Maximizing Privacy in Variable Bit Rate Coding

Jiyun Yao
ECE Department
Lehigh University
Email: jiy312@lehigh.edu

Parv Venkitasubramaniam
ECE Department
Lehigh University
Email: parv.v@lehigh.edu

I. ABSTRACT

Variable Bitrate Coding (VBR) has shown to be an advantageous method of encoding data streams, with particular application to speech, audio and video streams. While the primary disadvantage of VBR has long been considered as the increasing encoding complexity, recent research into traffic analysis of VBR coded audio streams has exposed an important privacy vulnerability wherein an eavesdropper can utilize the observed length of VBR encoded data packets and determine the contents of the communication such as spoken words and audio. In this work, the privacy-utility tradeoff for VBR coding is studied from a theoretical foundational perspective. Specifically, the data source is modeled a mixture distribution, wherein the length of the encoded data packet is varied to maintain a constant quality (distortion) with respect to the source. Using Shannon's equivocation as a measure of data privacy, the tradeoff between privacy and utility (as measured by delay and overall bit rate) of VBR is investigated analytically. In particular, the tradeoffs are expressed as classical information theoretic rate distortion functions, which shed light into methods to increase the privacy of VBR encoded data without compromising on the desired output fidelity.

Keywords: Variable bit rate coding, privacy, markov decision process, rate distortion

II. INTRODUCTION

Traffic analysis, a technique where eavesdroppers monitor the transmission of encrypted data packets over a network and extract information about the communication or communicating parties using characteristics such as transmission timing, packet lengths, protocol headers and suchlike, has long been applied to compromise the privacy of network users. In the past decade, the use of packet timing and lengths to compromise user identities and passwords has been demonstrated over HTTP [1] and SSH protocols [2]. Consequently, anonymous networks, inspired by the idea of mixing proposed by David Chaum [3], have been deployed over networks to enable the protection of user identities and paths of data flow over networks.

A key requirement in mix based networks is the addition of random "dummy" bits to the data so that the packet lengths are identical thus preventing any information retrieval therefrom. The downside of this requirement is that it negates any possible utility achievable though variable bit rate coding (VBR). This raises some important questions: Is it possible to prevent information retrieval from packet lengths whilst achieving the desired utility from variable bit rate coding? Alternatively, what is the loss in utility of VBR necessary to achieve a desired degree of privacy? More generally, is there a tradeoff between privacy and utility in the context of variable bit rate coding? In this work, we address this question from a theoretical standpoint.

Variable bit rate coding is extensively used in the encoding of media streams. Modern media encoding standards such as MP3, AAC and WMA for audio, and MPEG2, XVid, Theora, H264 for video and CELP for speech employ VBR to enable a constant quality transmission at minimum overall bit rate [4]–[6]. The use of packet lengths to extract data from encrypted VoIP conversations has been studied in [7]–[11]. Researchers have shown that the packet lengths can be used to determine the language of a conversation [7], identify the speakers [8] and also determine presence of known phrases within the call [9]. The most telling of these investigations, in [10], show that one can segment a sequence of packet sizes into subsequences corresponding to individual phonemes, and further segment the phonetic transcript into word boundaries, consequently providing a hypothesized transcript of the conversation. The two critical design decisions that has led to this information retrieval are the use of VBR codecs for speech coupled with length preserving stream ciphers for encryption [6], which together result in a high correlation between content and packet length.

Our work is focused on studying the privacy achievability for the class of VBR applications where different source data are encoded at different bit rates to maintain a constant quality, a key requirement in effective multimedia transmission. Modelling the input as a stochastic source of symbols, we study a bit padding based privacy encoder: Here, each source symbol could be encoded at a higher rate (thus losing utility) to match another symbol thus creating uncertainty about the transmitted symbol. In particular, we demonstrate that the optimal solution can be determined using a classical information theoretic rate-distortion optimization when the source is memoryless. For a Markov modelled source, as is common in speech coding, we provide lower and upper bounds on the maximum achievable privacy using rate-distortion optimizations. We also propose an *instantaneous privacy* measure for stochastic sources, and show that our method achieves the maximum instantaneous

privacy for Markov sources as well. The paper is organized as follows. The mathematical model and the definition of privacy in the context are described in Section III. The encoder for memoryless sources and the corresponding maximization of privacy are provided in Section IV. The extension to Markov modelled sources, including an alternative measure for instantaneous privacy, is presented in Section V, followed by conclusions in Section VI.

III. Mathematical Model

Consider a source alphabet $\mathcal{S} = \{s_1, s_2, \cdots, s_S\}$. Each $s_i \in \mathcal{S}$ corresponds to one class of elementary units in the media stream. For instance, an s_i could refer to a phoneme in a speech transmission. Each class is encoded at a different rate to maintain constant quality across classes. For each class, we define a quality-packet length function $l_i : \mathcal{R} \mapsto \mathcal{Z}^+$, where $l_i(q)$ is the number of bits required to encode (and encrypt) data from class s_i at quality level q. The actual realization of the function would depend on the application, and we assume that the eavesdropper has perfect knowledge of the functions.

Arrival Process: Let $X_1, \cdots, X_n$ denote the random variables representing the sequence of classes of source symbols that arrive to the encoder. We model the sequence of source symbols as being generated by a stochastic source. In this work, we consider the special case of a Markov modelled source, where the class distribution satisfies

$$\Pr\{X_n | X_1, \cdots, X_{n-1}\} = \Pr\{X_n | X_{n-1} \forall n\}$$

Let the transition probability matrix of the homogenous Markov source be denoted by $\mathbf{P} = \{p_{ij}\}_{i,j}$. In other words, $p_{i,j} = \Pr\{X_n = j | X_{n-1} = i\}$. We consider the transition matrix to be irreducible and aperiodic and the source to be stationary.

Encoder: In practice, the job of the encoder is to decide the type of code used on each arrived source symbol depending on the quality and privacy requirements. Although, a uniform quality is desired across all classes of symbols, for privacy reasons, the encoder would be required to encode a given symbol using a higher bit rate code than required for the desired quality. Keeping these in perspective, we model the encoder as a sequence of mappings from source symbols to packet lengths. Specifically, an encoder E is specified as a sequence of functions $E_n : \mathcal{S} \times \mathcal{S}^{n-1} \mapsto \mathcal{Z}$. Where $l_n = E_n(x_n | x_1, \cdots, x_{n-1})$ denotes the length of the n^{th} packet transmitted by the encoder when the sequence of symbols belonging to classes $x_1, \cdots, x_n$ respectively arrive. Note that E_n could be a random mapping; in other words, each E_n can be represented as a collection of deterministic mappings with an associated probability distribution function.

Privacy: Let N denote the random variable that represents the number of source symbols in the stream. Correspondingly, let $X_1, \cdots, X_N$ denote the random variables representing the sequence of classes of source symbols that arrive to the encoder. Then, we quantify the privacy of a specific encoder E using entropy:

$$\mathcal{P}(E) = \frac{\mathbb{E}(H(X_1, \cdots, X_N | E(X_1, \cdots, X_N)))}{\mathbb{E}(N)}$$

where the expectation is over the arrival process and the length of the stream. The metric as defined above is bounded in $[0, h(\mathbf{p})]$ where

$$h(\mathbf{p}) = -\sum_i p_i \log p_i$$

is the entropy of the source probability distribution.

It is evident that the existing approach to VBR coding, where each class of symbols are encoded using the minimum bit rate required to maintain quality would provide minimum privacy. Our goal, in this work, is to study the design of encoders to maximize privacy given a constraint in the overhead. The type and level of overhead considered would limit the class of encoders to choose from and consequently determine the maximum achievable privacy within that class. In this work, we consider a bit-padded encoder, where the rate of coding is increased to create uncertainty amongst symbols across different classes.

IV. Bit Padded Encoder

Since the length of the encoded packet reveals the class of symbols thus compromising privacy, an obvious approach to increase privacy is to pad additional bits to each packet thus creating uncertainty for the eavesdropper. They key question is: given a constraint on the bit overhead what is the maximum achievable privacy? In the following exposition, we demonstrate that the optimal solution can be determined using a rate distortion optimization.

Let the desired quality of encoding be q. Then, the minimum length required to encode a symbol from class i is given by $l_i(q)$. We assume the encoder does not add delay to the system, and any encoder should transmit the encoded symbol as soon as it arrives (assuming negligible processing time). Since the arrivals are independent, it is sufficient to design a single encoder E_1 that processes a single symbol. Therefore, the bit overhead for any encoder E would be measured by the expected number of bits added by the encoder per symbol:

$$O(E, q) = \sum_i p(i) \mathbb{E}(E_1(s_i) - l_i(q)). \tag{1}$$

where the expectation is over the randomness in the encoder E_1. Further, the privacy of a bit-padded encoder, if the sources are independent, can be expressed as:

$$\mathcal{P}_{bit}(E) = \mathbb{E}(H(X | E_1(X)),$$

where the expectation is over the arrival process and the randomness in the encoder E_1. Note that even if the sources generate independent symbols, it is possible for an encoder to have a time varying algorithm thus forcing a dependence on the eavesdroppers observation across multiple symbols, in which case, the above definition of privacy would be invalid. For any encoder with memory, however, it is possible to design

a time invariant encoder with equal or greater privacy by using the marginal distribution of the encoder, since conditioning reduces entropy ($H(X_2|X_1) \leq H(X_2)$).

Our goal is to determine the maximum privacy subject to a constraint on the overhead:

$$\mathcal{P}^*_{bit}(o_{\max}) = \sup_{E:O(E,q)\leq o_{\max}} \mathcal{P}_{bit}(E).$$

When the sources are independent, this problem has been solved in [12]. The solution is described here. Let $\beta = \{\beta_{ij}\}$ be an arbitrary conditional probability distribution over $\mathcal{S}\times\mathcal{S}$. Consider a random encoder $E_1^{\beta}(s_i) = l_j(q)$ with probability β_{ij}. Let $\mathcal{E}^1 = \{E : E = E_1^{\beta} \text{ for some } \beta\}$ denote the subset of encoders formed by varying the conditional distribution β across the probability simplex. Define a distortion function:

$$d_{ij} = \begin{cases} l_j(q) - l_i(q) & l_i(q) \leq l_j(q) \\ \infty & \text{o.w.} \end{cases} \quad (2)$$

The optimal encoder within the subset $\mathcal{E}^1$ can then be determined using a rate distortion optimization:

$$\begin{aligned} \mathcal{P}^1_{bit}(o_{\max}, q) &\stackrel{\triangle}{=} \sup_{E\in\mathcal{E}^1, O(E,q)\leq o_{\max}} \mathcal{P}_{bit}(E) \\ &= \sup_{\beta_{ij}:\sum_{i,j} p_i\beta_{ij}d_{ij}\leq o_{\max}} H(X|E_1(X)) \quad (3) \end{aligned}$$

The result in [12] proves that the optimization within the subset yields the maximum privacy of a bit padded encoder, and the result is stated here as is relevant to this work.

Theorem 1: (from [12])

$$\mathcal{P}^*_{bit}(o_{\max}, q) = \mathcal{P}^1_{bit}(o_{\max}, q)$$

For a two class source, the optimal tradeoff has a closed form characterization obtained by solving the rate-distortion optimization.

Corollary 1: For a two class system, the maximum privacy is given by:

$$\mathcal{P}^*_{bit}(o_{\max}, q) = (p_1p^* + p_2)h\left(\frac{p_1p^*}{p_1p^* + p_2}\right)$$

where $h(p) = -p\log p - (1-p)\log(1-p)$ is the binary entropy and

$$p^* = \frac{o_{\max}}{l_2(q) - l_1(q)}.$$

V. Stochastic Source Model

When the source alphabets are not independently distributed, and instead follow a stochastic model, (3) no longer provides the optimal solution. Indeed, a stochastic source model would require consideration of the information gathered by the eavesdropper over the entire time horizon to decode a single class. In [12], the authors consider a causal privacy metric, wherein future arrivals are not used to determine the present source symbol. In the application considered here, we do not limit that capability. In such a scenario it can be shown that the expected privacy per slot can be expressed as a difference between the prior and posterior entropy of the expected output:

$$\mathcal{P}_{bit}(E) = \lim_{n\to\infty} \frac{\mathcal{E}(H_X + \sum_{i=1}^n (H(Y_i|Y^{i-1}, X_n) - H(Y_i|Y^{i-1})))}{n}$$

where H_X is the entropy rate of the Markov source. The above privacy function is a non linear yet convex function of the probabilistic encoding function $\{q^n_{i,j}\}$ at step n. Furthermore, the probabilistic encoding will result in dynamic privacy reward function at each step, and the optimal sequential encoder can be solved for using a $\rho-$POMDP as in [13]. In this work, we provide bounds on the optimal tradeoff that are easily computable for a Markov source.

In order to determine an upper bound, it is useful to define a weaker notion of privacy catering to such applications. This notion of *instantaneous privacy* appeals to a "causal" eavesdropper who is only allowed to use past history in determining the class of an observed source packet, but not the future arrivals. Accordingly, the definition is as follows:

Instantaneous Privacy: We define instantaneous privacy of an encoder E as:

$$\mathcal{IP}(E) = \frac{\sum_{n=1}^N \mathbb{E}(H(X_n|X_1, \cdots, X_{n-1}, E(X_1, \cdots, X_n))}{\mathbb{E}(N)}$$

where the expectation is over the arrival process and the length of the stream.

Under these assumptions, we design an encoder that maximizes instantaneous privacy subject to a constraint on the overhead. The result is a generalization of Theorem 1 by applying the Markov model to compute the entropy of a stochastic process and allocating overhead to different underlying distributions. Specifically, let $\mathbf{p}_i = [p_{i,1}\ p_{i,2}\ \cdots\ p_{i,S}]$ denote the i^{th} row of the transition probability matrix $\mathbf{P}$ for the Markov source. The following theorem characterizes the maximum achievable instantaneous privacy for a Markov Source.

Theorem 2: Let $\mathcal{P}^*_{bit}(o_{\max}, q, \mathbf{p})$ denote the maximum achievable privacy for a source distributed i.i.d according to $\mathbf{p}$ and maximum allowable overhead $o_{\max}$. Then, for a Markov source with transition probability matrix $\mathbf{P}$, the maximum achievable instantaneous privacy by a bit padded encoder is given by:

$$\mathcal{IP}^*_{bit}(o_{\max}, q) = \sum_{i=1}^S \pi_i \mathcal{P}^*_{bit}(o^*_i, q, \mathbf{p}_i),$$

where $\pi = \{\pi_1, \cdots, \pi_S\}$ is the stationary distribution of the Markov source and $\{o^*_1, \cdots, o^*_S\}$ is the unique positive vector that satisfies $\sum_i \pi_i o_i = o_{\max}$ and:

$$\frac{\partial \mathcal{P}^*_{bit}(o^*_i, q, \mathbf{p}_i)}{\partial o_i} = \frac{\partial \mathcal{P}^*_{bit}(o^*_j, q, \mathbf{p}_i)}{\partial o_j} \forall i, j$$

Proof: Since we consider the Markov chain to be stationary, and the forward decision of any encoder is necessarily causal, we can argue that $X_n - E(X_1, \cdots, X_n), X_{n-1} - X_1, \cdots, X_{n-2}$ form a Markov string. In other words, $\Pr\{X_n|E(X_1, \cdots, X_n), X_{n-1}, X_1, \cdots, X_{n-1}\} = \Pr\{X_n|E(X_1, \cdots, X_n), X_{n-1}\}$.

Using the argument identical to that in the proof of Theorem 1, were the encoder to consider classes of arrivals prior to X_{n-1} in determining the length of the X_n packet, then the observation would reveal more information about past arrivals without affecting the overhead, thereby reducing privacy at no reduction in overhead. It is therefore sufficient for an encoder to determine the length of a packet as a function of X_n and X_{n-1}. The instantaneous privacy can then be rewritten as:

$$\mathcal{P}_I(E) = \frac{\sum_{n=1}^{N} \mathbb{E}(H(X_n|X_{n-1}, E_2(X_{n-1}, X_n)}{\mathbb{E}(N)}$$

which when applying the stationarity of the source reduces to:

$$\mathcal{P}_I(E) = \sum_{i=1}^{S} \pi_i H(X_n|X_{n-1} = i, E_2(X_{n-1} = i, X_n))$$

The remainder of the proof involves allocating the overhead to each underlying entropy maximization $H(X_n|X_{n-1} = i, E_2(X_{n-1} = i, X_n))$ such that the overall privacy is maximized. Since the distortion constraint is linear, the resulting optimal allocation reduces to equating the partial derivatives of the corresponding rate distortion functions. Details of the proof are omitted in this submission due to paucity of space. □

Bounds on Maximum Privacy While instantaneous privacy captures a specific kind of application where information has an expiration time, the approach outlined previously can be used to provide bounds for the general definition of privacy in Section III. Specifically, since the instantaneous privacy represents a particular kind of adversary who does not utilize future observations to determine the class of a particular source packet, the maximum instantaneous privacy provides an upper bound on the maximum achievable (general) privacy. A lower bound can be similarly obtained by empowering the adversary to have perfect knowledge of future arrivals in determining the class of a particular source packet. Specifically, let $p'(i,j,k) = \Pr\{X_n = j | X_{n-1} = i, X_{n+1} = k\}$ denote the two-sided transition probability and $\mathbf{p}'_{i,k} = \{p'(i,\cdot,k)\}$ denote the probability mass function for a source arrival conditioned on a past and future observation. Correspondingly, a stationary distribution exists, for a pair of past and future observations; let $\pi'_{i,k} = \Pr\{X_{n-1} = i, X_{n+1} = k\}$ denote that stationary probability.

Theorem 3: Let $\mathcal{P}^*(o_{\max}, q, \mathbf{p})$ denote the maximum achievable privacy for an underlying i.i.d source distributed according to $\mathbf{p}$ and maximum allowable overhead $o_{\max}$. Then, for a Markov source with transition probability matrix $\mathbf{P}$, the maximum achievable privacy $\mathcal{P}^*_{bit}(o_{\max}, q, \mathbf{P})$ is bounded as

$$\sum_{i,j} \pi'_{i,j} \mathcal{P}^*_{bit}(o^*_{i,k}, q, \mathbf{p}'_{i,k}) \leq \mathcal{P}^*_{bit}(o_{\max}, q) \leq \sum_i \pi_i \mathcal{P}^*(o^*_i, q, \mathbf{p}_i).$$

Proof: Extension of the proof of Theorem 2. □.

Note that the bounds are not tight, and the optimal privacy for a given overhead constraint remains an open problem. In particular, the difficulty in solving the problem lies in the ability of the adversary to obtain information from future observations, which at the time of transmission is not available to the encoder. In general, the problem can be modelled as a Partially Observable Markov Decision Process (PoMDP); however, in contrast to the classical PoMDP model, the reward is not linear in the probability of the system state. The problem is also similar to the causal source coding problem, which also remains open for the scenario when instantaneous decoding is not necessary [14].

For a two class source, the bounds on the general privacy can be characterized in closed-form, given by the following corollary:

Corollary 2: For a two class source with transition probability matrix $\mathbf{P} = \begin{bmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{bmatrix}$, the maximum privacy can be bounded as:

$$\mathcal{P}_{lb}(o_{\max}, q, \mathbf{P}) \leq \mathcal{P}^*_{bit}(o_{\max}, q, \mathbf{P}) \leq \mathcal{P}_{ub}(o_{\max}, q, \mathbf{P})$$

where $\gamma = o_{\max}\frac{\alpha+\beta}{\beta}$ and

$$\begin{aligned}
&= \frac{\beta}{\alpha+\beta}\left[\gamma(1-\alpha)^2 + \alpha\beta\right] \cdot h\left(\frac{\gamma(1-\alpha)^2}{\gamma(1-\alpha)^2 + \alpha\beta}\right) \\
&+ \frac{\beta}{\alpha+\beta}\left[\gamma\alpha(1-\alpha) + \alpha(1-\beta)\right] \cdot h\left(\frac{\gamma\alpha(1-\alpha)}{\gamma\alpha(1-\alpha) + \alpha(1-\beta)}\right) \\
&+ \frac{\alpha}{\alpha+\beta}\left[\gamma\beta(1-\alpha) + \beta(1-\beta)\right] \cdot h\left(\frac{\gamma\beta(1-\alpha)}{\gamma\beta(1-\alpha) + \beta(1-\beta)}\right) \\
&+ \frac{\alpha}{\alpha+\beta}\left[\gamma\beta\alpha + (1-\beta)^2\right] \cdot h\left(\frac{\gamma\beta\alpha}{\gamma\beta\alpha + (1-\beta)^2}\right) \qquad (4)
\end{aligned}$$

$$\begin{aligned}
\mathcal{P}_{ub}(o_{\max}, q) =& \frac{\beta}{\alpha+\beta}[\gamma(1-\alpha) + \alpha] \cdot h\left(\frac{\gamma(1-\alpha)}{\gamma(1-\alpha) + \alpha}\right) \\
&+ \frac{\alpha}{\alpha+\beta}[\gamma\beta + (1-\beta)] \cdot h\left(\frac{\gamma\beta}{\gamma\beta + (1-\beta)}\right) \qquad (5)
\end{aligned}$$

VI. Conclusions

In this work, we studied a privacy problem in Variable Bit Rate coding wherein the length of the packet provides information about an underlying parameter that generates the data in each packet. Using an entropy-based definition of privacy, we demonstrated a method of increasing the privacy by padding bits at the cost of higher rate. In particular, we demonstrated that the tradeoff is expressible using classical rate-distortion functions.

VII. Acknowledgements

This work was supported in part by the National Science Foundations through the grants CCF-1149495 and CNS-1117701.

References

[1] Marc Liberatore and Brian Neil Levine, "Inferring the source of encrypted http connections," in *Proceedings of the 13th ACM conference on Computer and communications security*, New York, NY, USA, 2006, CCS '06, pp. 255–263, ACM.

[2] D. X. Song, D. Wagner, and X. Tian, "Timing Analysis of Keystrokes and Timing Attacks on SSH," in *Proc. 10th USENIX Security Symposium*, 2001.

[3] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, February 1981.

[4] Mark W. Garrett and Walter Willinger, "Analysis, modeling and generation of self-similar vbr video traffic," *SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 269–280, Oct. 1994.

[5] Marina Brandenburg, Karlheinz; Bosi, "Overview of mpeg audio: Current and future standards for low bit-rate audio coding," *J. Audio Eng. Soc*, vol. 45, no. 1/2, pp. 4–21, 1997.

[6] M. Schroeder and B. Atal, "Code-excited linear prediction(celp): High-quality speech at very low bit rates," in *Acoustics, Speech, and Signal Processing, IEEE International Conference on ICASSP '85.*, apr 1985, vol. 10, pp. 937 – 940.

[7] C.V. Wright, L. Ballard, F. Monrose, and G.M. Masson, "Language identification of encrypted voip traffic: Alejandra y roberto or alice and bob," in *Proceedings of the 16th USENIX Security Symposium*, 2007, pp. 1–12.

[8] Michael Backes, Goran Doychev, Markus Drmuth, and Boris Kpf, "Speaker recognition in encrypted voice streams," in *Computer Security ESORICS 2010*, Dimitris Gritzalis, Bart Preneel, and Marianthi Theoharidou, Eds., vol. 6345 of *Lecture Notes in Computer Science*, pp. 508–523. Springer Berlin / Heidelberg, 2010.

[9] C.V. Wright, L. Ballard, S.E. Coull, F. Monrose, and G.M. Masson, "Spot me if you can: Uncovering spoken phrases in encrypted voip conversations," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, may 2008, pp. 35 –49.

[10] A.M. White, A.R. Matthews, K.Z. Snow, and F. Monrose, "Phonotactic reconstruction of encrypted voip conversations: Hookt on fon-iks," in *Security and Privacy (SP), 2011 IEEE Symposium on*, may 2011, pp. 3 –18.

[11] Benot Dupasquier, Stefan Burschka, Kieran McLaughlin, and Sakir Sezer, "Analysis of information leakage from encrypted skype conversations," *International Journal of Information Security*, vol. 9, pp. 313–325, 2010.

[12] Suhas Mathur and Wade Trappe, "BIT-TRAPS: Building Information-Theoretic Traffic Privacy Into Packet Streams," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 752–762, 2011.

[13] Mauricio Araya-López, Olivier Buffet, Vincent Thomas, François Charpillet, et al., "A pomdp extension with belief-dependent rewards," in *Neural Information Processing Systems-NIPS 2010*, 2010.

[14] S. Yuksel, T. Basar, and S.P. Meyn, "Optimal causal quantization of markov sources with distortion constraints," in *Information Theory and Applications Workshop, 2008*, 27 2008-feb. 1 2008, pp. 26 –30.