \ P_{l'}\in\Phi_l} v_{l,l'} \varepsilon(\pi_l, l') \qquad (3)$$

The term $v_{l,l'}$ can be computed by $v_{l,l'} = (SA_{l,l'} + SD_{l,l'})/\lambda(B_l + O_l)$, where $SA_{l,l'}$ and $SD_{l,l'}$ are the authentication importance and decoding importance of packet P_l with respect to the display deadline of $P_{l'}$. Note the decoding importance is zero for all deadlines except the first one, as we assume the error concealment and coding dependency are implicitly accounted for by the distortion increment Δd_l as in [7]. The decoding importance is computed using (4), where V_l is the verification probability of P_l and $\varepsilon(\pi_{sig}, l')$ is the error probability of the signature packet.

$$SD_{l,l'} = \begin{cases} (1-\varepsilon(\pi_{sig}, l'))V_l \Delta d_l & l = l' \\ 0 & otherwise \end{cases} \quad (4)$$

The arrival of packet P_l will benefit the verification of the packets in Φ_l with display deadline later than or equal to the arrival time of P_l. Thus, the authentication importance $SA_{l,l'}$ can be computed using (5), where $\alpha_l^{l''}$ is the influence packet P_l has on the verification probability of packet $P_{l''}$.

$$SA_{l,l'} = (1-\varepsilon(\pi_{sig}, l')) \sum_{P_{l''}:T_{l''}=T_{l'}} \alpha_l^{l''} (1-\varepsilon(\pi_{l''}, l'))\Delta d_{l'} \quad (5)$$

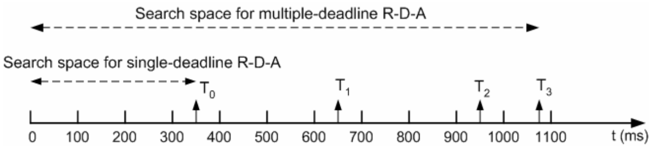

Fig. 1 – Search space in single-deadline and multiple-deadline R-D-A optimization (transmission interval = 100ms)

Suppose a packet has 4 deadlines, out of which the first deadline is its display deadline T_0, as shown in Fig. 1. In single-deadline R-D-A optimization, the packet is only considered for transmission in the first 4 transmission opportunities, while in multiple-deadline R-D-A optimization, it is still considered for transmission even after T_0. This will increase the verification probability of other packets with dependence on the given packet, and therefore improve the quality of the authenticated video.

On the other hand, the consideration of multiple deadlines drastically increases the complexity, as the search space grows exponentially with the number of transmission opportunities. This is illustrated in Fig. 1, where in this example the multiple-deadline R-D-A optimization has to search 2^{10} possible transmission policies, compared with 2^4 possibilities for single-deadline case.

3.2. Reducing Complexity

We next examine a number of methods to reduce the complexity associated with multiple-deadline R-D-A optimization. The first method (referred to as *window-split* method) is to split the transmission window into two segments: the first segment lasts until T_0-k and the second segment starts from T_0-k and ends at the last deadline, where k is the minimum forward propagation delay. In each time segment, the R-D-A optimization searches transmission possibilities within the segment only, although it still accounts for multiple error probabilities with respect to all deadlines. This greatly reduces the search space, e.g., the search space is reduced from 2^{10} to 2^4+2^6 in Fig. 1.

The single-deadline R-D-A optimization method seldom transmits a packet in the time interval [T_0-t_{avg}, T_0], as transmission in this interval does not increase the probability of being received before T_0, where t_{avg} is the average forward transmission time. However, the window-split method still transmits the packet in this interval due to two reasons: (1) The consideration of multiple deadlines increases the authentication importance of those packets with a large number of dependent packets and therefore increases its chance of being transmitted; (2) In the first segment, the window-split method assumes no transmission after deadline T_0 (while in fact there can still be transmissions after T_0) and therefore it forces the transmission of a packet even as it approaches T_0, adversely effecting other packets whos deadlines have not yet been reached.

We also found that the gain from transmitting a packet after its first deadline T_0 decays very fast. Therefore, we propose the second method (referred to as *extended-window* method) to simply extend the transmission window to time T_W, where $T_0 \leq T_W \leq T_M$, where T_M is the last deadline. A packet is not considered for transmission after T_W. The length of the extended window is chosen so that it has acceptable complexity while still maintaining most of the gain from the use of multiple deadlines.

4. EXPERIMENTAL RESULTS

We implements three R-D-A optimization methods: (1) single-deadline (SD); (2) multiple-deadline with window-split; (3) multiple-deadline with extended-window. The packet loss and delay are random and independent in the forward and backward channel. Packet loss follows an IID erasure model and we measure the performance at loss rate e=0.03, 0.1 and 0.2. Packet delay follows a shifted Gamma distribution with shift k=50ms, mean μ=100ms and variance σ=13.5ms. The interval between two consecutive transmission opportunities is 100ms and the buffer delay is 400ms. NS-2 [10] is used for simulating the network loss and delay.

Two QCIF video sequences, *foreman* (400 frames) and *container* (300 frames), are encoded using H.264/AVC reference software JM 10.2 [11] at approximately 150Kbps and 70Kbps respectively. The frame rate is 30 f/s and each GOP comprises one I-frame followed by 14 P-frames. A frame can be divided into one or more NAL units in order to fit into a network packet. The Butterfly Authentication method [1] is used for authenticating the video stream. A signature is amortized among a group of 33 consecutive packets (corresponding to about one-second of video). In total, the authentication overhead constitutes around 8Kbps on top of the coded rate of the video.

Table 1 – Statistics of packet transmission, delivery and verification (Forman, loss rate = 0.1)

Algorithm Tested	BW(Kbps)	No. of tx / pkt	Before T_0 (%)	No. of rx / pkt	Before T_0 (%)	Rx prob. before T_0 (%)	Veri. Prob. (%)	% of pkt sent after T_0
			After T_0 (%)					
			In [T_0-k, T_0] (%)		After T_0 (%)			
Single Deadline R-D-A	199	1.278	100	1.015	98.53	79.34	98.5	0
			0					
			0.37		1.47			
Multiple Deadline _Window_Split	198	1.113	99.1	0.9997	96.33	80.4	99.3	4.5
			0.9					
			1.34		3.67			
Multiple Deadline _Extended_Window	196	1.11	99.01	0.9967	96.36	80.36	99.5	4.9
			0.99					
			1.28		3.64			

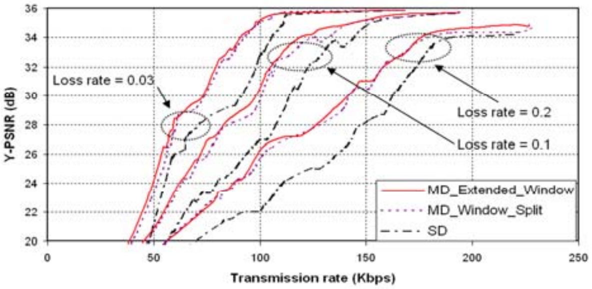

Fig. 2 – Rate-distortion curves for *Container* sequence for SD, MD_Window_Split and MD_Extended_Window

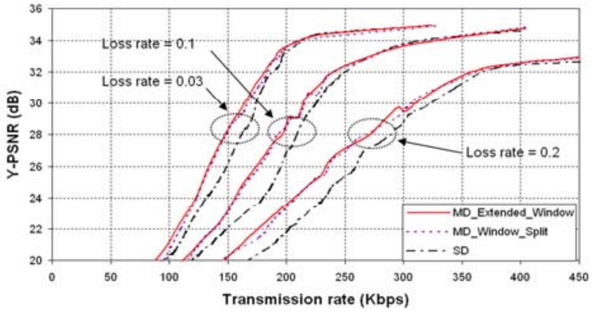

Fig. 3 – Rate-distortion curves for *Foreman* sequence for SD, MD_Window_Split and MD_Extended_Window

Fig. 2 and Fig. 3 compare the PSNR performance of the three methods using *Foreman* and *Container*. The two multiple-deadline methods outperform the single-deadline method by up to 4dB. The reason can be found from the statistics in Table 1. The window-split method and extended window method have higher verification probability than the single-deadline method, due to re-transmission of expired but still important packets. Note that while the single-deadline method has a higher fraction of its received packets delivered before the display deadline, its receiving probability before display deadline is lower than the other two. This results from an unbalanced bandwidth distribution, i.e., certain packets are given too much bandwidth, while other packets are starved. This occurs because some packets never get a chance to be transmitted, as the packet(s) they depend on for verification is either lost or not transmitted, and then the single deadline R-D-A algorithm realizes that the packet in question should not be transmitted, given single-deadline constraint. The multiple-deadline R-D-A algorithm provides valuable transmission flexibility which overcomes the above inefficiencies. It is also interesting to note that the two multiple deadline algorithms transmit a sizable percentage of the packets after their display deadline (4.5% and 4.9%).

5. CONCLUSIONS

This paper extends the R-D-A optimized framework to allow the consideration of multiple deadlines introduced by inter-packet graph-based authentication. Incorporation of multiple deadlines improves the performance by up to 4dB over the original single-deadline method. As the Butterfly graph [1] has high robustness against packet loss, the benefit from re-transmitting lost packets is somewhat limited. Therefore, the performance gain may be even larger for other authentication methods like Simple Hash Chain [2].

6. REFERENCES

[1] Z. Zhang, Q. Sun and W.C. Wong, “A proposal of butterfly-graph based stream authentication over lossy networks,” ICME’05.

[2] R. Gennaro and P. Rohatgi, “How to sign digital streams,” CRYPTO’97.

[3] C.K. Wong and S. Lam, “Digital Signature for Flows and Multicasts,” IEEE/ACM Trans. On Networking, August 1999.

[4] A. Perrig, R. Canetti, J. Tygar and D. Song, “Efficient authentication and signing of multicast streams over lossy channels,” IEEE Symposium on Security and Privacy, 2000.

[5] P. Golle and N. Modadugu, “Authenticating streamed data in the presence of random packet loss,” ISOC Network and Distributed System Security Symposium, 2001.

[6] P.A. Chou and Z. Miao, “Rate-distortion optimized streaming of packetized media,” IEEE Trans. On Multimedia, April 2006.

[7] J. Chakareski, J. Apostolopoulos, S. Wee, W.-T. Tan, and B. Girod, “Rate-distortion hint tracks for adaptive video streaming,” IEEE Trans. on CSVT, Oct. 2005.

[8] Z. Zhang, Q. Sun, W.-C. Wong, J. Apostolopoulos and S. Wee, “Rate-Distortion Optimized Streaming of Authenticated Video” ICIP’06.

[9] M. Kalman, P. Ramanathan, and B. Girod, "Rate-Distortion Optimized Streaming with Multiple Deadlines," ICIP’03.

[10] The Network Simulator (NS-2), http://www.isi.edu/nsnam/ns/

[11] H.264/AVC Reference Software, JM Version 10.2, http://iphome.hhi.de/suehring/tml